AIDA64 Extreme

Navigation

Version	AIDA64 v5.20.3400
Benchmark Module	4.1.633-x64
Homepage	http://www.aida64.com/
Report Type	Report Wizard
Computer	LTRANPHD
Generator	Liem
Operating System	Microsoft Windows 8.1 Professional 6.3.9600.17736 (Win8.1 RTM)
Date	2015-04-29
Time	11:38

Summary

Computer:

Computer Type	ACPI x64-based PC (Mobile)
Operating System	Microsoft Windows 8.1 Professional
OS Service Pack	-
Internet Explorer	11.0.9600.17728
DirectX	DirectX 11.2
Computer Name	LTRANPHD
User Name	Liem
Logon Domain	LTRANPHD
Date / Time	2015-04-29 / 11:38

Motherboard:

CPU Type	Mobile DualCore Intel Core i7-3520M, 3600 MHz (36 x 100)
Motherboard Name	Gateway EG50_HC_HR
Motherboard Chipset	Intel Panther Point HM70, Intel Ivy Bridge
System Memory	16276 MB (DDR3-1600 DDR3 SDRAM)
DIMM1: Kingston 99U5428-018.A00LF	8 GB DDR3-1600 DDR3 SDRAM (11-11-11-28 @ 800 MHz) (10-10-10-27 @ 761 MHz) (9-9-9-24 @ 685 MHz) (8-8-8-22 @ 609 MHz) (7-7-7-19 @ 533 MHz) (6-6-6-16 @ 457 MHz) (5-5-5-14 @ 380 MHz)
DIMM3: Kingston 99U5428-018.A00LF	8 GB DDR3-1600 DDR3 SDRAM (11-11-11-28 @ 800 MHz) (10-10-10-27 @ 761 MHz) (9-9-9-24 @ 685 MHz) (8-8-8-22 @ 609 MHz) (7-7-7-19 @ 533 MHz) (6-6-6-16 @ 457 MHz) (5-5-5-14 @ 380 MHz)
BIOS Type	Insyde (12/16/2013)

Display:

Video Adapter	Intel(R) HD Graphics 4000 (2112 MB)
Video Adapter	Intel(R) HD Graphics 4000 (2112 MB)
Video Adapter	Intel(R) HD Graphics 4000 (2112 MB)
3D Accelerator	Intel HD Graphics 4000
Monitor	AU Optronics B156XW02 V6 [15.6" LCD]

Multimedia:

Audio Adapter	Intel Panther Point HDMI @ Intel Panther Point PCH - High Definition Audio Controller [C-1]
Audio Adapter	Realtek ALC269 @ Intel Panther Point PCH - High Definition Audio Controller [C-1]

Storage:

IDE Controller	Intel(R) 7 Series/C216 Chipset Family SATA AHCI Controller - 1E03
Storage Controller	Microsoft Storage Spaces Controller

Disk Drive	OCZ-AGILITY4 (SATA-III)
Optical Drive	MATSHITA DVD-RAM UJ8C0
SMART Hard Disks Status	OK

Partitions:

C: (NTFS)	276.9 GB (227.6 GB free)
Total Size	276.9 GB (227.6 GB free)

Input:

Keyboard	Standard PS/2 Keyboard
Mouse	HID-compliant mouse
Mouse	PS/2 Compatible Mouse

Network:

Primary IP Address	192.168.1.109
Primary MAC Address	D8-FC-93-E4-C0-EB
Network Adapter	Bluetooth Device (Personal Area Network)
Network Adapter	Broadcom NetLink (TM) Gigabit Ethernet
Network Adapter	Intel(R) Dual Band Wireless-AC 7260 (192.168.1.109)
Network Adapter	Microsoft Wi-Fi Direct Virtual Adapter #4

Peripherals:

Printer	Fax
Printer	Microsoft XPS Document Writer
Printer	Send To OneNote 2013
USB2 Controller	Intel Panther Point PCH - USB 2.0 EHCI Controller #1 [C-1]
USB2 Controller	Intel Panther Point PCH - USB 2.0 EHCI Controller #2 [C-1]
USB Device	Generic Bluetooth Radio
USB Device	Generic USB Hub
USB Device	Generic USB Hub
USB Device	HD Webcam
USB Device	USB Composite Device
USB Device	USB Input Device
Battery	Microsoft AC Adapter
Battery	Microsoft ACPI-Compliant Control Method Battery

DMI:

DMI BIOS Vendor	Gateway
DMI BIOS Version	V2.21
DMI System Manufacturer	Gateway
DMI System Product	NE56R
DMI System Version	V2.21
DMI System Serial Number	NXY1UAA0052191440E1601
DMI System UUID	98097BAD-95BB11E1-B778DC0E-A1B4F190
DMI Motherboard Manufacturer	Gateway
DMI Motherboard Product	EG50_HC_HR
DMI Motherboard Version	Type2 - Board Version
DMI Motherboard Serial Number	Type2 - Board Serial Number
DMI Chassis Manufacturer	Gateway
DMI Chassis Version	V2.21
DMI Chassis Serial Number	NXY1UAA0052191440E1601
DMI Chassis Asset Tag	
DMI Chassis Type	Notebook

DMI Total / Free Memory Sockets	4 / 2

Computer Name

Type	Class	Computer Name
Computer Comment	Logical	
NetBIOS Name	Logical	LTRANPHD
DNS Host Name	Logical	LTranPHD
DNS Domain Name	Logical	
Fully Qualified DNS Name	Logical	LTranPHD
NetBIOS Name	Physical	LTRANPHD
DNS Host Name	Physical	LTranPHD
DNS Domain Name	Physical	
Fully Qualified DNS Name	Physical	LTranPHD

DMI

[BIOS]

BIOS Properties:

Vendor	Gateway
Version	V2.21
Release Date	12/16/2013
Size	3584 KB
System BIOS Version	2.21
Embedded Controller Firmware Version	0.0
Boot Devices	Floppy Disk, Hard Disk, CD-ROM
Capabilities	Flash BIOS, Shadow BIOS, Selectable Boot, EDD, BBS
Supported Standards	DMI, ACPI, UEFI
Expansion Capabilities	PCI, USB
Virtual Machine	No

[System]

System Properties:

Manufacturer	Gateway
Product	NE56R
Version	V2.21
Serial Number	NXY1UAA0052191440E1601
SKU#	NE56R_0649_V2.21
Family	Type1Family
Universal Unique ID	98097BAD-95BB11E1-B778DC0E-A1B4F190
Wake-Up Type	Power Switch

[Motherboard]

Motherboard Properties:

Manufacturer	Gateway
Product	EG50_HC_HR
Version	Type2 - Board Version
Serial Number	Type2 - Board Serial Number
Asset Tag	Type2 - Board Asset Tag

[Chassis]

Chassis Properties:

Manufacturer	Gateway
Version	V2.21
Serial Number	NXY1UAA0052191440E1601
Chassis Type	Notebook
Boot-Up State	Safe
Power Supply State	Safe
Thermal State	Safe
Security Status	None

[Memory Controller]

Memory Controller Properties:

Error Detection Method	None
Error Correction	None
Supported Memory Interleave	1-Way
Current Memory Interleave	1-Way
Maximum Memory Module Size	8192 MB
Memory Slots	4

[Processors / Intel(R) Core(TM) i7-3520M CPU @ 2.90GHz]

Processor Properties:

Manufacturer	Intel(R) Corporation
Version	Intel(R) Core(TM) i7-3520M CPU @ 2.90GHz
Serial Number	To Be Filled By O.E.M.
Asset Tag	To Be Filled By O.E.M.
Part Number	To Be Filled By O.E.M.
External Clock	100 MHz
Maximum Clock	4000 MHz
Current Clock	2900 MHz
Type	Central Processor
Voltage	1.0 V
Status	Enabled
Upgrade	Socket rPGA988B
Socket Designation	U3E1
HTT / CMP Units	2 / 2
Capabilities	64-bit, Multi-Core, Multiple Hardware Threads, Execute Protection, Enhanced Virtualization, Power/Performance Control

CPU Manufacturer:

Company Name	Intel Corporation
Product Information	http://ark.intel.com/search.aspx?q=Intel Core i7-3520M
Driver Update	http://www.aida64.com/driver-updates

[Caches / L1 Cache]

Cache Properties:

Type	Internal
Status	Enabled
Operational Mode	Write-Through
Associativity	8-way Set-Associative
Maximum Size	32 KB
Installed Size	32 KB
Error Correction	Parity
Socket Designation	L1 Cache

[Caches / L1 Cache]

Cache Properties:

Type	Internal
Status	Enabled
Operational Mode	Write-Through
Associativity	8-way Set-Associative
Maximum Size	32 KB
Installed Size	32 KB
Error Correction	Parity
Socket Designation	L1 Cache

[Caches / L2 Cache]

Cache Properties:

Type	Internal
Status	Enabled
Operational Mode	Write-Through
Associativity	8-way Set-Associative
Maximum Size	256 KB
Installed Size	256 KB
Error Correction	Multi-bit ECC
Socket Designation	L2 Cache

[Caches / L3 Cache]

Cache Properties:

Type	Internal
Status	Enabled
Operational Mode	Write-Back
Associativity	16-way Set-Associative
Maximum Size	4096 KB
Installed Size	4096 KB
Error Correction	Multi-bit ECC
Socket Designation	L3 Cache

[Memory Arrays / System Memory]

Memory Array Properties:

Location	Motherboard
Memory Array Function	System Memory
Error Correction	None

Max. Memory Capacity	32 GB
Memory Devices	4

[Memory Modules / DIMM0]

Memory Module Properties:

Socket Designation	DIMM0
Type	DIMM
Installed Size	8192 MB
Enabled Size	8192 MB

[Memory Modules / DIMM1]

Memory Module Properties:

Socket Designation	DIMM1
Type	DIMM
Installed Size	Not Installed
Enabled Size	Not Installed

[Memory Modules / DIMM1]

Memory Module Properties:

Socket Designation	DIMM1
Type	DIMM
Installed Size	8192 MB
Enabled Size	8192 MB

[Memory Modules / DIMM3]

Memory Module Properties:

Socket Designation	DIMM3
Type	DIMM
Installed Size	Not Installed
Enabled Size	Not Installed

[Memory Devices / DIMM0]

Memory Device Properties:

Form Factor	SODIMM
Type	DDR3
Type Detail	Synchronous
Size	8 GB
Max. Clock Speed	1600 MHz
Current Clock Speed	1600 MHz
Total Width	64-bit
Data Width	64-bit
Ranks	2
Device Locator	DIMM0
Bank Locator	BANK 0
Manufacturer	Kingston
Serial Number	5E290E52
Asset Tag	Unknown

Part Number	99U5428-018.A00LF

[Memory Devices / DIMM1]

Memory Device Properties:

Form Factor	DIMM
Device Locator	DIMM1
Bank Locator	BANK 1
Manufacturer	Empty
Serial Number	Empty
Asset Tag	Unknown
Part Number	Empty

[Memory Devices / DIMM1]

Memory Device Properties:

Form Factor	SODIMM
Type	DDR3
Type Detail	Synchronous
Size	8 GB
Max. Clock Speed	1600 MHz
Current Clock Speed	1600 MHz
Total Width	64-bit
Data Width	64-bit
Ranks	2
Device Locator	DIMM1
Bank Locator	BANK 2
Manufacturer	Kingston
Serial Number	5F290052
Asset Tag	Unknown
Part Number	99U5428-018.A00LF

[Memory Devices / DIMM3]

Memory Device Properties:

Form Factor	DIMM
Device Locator	DIMM3
Bank Locator	BANK 3
Manufacturer	Empty
Serial Number	Empty
Asset Tag	Unknown
Part Number	Empty

[System Slots / J5C1]

System Slot Properties:

Slot Designation	J5C1
Type	PCI-E x16
Usage	Empty
Data Bus Width	x16

[System Slots / J6C1]

System Slot Properties:

Slot Designation	J6C1
Type	PCI-E x1
Usage	Empty
Data Bus Width	x1

[System Slots / J6C2]

System Slot Properties:

Slot Designation	J6C2
Type	PCI-E x1
Usage	Empty
Data Bus Width	x1

[System Slots / J6D2]

System Slot Properties:

Slot Designation	J6D2
Type	PCI-E x1
Usage	Empty
Data Bus Width	x1

[System Slots / J7C1]

System Slot Properties:

Slot Designation	J7C1
Type	PCI-E x1
Usage	Empty
Data Bus Width	x1

[System Slots / J7D2]

System Slot Properties:

Slot Designation	J7D2
Type	PCI-E x1
Usage	Empty
Data Bus Width	x1

[System Slots / J8C1]

System Slot Properties:

Slot Designation	J8C1
Type	PCI-E x1
Usage	Empty
Data Bus Width	x1

[System Slots / J8C2]

System Slot Properties:

Slot Designation	J8C2
Type	PCI-E x16

Usage	Empty
Data Bus Width	x16

[On-Board Devices / Video Graphics Controller]

On-Board Device Properties:

Description	Video Graphics Controller
Type	Video
Status	Enabled

[On-Board Devices / Lan Controller]

On-Board Device Properties:

Description	Lan Controller
Type	Ethernet
Status	Enabled

[Miscellaneous]

Miscellaneous:

OEM String	String1 for Original Equipment Manufacturer
OEM String	String2 for Original Equipment Manufacturer
OEM String	String3 for Original Equipment Manufacturer
OEM String	String4 for Original Equipment Manufacturer
OEM String	String5 for Original Equipment Manufacturer
System Configuration Option	String2 for Type12 Equipment Manufacturer
System Configuration Option	String3 for Type12 Equipment Manufacturer
System Configuration Option	String4 for Type12 Equipment Manufacturer

Overclock

CPU Properties:

CPU Type	Mobile DualCore Intel Core i7-3520M
CPU Alias	Ivy Bridge-MB
CPU Stepping	E1/L1/N0/P0
Engineering Sample	No
CPUID CPU Name	Intel(R) Core(TM) i7-3520M CPU @ 2.90GHz
CPUID Revision	000306A9h
CPU VID	1.1859 V

CPU Speed:

CPU Clock	3392.4 MHz (original: 2900 MHz, overclock: 17%)
CPU Multiplier	34x
CPU FSB	99.8 MHz (original: 100 MHz)
North Bridge Clock	3392.4 MHz
Memory Bus	798.2 MHz
DRAM:FSB Ratio	24:3

CPU Cache:

L1 Code Cache	32 KB per core
L1 Data Cache	32 KB per core

L2 Cache	256 KB per core (On-Die, ECC, Full-Speed)
L3 Cache	4 MB (On-Die, ECC, Full-Speed)

Motherboard Properties:

Motherboard ID	<DMI>
Motherboard Name	Gateway EG50_HC_HR

Chipset Properties:

Motherboard Chipset	Intel Panther Point HM70, Intel Ivy Bridge
Memory Timings	11-11-11-28 (CL-RCD-RP-RAS)
Command Rate (CR)	1T
DIMM1: Kingston 99U5428-018.A00LF	8 GB DDR3-1600 DDR3 SDRAM (11-11-11-28 @ 800 MHz) (10-10-10-27 @ 761 MHz) (9-9-9-24 @ 685 MHz) (8-8-8-22 @ 609 MHz) (7-7-7-19 @ 533 MHz) (6-6-6-16 @ 457 MHz) (5-5-5-14 @ 380 MHz)
DIMM3: Kingston 99U5428-018.A00LF	8 GB DDR3-1600 DDR3 SDRAM (11-11-11-28 @ 800 MHz) (10-10-10-27 @ 761 MHz) (9-9-9-24 @ 685 MHz) (8-8-8-22 @ 609 MHz) (7-7-7-19 @ 533 MHz) (6-6-6-16 @ 457 MHz) (5-5-5-14 @ 380 MHz)

BIOS Properties:

System BIOS Date	12/16/2013
Video BIOS Date	03/14/12
DMI BIOS Version	V2.21

Graphics Processor Properties:

Video Adapter	Intel Ivy Bridge-MB - Integrated Graphics Controller (MB GT2)
GPU Code Name	Ivy Bridge-MB GT2 (Integrated 8086 / 0166, Rev 09)
GPU Clock	349 MHz (original: 649 MHz)

Power Management

Power Management Properties:

Current Power Source	AC Line
Battery Status	100 % (High Level)
Full Battery Lifetime	Unknown
Remaining Battery Lifetime	Unknown

Battery Properties:

Device Name	Li_Ion_4000mA
Manufacturer	PANASONIC
Serial Number	8E9
Unique ID	8E9PANASONIC Li_Ion_4000mA
Battery Type	Rechargeable Li-Ion
Designed Capacity	47520 mWh
Fully Charged Capacity	38081 mWh
Current Capacity	38081 mWh (100 %)
Battery Voltage	12.386 V
Wear Level	19 %
Power State	AC Line

Portable Computer

Centrino (Carmel) Platform Compliancy:

CPU: Intel Pentium M (Banias/Dothan)	No (Mobile Intel Core i7-3520M)
Chipset: Intel i855GM/PM	No (Intel Panther Point HM70, Intel Ivy Bridge)
WLAN: Intel PRO/Wireless	No
System: Centrino Compliant	No

Centrino (Sonoma) Platform Compliancy:

CPU: Intel Pentium M (Dothan)	No (Mobile Intel Core i7-3520M)
Chipset: Intel i915GM/PM	No (Intel Panther Point HM70, Intel Ivy Bridge)
WLAN: Intel PRO/Wireless 2200/2915	No
System: Centrino Compliant	No

Centrino (Napa) Platform Compliancy:

CPU: Intel Core (Yonah) / Core 2 (Merom)	No (Mobile Intel Core i7-3520M)
Chipset: Intel i945GM/PM	No (Intel Panther Point HM70, Intel Ivy Bridge)
WLAN: Intel PRO/Wireless 3945/3965	No
System: Centrino Compliant	No

Centrino (Santa Rosa) Platform Compliancy:

CPU: Intel Core 2 (Merom/Penryn)	No (Mobile Intel Core i7-3520M)
Chipset: Intel GM965/PM965	No (Intel Panther Point HM70, Intel Ivy Bridge)
WLAN: Intel Wireless WiFi Link 4965	No
System: Centrino Compliant	No

Centrino 2 (Montevina) Platform Compliancy:

CPU: Intel Core 2 (Penryn)	No (Mobile Intel Core i7-3520M)
Chipset: Mobile Intel 4 Series	No (Intel Panther Point HM70, Intel Ivy Bridge)
WLAN: Intel WiFi Link 5000 Series	No
System: Centrino 2 Compliant	No

Centrino (Calpella) Platform Compliancy:

CPU: Intel Core i3/i5/i7 (Arrandale/Clarksfield)	No (Mobile Intel Core i7-3520M)
Chipset: Mobile Intel 5 Series	No (Intel Panther Point HM70, Intel Ivy Bridge)
WLAN: Intel Centrino Advanced-N / Ultimate-N / Wireless-N	No
System: Centrino Compliant	No

Centrino (Huron River) Platform Compliancy:

CPU: Intel Core i3/i5/i7 (Sandy Bridge-MB)	No (Mobile Intel Core i7-3520M)
Chipset: Mobile Intel 6 Series	No (Intel Panther Point HM70, Intel Ivy Bridge)
WLAN: Intel Centrino Advanced-N / Ultimate-N / Wireless-N	No
System: Centrino Compliant	No

Centrino (Chief River) Platform Compliancy:

CPU: Intel Core i3/i5/i7 (Ivy Bridge-MB)	Yes (Mobile Intel Core i7-3520M)
Chipset: Mobile Intel 7 Series	Yes (Intel Panther Point HM70, Intel Ivy Bridge)
WLAN: Intel Centrino Advanced-N / Ultimate-N / Wireless-N	No
System: Centrino Compliant	No

Centrino (Shark Bay-MB) Platform Compliancy:

CPU: Intel Core i3/i5/i7 (Haswell-MB)	No (Mobile Intel Core i7-3520M)
Chipset: Mobile Intel 8/9 Series	No (Intel Panther Point HM70, Intel Ivy Bridge)
WLAN: Intel Centrino Advanced-N / Ultimate-N / Wireless-N	Yes
System: Centrino Compliant	No

Sensor

Sensor Properties:

Sensor Type	CPU, PCH, SNB

Temperatures:

CPU Package	54 °C (129 °F)
CPU IA Cores	52 °C (126 °F)
CPU GT Cores	54 °C (129 °F)
CPU #1 / Core #1	55 °C (131 °F)
CPU #1 / Core #2	54 °C (129 °F)
PCH Diode	60 °C (140 °F)

Voltage Values:

CPU Core	1.166 V
Battery	12.386 V

Power Values:

CPU Package	3.69 W
CPU IA Cores	1.44 W
CPU GT Cores	0.00 W
CPU Uncore	2.25 W
Battery Charge Rate	AC Line

CPU

CPU Properties:

CPU Type	Mobile DualCore Intel Core i7-3520M, 3600 MHz (36 x 100)
CPU Alias	Ivy Bridge-MB
CPU Stepping	E1/L1/N0/P0
Instruction Set	x86, x86-64, MMX, SSE, SSE2, SSE3, SSSE3, SSE4.1, SSE4.2, AVX, AES
Original Clock	2900 MHz
Min / Max CPU Multiplier	12x / 33x
Engineering Sample	No
L1 Code Cache	32 KB per core
L1 Data Cache	32 KB per core
L2 Cache	256 KB per core (On-Die, ECC, Full-Speed)
L3 Cache	4 MB (On-Die, ECC, Full-Speed)

CPU Physical Info:

Package Type	988 Pin rPGA
Package Size	37.5 mm x 37.5 mm
Process Technology	22 nm, CMOS, Cu, High-K + Metal Gate
Typical Power	35 W

CPU Manufacturer:

Company Name	Intel Corporation
Product Information	http://ark.intel.com/search.aspx?q=Intel Core i7-3520M
Driver Update	http://www.aida64.com/driver-updates

Multi CPU:

Motherboard ID	Insyde Calpella
CPU #1	Intel(R) Core(TM) i7-3520M CPU @ 2.90GHz, 2893 MHz
CPU #2	Intel(R) Core(TM) i7-3520M CPU @ 2.90GHz, 2893 MHz
CPU #3	Intel(R) Core(TM) i7-3520M CPU @ 2.90GHz, 2893 MHz
CPU #4	Intel(R) Core(TM) i7-3520M CPU @ 2.90GHz, 2893 MHz

CPU Utilization:

CPU #1 / Core #1 / HTT Unit #1	0%
CPU #1 / Core #1 / HTT Unit #2	0%
CPU #1 / Core #2 / HTT Unit #1	0%
CPU #1 / Core #2 / HTT Unit #2	0%

CPUID

CPUID Properties:

CPUID Manufacturer	GenuineIntel
CPUID CPU Name	Intel(R) Core(TM) i7-3520M CPU @ 2.90GHz
CPUID Revision	000306A9h
IA Brand ID	00h (Unknown)
Platform ID	29h / MC 10h (rPGA988B)
Microcode Update Revision	1Bh
HTT / CMP Units	2 / 2
Tjmax Temperature	105 °C (221 °F)
CPU Thermal Design Power	35 W
CPU IA Cores Thermal Design Current	112 A
CPU GT Cores Thermal Design Current	50 A
CPU Max Power Limit	Unlimited Power / Unlimited Time
CPU Power Limit 1 (Long Duration)	35 W / 28.00 sec (Locked)
CPU Power Limit 2 (Short Duration)	43.8 W / Unlimited Time (Locked)
Max Turbo Boost Multipliers	1C: 36x, 2C: 34x

Instruction Set:

64-bit x86 Extension (AMD64, Intel64)	Supported
AMD 3DNow!	Not Supported
AMD 3DNow! Professional	Not Supported
AMD 3DNowPrefetch	Not Supported
AMD Enhanced 3DNow!	Not Supported
AMD Extended MMX	Not Supported
AMD FMA4	Not Supported
AMD MisAligned SSE	Not Supported
AMD SSE4A	Not Supported
AMD XOP	Not Supported
Cyrix Extended MMX	Not Supported
Enhanced REP MOVSB/STOSB	Supported
Float-16 Conversion Instructions	Supported, Enabled
IA-64	Not Supported
IA AES Extensions	Supported
IA AVX	Supported, Enabled
IA AVX2	Not Supported
IA AVX-512 (AVX512F)	Not Supported
IA AVX-512 52-bit Integer Instructions (AVX512IFMA52)	Not Supported

IA AVX-512 Byte and Word Instructions (AVX512BW)	Not Supported
IA AVX-512 Conflict Detection Instructions (AVX512CD)	Not Supported
IA AVX-512 Doubleword and Quadword Instructions (AVX512DQ)	Not Supported
IA AVX-512 Exponential and Reciprocal Instructions (AVX512ER)	Not Supported
IA AVX-512 Prefetch Instructions (AVX512PF)	Not Supported
IA AVX-512 Vector Bit Manipulation Instructions (AVX512VBMI)	Not Supported
IA AVX-512 Vector Length Extensions (AVX512VL)	Not Supported
IA BMI1	Not Supported
IA BMI2	Not Supported
IA FMA	Not Supported
IA MMX	Supported
IA SHA Extensions	Not Supported
IA SSE	Supported
IA SSE2	Supported
IA SSE3	Supported
IA Supplemental SSE3	Supported
IA SSE4.1	Supported
IA SSE4.2	Supported
VIA Alternate Instruction Set	Not Supported
ADCX / ADOX Instruction	Not Supported
CLFLUSH Instruction	Supported
CLFLUSHOPT Instruction	Not Supported
CLWB Instruction	Not Supported
CMPXCHG8B Instruction	Supported
CMPXCHG16B Instruction	Supported
Conditional Move Instruction	Supported
INVPCID Instruction	Not Supported
LAHF / SAHF Instruction	Supported
LZCNT Instruction	Not Supported
MONITOR / MWAIT Instruction	Supported
MONITORX / MWAITX Instruction	Not Supported
MOVBE Instruction	Not Supported
PCLMULQDQ Instruction	Supported
PCOMMIT Instruction	Not Supported
POPCNT Instruction	Supported
PREFETCHWT1 Instruction	Not Supported
RDFSBASE / RDGSBASE / WRFSBASE / WRGSBASE Instruction	Supported
RDRAND Instruction	Supported
RDSEED Instruction	Not Supported
RDTSCP Instruction	Supported
SKINIT / STGI Instruction	Not Supported
SYSCALL / SYSRET Instruction	Not Supported
SYSENTER / SYSEXIT Instruction	Supported
Trailing Bit Manipulation Instructions	Not Supported
VIA FEMMS Instruction	Not Supported

Security Features:

Advanced Cryptography Engine (ACE)	Not Supported
Advanced Cryptography Engine 2 (ACE2)	Not Supported
Data Execution Prevention (DEP, NX, EDB)	Supported
Hardware Random Number Generator (RNG)	Not Supported
Hardware Random Number Generator 2 (RNG2)	Not Supported
Memory Protection Extensions (MPX)	Not Supported
PadLock Hash Engine (PHE)	Not Supported

PadLock Hash Engine 2 (PHE2)	Not Supported
PadLock Montgomery Multiplier (PMM)	Not Supported
PadLock Montgomery Multiplier 2 (PMM2)	Not Supported
Processor Serial Number (PSN)	Not Supported
Safer Mode Extensions (SMX)	Supported
Software Guard Extensions (SGX)	Not Supported
Supervisor Mode Access Prevention (SMAP)	Not Supported
Supervisor Mode Execution Protection (SMEP)	Supported

Power Management Features:

Application Power Management (APM)	Not Supported
Automatic Clock Control	Supported
Core C6 State (CC6)	Not Supported
Digital Thermometer	Supported
Dynamic FSB Frequency Switching	Not Supported
Enhanced Halt State (C1E)	Supported, Enabled
Enhanced SpeedStep Technology (EIST, ESS)	Supported, Enabled
Frequency ID Control	Not Supported
Hardware P-State Control	Not Supported
Hardware Thermal Control (HTC)	Not Supported
LongRun	Not Supported
LongRun Table Interface	Not Supported
Overstress	Not Supported
Package C6 State (PC6)	Not Supported
Parallax	Not Supported
PowerSaver 1.0	Not Supported
PowerSaver 2.0	Not Supported
PowerSaver 3.0	Not Supported
Processor Duty Cycle Control	Supported
Software Thermal Control	Not Supported
Temperature Sensing Diode	Not Supported
Thermal Monitor 1	Supported
Thermal Monitor 2	Supported
Thermal Monitor 3	Not Supported
Thermal Monitoring	Not Supported
Thermal Trip	Not Supported
Voltage ID Control	Not Supported

Virtualization Features:

Extended Page Table (EPT)	Supported
Hypervisor	Not Present
INVEPT Instruction	Supported
INVVPID Instruction	Supported
Nested Paging (NPT, RVI)	Not Supported
Secure Virtual Machine (SVM, Pacifica)	Not Supported
Virtual Machine Extensions (VMX, Vanderpool)	Supported
Virtual Processor ID (VPID)	Supported

CPUID Features:

1 GB Page Size	Not Supported
36-bit Page Size Extension	Supported
64-bit DS Area	Supported
Adaptive Overclocking	Not Supported
Address Region Registers (ARR)	Not Supported

Configurable TDP (cTDP)	Not Supported
Core Performance Boost (CPB)	Not Supported
Core Performance Counters	Not Supported
CPL Qualified Debug Store	Supported
Data Breakpoint Extension	Not Supported
Debug Trace Store	Supported
Debugging Extension	Supported
Deprecated FPU CS and FPU DS	Not Supported
Direct Cache Access	Not Supported
Dynamic Acceleration Technology (IDA)	Not Supported
Dynamic Configurable TDP (DcTDP)	Not Supported
Extended APIC Register Space	Not Supported
Fast Save & Restore	Supported
Hardware Lock Elision (HLE)	Not Supported
Hybrid Boost	Not Supported
Hyper-Threading Technology (HTT)	Supported, Enabled
Instruction Based Sampling	Not Supported
Invariant Time Stamp Counter	Supported
L1 Context ID	Not Supported
L2I Performance Counters	Not Supported
Lightweight Profiling	Not Supported
Local APIC On Chip	Supported
Machine Check Architecture (MCA)	Supported
Machine Check Exception (MCE)	Supported
Memory Configuration Registers (MCR)	Not Supported
Memory Type Range Registers (MTRR)	Supported
Model Specific Registers (MSR)	Supported
NB Performance Counters	Not Supported
Page Attribute Table (PAT)	Supported
Page Global Extension	Supported
Page Size Extension (PSE)	Supported
Pending Break Event (PBE)	Supported
Performance Time Stamp Counter (PTSC)	Not Supported
Physical Address Extension (PAE)	Supported
Platform Quality of Service Enforcement (PQE)	Not Supported
Platform Quality of Service Monitoring (PQM)	Not Supported
Process Context Identifiers (PCID)	Supported
Processor Feedback Interface	Not Supported
Processor Trace (PT)	Not Supported
Restricted Transactional Memory (RTM)	Not Supported
Self-Snoop	Supported
Time Stamp Counter (TSC)	Supported
Turbo Boost	Supported, Enabled
Virtual Mode Extension	Supported
Watchdog Timer	Not Supported
x2APIC	Supported, Enabled
XGETBV / XSETBV OS Enabled	Supported
XSAVE / XRSTOR / XSETBV / XGETBV Extended States	Supported
XSAVEOPT	Supported

CPUID Registers (CPU #1):

CPUID 00000000	0000000D-756E6547-6C65746E-49656E69 [GenuineIntel]
CPUID 00000001	000306A9-00100800-7FBAE3FF-BFEBFBFF
CPUID 00000002	76035A01-00F0B2FF-00000000-00CA0000

CPUID 00000003	00000000-00000000-00000000-00000000
CPUID 00000004	1C004121-01C0003F-0000003F-00000000 [SL 00]
CPUID 00000004	1C004122-01C0003F-0000003F-00000000 [SL 01]
CPUID 00000004	1C004143-01C0003F-000001FF-00000000 [SL 02]
CPUID 00000004	1C03C163-03C0003F-00000FFF-00000006 [SL 03]
CPUID 00000005	00000040-00000040-00000003-00021120
CPUID 00000006	00000077-00000002-00000009-00000000
CPUID 00000007	00000000-00000281-00000000-00000000
CPUID 00000008	00000000-00000000-00000000-00000000
CPUID 00000009	00000000-00000000-00000000-00000000
CPUID 0000000A	07300403-00000000-00000000-00000603
CPUID 0000000B	00000001-00000002-00000100-00000000 [SL 00]
CPUID 0000000B	00000004-00000004-00000201-00000000 [SL 01]
CPUID 0000000C	00000000-00000000-00000000-00000000
CPUID 0000000D	00000007-00000340-00000340-00000000 [SL 00]
CPUID 0000000D	00000001-00000000-00000000-00000000 [SL 01]
CPUID 0000000D	00000100-00000240-00000000-00000000 [SL 02]
CPUID 80000000	80000008-00000000-00000000-00000000
CPUID 80000001	00000000-00000000-00000001-28100000
CPUID 80000002	20202020-49202020-6C65746E-20295228 [Intel(R)]
CPUID 80000003	65726F43-294D5428-2D376920-30323533 [Core(TM) i7-3520]
CPUID 80000004	5043204D-20402055-30392E32-007A4847 [M CPU @ 2.90GHz]
CPUID 80000005	00000000-00000000-00000000-00000000
CPUID 80000006	00000000-00000000-01006040-00000000
CPUID 80000007	00000000-00000000-00000000-00000100
CPUID 80000008	00003024-00000000-00000000-00000000

CPUID Registers (CPU #2 Virtual):

CPUID 00000000	0000000D-756E6547-6C65746E-49656E69 [GenuineIntel]
CPUID 00000001	000306A9-01100800-7FBAE3FF-BFEBFBFF
CPUID 00000002	76035A01-00F0B2FF-00000000-00CA0000
CPUID 00000003	00000000-00000000-00000000-00000000
CPUID 00000004	1C004121-01C0003F-0000003F-00000000 [SL 00]
CPUID 00000004	1C004122-01C0003F-0000003F-00000000 [SL 01]
CPUID 00000004	1C004143-01C0003F-000001FF-00000000 [SL 02]
CPUID 00000004	1C03C163-03C0003F-00000FFF-00000006 [SL 03]
CPUID 00000005	00000040-00000040-00000003-00021120
CPUID 00000006	00000077-00000002-00000009-00000000
CPUID 00000007	00000000-00000281-00000000-00000000
CPUID 00000008	00000000-00000000-00000000-00000000
CPUID 00000009	00000000-00000000-00000000-00000000
CPUID 0000000A	07300403-00000000-00000000-00000603
CPUID 0000000B	00000001-00000002-00000100-00000001 [SL 00]
CPUID 0000000B	00000004-00000004-00000201-00000001 [SL 01]
CPUID 0000000C	00000000-00000000-00000000-00000000
CPUID 0000000D	00000007-00000340-00000340-00000000 [SL 00]
CPUID 0000000D	00000001-00000000-00000000-00000000 [SL 01]
CPUID 0000000D	00000100-00000240-00000000-00000000 [SL 02]
CPUID 80000000	80000008-00000000-00000000-00000000
CPUID 80000001	00000000-00000000-00000001-28100000
CPUID 80000002	20202020-49202020-6C65746E-20295228 [Intel(R)]
CPUID 80000003	65726F43-294D5428-2D376920-30323533 [Core(TM) i7-3520]
CPUID 80000004	5043204D-20402055-30392E32-007A4847 [M CPU @ 2.90GHz]
CPUID 80000005	00000000-00000000-00000000-00000000

CPUID 80000006	00000000-00000000-01006040-00000000
CPUID 80000007	00000000-00000000-00000000-00000100
CPUID 80000008	00003024-00000000-00000000-00000000

CPUID Registers (CPU #3):

CPUID 00000000	0000000D-756E6547-6C65746E-49656E69 [GenuineIntel]
CPUID 00000001	000306A9-02100800-7FBAE3FF-BFEBFBFF
CPUID 00000002	76035A01-00F0B2FF-00000000-00CA0000
CPUID 00000003	00000000-00000000-00000000-00000000
CPUID 00000004	1C004121-01C0003F-0000003F-00000000 [SL 00]
CPUID 00000004	1C004122-01C0003F-0000003F-00000000 [SL 01]
CPUID 00000004	1C004143-01C0003F-000001FF-00000000 [SL 02]
CPUID 00000004	1C03C163-03C0003F-00000FFF-00000006 [SL 03]
CPUID 00000005	00000040-00000040-00000003-00021120
CPUID 00000006	00000077-00000002-00000009-00000000
CPUID 00000007	00000000-00000281-00000000-00000000
CPUID 00000008	00000000-00000000-00000000-00000000
CPUID 00000009	00000000-00000000-00000000-00000000
CPUID 0000000A	07300403-00000000-00000000-00000603
CPUID 0000000B	00000001-00000002-00000100-00000002 [SL 00]
CPUID 0000000B	00000004-00000004-00000201-00000002 [SL 01]
CPUID 0000000C	00000000-00000000-00000000-00000000
CPUID 0000000D	00000007-00000340-00000340-00000000 [SL 00]
CPUID 0000000D	00000001-00000000-00000000-00000000 [SL 01]
CPUID 0000000D	00000100-00000240-00000000-00000000 [SL 02]
CPUID 80000000	80000008-00000000-00000000-00000000
CPUID 80000001	00000000-00000000-00000001-28100000
CPUID 80000002	20202020-49202020-6C65746E-20295228 [Intel(R)]
CPUID 80000003	65726F43-294D5428-2D376920-30323533 [Core(TM) i7-3520]
CPUID 80000004	5043204D-20402055-30392E32-007A4847 [M CPU @ 2.90GHz]
CPUID 80000005	00000000-00000000-00000000-00000000
CPUID 80000006	00000000-00000000-01006040-00000000
CPUID 80000007	00000000-00000000-00000000-00000100
CPUID 80000008	00003024-00000000-00000000-00000000

CPUID Registers (CPU #4 Virtual):

CPUID 00000000	0000000D-756E6547-6C65746E-49656E69 [GenuineIntel]
CPUID 00000001	000306A9-03100800-7FBAE3FF-BFEBFBFF
CPUID 00000002	76035A01-00F0B2FF-00000000-00CA0000
CPUID 00000003	00000000-00000000-00000000-00000000
CPUID 00000004	1C004121-01C0003F-0000003F-00000000 [SL 00]
CPUID 00000004	1C004122-01C0003F-0000003F-00000000 [SL 01]
CPUID 00000004	1C004143-01C0003F-000001FF-00000000 [SL 02]
CPUID 00000004	1C03C163-03C0003F-00000FFF-00000006 [SL 03]
CPUID 00000005	00000040-00000040-00000003-00021120
CPUID 00000006	00000077-00000002-00000009-00000000
CPUID 00000007	00000000-00000281-00000000-00000000
CPUID 00000008	00000000-00000000-00000000-00000000
CPUID 00000009	00000000-00000000-00000000-00000000
CPUID 0000000A	07300403-00000000-00000000-00000603
CPUID 0000000B	00000001-00000002-00000100-00000003 [SL 00]
CPUID 0000000B	00000004-00000004-00000201-00000003 [SL 01]
CPUID 0000000C	00000000-00000000-00000000-00000000
CPUID 0000000D	00000007-00000340-00000340-00000000 [SL 00]

CPUID 0000000D	00000001-00000000-00000000-00000000 [SL 01]
CPUID 0000000D	00000100-00000240-00000000-00000000 [SL 02]
CPUID 80000000	80000008-00000000-00000000-00000000
CPUID 80000001	00000000-00000000-00000001-28100000
CPUID 80000002	20202020-49202020-6C65746E-20295228 [Intel(R)]
CPUID 80000003	65726F43-294D5428-2D376920-30323533 [Core(TM) i7-3520]
CPUID 80000004	5043204D-20402055-30392E32-007A4847 [M CPU @ 2.90GHz]
CPUID 80000005	00000000-00000000-00000000-00000000
CPUID 80000006	00000000-00000000-01006040-00000000
CPUID 80000007	00000000-00000000-00000000-00000100
CPUID 80000008	00003024-00000000-00000000-00000000

MSR Registers:

MSR 00000017	0010-0000-0000-0000 [PlatID = 4]
MSR 0000001B	0000-0000-FEE0-0D00
MSR 00000035	0000-0000-0002-0004
MSR 0000008B	0000-001B-0000-0000
MSR 000000CE	0008-0C10-F001-1D00 [eD = 0]
MSR 000000E7	0000-0000-0001-B65D
MSR 000000E7	0000-0000-0002-CF3E [S200]
MSR 000000E7	0000-0000-005B-60BC [S200]
MSR 000000E8	0000-0000-0000-C6E9 [S200]
MSR 000000E8	0000-0000-0000-FF14 [S200]
MSR 000000E8	0000-0000-0001-1FA3
MSR 00000194	0000-0000-0019-0000
MSR 00000198	0000-254F-0000-2200
MSR 00000198	0000-254F-0000-2200 [S200]
MSR 00000198	0000-254F-0000-2200 [S200]
MSR 00000199	0000-0000-0000-FF00
MSR 0000019A	0000-0000-0000-0008
MSR 0000019B	0000-0000-0000-0010
MSR 0000019C	0000-0000-883A-0008 [S200]
MSR 0000019C	0000-0000-883F-0008
MSR 0000019C	0000-0000-883F-0008 [S200]
MSR 0000019D	0000-0000-0000-0000
MSR 000001A0	0000-0000-0085-0089
MSR 000001A2	0000-0000-0069-1200
MSR 000001A4	0000-0000-0000-0000
MSR 000001AA	0000-0000-0040-0000
MSR 000001AC	< FAILED >
MSR 000001AD	0000-0000-2222-2224
MSR 000001B0	0000-0000-0000-0000
MSR 000001B1	0000-0000-883F-0008
MSR 000001B2	0000-0000-0000-0000
MSR 000001FC	0000-0000-0014-005F
MSR 00000300	< FAILED >
MSR 00000480	00DA-0400-0000-0010
MSR 00000481	0000-007F-0000-0016
MSR 00000482	FFF9-FFFE-0401-E172
MSR 00000483	007F-FFFF-0003-6DFF
MSR 00000484	0000-FFFF-0000-11FF
MSR 00000485	0000-0000-1004-01E5
MSR 00000486	0000-0000-8000-0021
MSR 00000487	0000-0000-FFFF-FFFF

MSR 00000488	0000-0000-0000-2000
MSR 00000489	0000-0000-0017-67FF
MSR 0000048A	0000-0000-0000-002A
MSR 0000048B	0000-08FF-0000-0000
MSR 0000048C	0000-0F01-0611-4141
MSR 0000048D	0000-007F-0000-0016
MSR 0000048E	FFF9-FFFE-0400-6172
MSR 0000048F	007F-FFFF-0003-6DFB
MSR 00000490	0000-FFFF-0000-11FB
MSR 00000601	1814-1494-8000-0380
MSR 00000602	1814-1494-8000-0190
MSR 00000603	0000-0000-8030-3030
MSR 00000604	0000-0000-8064-6464
MSR 00000606	0000-0000-000A-1003
MSR 0000060A	0000-0000-0000-883B
MSR 0000060B	0000-0000-0000-8850
MSR 0000060C	0000-0000-0000-8857
MSR 0000060D	0000-0008-A6B9-1A3D
MSR 00000610	8000-815E-00DC-8118
MSR 00000611	0000-0000-0799-6197 [S200]
MSR 00000611	0000-0000-0799-E232 [S200]
MSR 00000611	0000-0000-079A-623C
MSR 00000613	< FAILED >
MSR 00000614	0000-0000-00C0-0118
MSR 00000618	< FAILED >
MSR 00000619	< FAILED >
MSR 0000061B	< FAILED >
MSR 0000061C	< FAILED >
MSR 00000638	0000-0000-0000-0000
MSR 00000639	0000-0000-053E-E611 [S200]
MSR 00000639	0000-0000-053E-FEAA [S200]
MSR 00000639	0000-0000-053F-15BC
MSR 0000063A	0000-0000-0000-0000
MSR 0000063B	< FAILED >
MSR 00000640	0000-0000-0000-0000
MSR 00000641	0000-0000-0027-5086
MSR 00000641	0000-0000-0027-5086 [S200]
MSR 00000641	0000-0000-0027-5086 [S200]
MSR 00000642	0000-0000-0000-0008
MSR 00000648	0000-0000-0000-001D
MSR 00000649	00C0-0000-0000-0000
MSR 0000064A	00C0-0000-0000-0000
MSR 0000064B	0000-0000-8000-0000
MSR 0000064C	0000-0000-0000-0000
MSR 00000832	0000-0000-0003-00D1
MSR 00000838	0000-0000-0000-0000
MSR 00000839	0000-0000-0000-0000
MSR 0000083E	0000-0000-0000-000A

Motherboard

Motherboard Properties:

Motherboard ID	<DMI>
Motherboard Name	Gateway EG50_HC_HR

Front Side Bus Properties:

Bus Type	BCLK
Real Clock	100 MHz
Effective Clock	100 MHz

Memory Bus Properties:

Bus Type	Dual DDR3 SDRAM
Bus Width	128-bit
DRAM:FSB Ratio	24:3
Real Clock	800 MHz (DDR)
Effective Clock	1600 MHz
Bandwidth	25600 MB/s

Chipset Bus Properties:

Bus Type	Intel Direct Media Interface v2.0

Memory

Physical Memory:

Total	16276 MB
Used	1842 MB
Free	14435 MB
Utilization	11 %

Swap Space:

Total	18708 MB
Used	2253 MB
Free	16456 MB
Utilization	12 %

Virtual Memory:

Total	34985 MB
Used	4094 MB
Free	30891 MB
Utilization	12 %

Paging File:

Paging File	C:\pagefile.sys
Current Size	2432 MB
Current / Peak Usage	0 MB / 0 MB
Utilization	0 %

Physical Address Extension (PAE):

Supported by Operating System	Yes
Supported by CPU	Yes
Active	Yes

SPD

[DIMM1: Kingston 99U5428-018.A00LF]

Memory Module Properties:

Module Name	Kingston 99U5428-018.A00LF
Serial Number	5E290E52h (1376659806)
Manufacture Date	Week 4 / 2015
Module Size	8 GB (2 ranks, 8 banks)
Module Type	SO-DIMM
Memory Type	DDR3 SDRAM
Memory Speed	DDR3-1600 (800 MHz)
Module Width	64 bit
Module Voltage	1.35 V / 1.5 V
Error Detection Method	None
Refresh Rate	Normal (7.8 us)

Memory Timings:

@ 800 MHz	11-11-11-28 (CL-RCD-RP-RAS) / 39-208-5-12-6-6-24 (RC-RFC-RRD-WR-WTR-RTP-FAW)
@ 761 MHz	10-10-10-27 (CL-RCD-RP-RAS) / 37-199-5-12-6-6-23 (RC-RFC-RRD-WR-WTR-RTP-FAW)
@ 685 MHz	9-9-9-24 (CL-RCD-RP-RAS) / 33-179-5-11-6-6-21 (RC-RFC-RRD-WR-WTR-RTP-FAW)
@ 609 MHz	8-8-8-22 (CL-RCD-RP-RAS) / 30-159-4-10-5-5-19 (RC-RFC-RRD-WR-WTR-RTP-FAW)
@ 533 MHz	7-7-7-19 (CL-RCD-RP-RAS) / 26-139-4-8-4-4-16 (RC-RFC-RRD-WR-WTR-RTP-FAW)
@ 457 MHz	6-6-6-16 (CL-RCD-RP-RAS) / 22-119-3-7-4-4-14 (RC-RFC-RRD-WR-WTR-RTP-FAW)
@ 380 MHz	5-5-5-14 (CL-RCD-RP-RAS) / 19-100-3-6-3-3-12 (RC-RFC-RRD-WR-WTR-RTP-FAW)

Memory Module Features:

Auto Self Refresh (ASR)	Not Supported
DLL-Off Mode	Supported
Extended Temperature Range	Supported
Extended Temperature 1X Refresh Rate	Not Supported
On-Die Thermal Sensor Readout (ODTS)	Not Supported
Partial Array Self Refresh (PASR)	Supported
RZQ/6	Supported
RZQ/7	Supported

Memory Module Manufacturer:

Company Name	Kingston Technology Corporation
Product Information	http://www.kingston.com/products/default.asp

[DIMM3: Kingston 99U5428-018.A00LF]

Memory Module Properties:

Module Name	Kingston 99U5428-018.A00LF
Serial Number	5F290052h (1375742303)
Manufacture Date	Week 4 / 2015
Module Size	8 GB (2 ranks, 8 banks)
Module Type	SO-DIMM
Memory Type	DDR3 SDRAM
Memory Speed	DDR3-1600 (800 MHz)
Module Width	64 bit
Module Voltage	1.35 V / 1.5 V

Error Detection Method	None
Refresh Rate	Normal (7.8 us)

Memory Timings:

@ 800 MHz	11-11-11-28 (CL-RCD-RP-RAS) / 39-208-5-12-6-6-24 (RC-RFC-RRD-WR-WTR-RTP-FAW)
@ 761 MHz	10-10-10-27 (CL-RCD-RP-RAS) / 37-199-5-12-6-6-23 (RC-RFC-RRD-WR-WTR-RTP-FAW)
@ 685 MHz	9-9-9-24 (CL-RCD-RP-RAS) / 33-179-5-11-6-6-21 (RC-RFC-RRD-WR-WTR-RTP-FAW)
@ 609 MHz	8-8-8-22 (CL-RCD-RP-RAS) / 30-159-4-10-5-5-19 (RC-RFC-RRD-WR-WTR-RTP-FAW)
@ 533 MHz	7-7-7-19 (CL-RCD-RP-RAS) / 26-139-4-8-4-4-16 (RC-RFC-RRD-WR-WTR-RTP-FAW)
@ 457 MHz	6-6-6-16 (CL-RCD-RP-RAS) / 22-119-3-7-4-4-14 (RC-RFC-RRD-WR-WTR-RTP-FAW)
@ 380 MHz	5-5-5-14 (CL-RCD-RP-RAS) / 19-100-3-6-3-3-12 (RC-RFC-RRD-WR-WTR-RTP-FAW)

Memory Module Features:

Auto Self Refresh (ASR)	Not Supported
DLL-Off Mode	Supported
Extended Temperature Range	Supported
Extended Temperature 1X Refresh Rate	Not Supported
On-Die Thermal Sensor Readout (ODTS)	Not Supported
Partial Array Self Refresh (PASR)	Supported
RZQ/6	Supported
RZQ/7	Supported

Memory Module Manufacturer:

Company Name	Kingston Technology Corporation
Product Information	http://www.kingston.com/products/default.asp

Chipset

[North Bridge: Intel Ivy Bridge-MB IMC]

North Bridge Properties:

North Bridge	Intel Ivy Bridge-MB IMC
Intel Platform	Chief River
Supported Memory Types	DDR3-1066, DDR3-1333, DDR3-1600, DDR3-1866 SDRAM
Maximum Memory Amount	16 GB
Revision	09
Process Technology	22 nm
VT-d	Supported
Extended APIC (x2APIC)	Supported

Memory Controller:

Type	Dual Channel (128-bit)
Active Mode	Dual Channel (128-bit)

Memory Timings:

CAS Latency (CL)	11T
RAS To CAS Delay (tRCD)	11T
RAS Precharge (tRP)	11T
RAS Active Time (tRAS)	28T
Row Refresh Cycle Time (tRFC)	208T
Command Rate (CR)	1T

RAS To RAS Delay (tRRD)	5T
Write Recovery Time (tWR)	12T
Read To Read Delay (tRTR)	Same Rank: 4T, Different Rank: 1T, Different DIMM: 3T
Read To Write Delay (tRTW)	Same Rank: 3T, Different Rank: 5T, Different DIMM: 5T
Write To Read Delay (tWTR)	6T, Different Rank: 1T, Different DIMM: 1T
Write To Write Delay (tWTW)	Same Rank: 4T, Different Rank: 3T, Different DIMM: 3T
Read To Precharge Delay (tRTP)	6T
Four Activate Window Delay (tFAW)	24T
Write CAS Latency (tWCL)	8T
CKE Min. Pulse Width (tCKE)	4T
Refresh Period (tREF)	6240T
Round Trip Latency (tRTL)	DIMM1: 39T, DIMM2: 32T, DIMM3: 40T, DIMM4: 32T
I/O Latency (tIOL)	DIMM2: 0T, DIMM3: 3T, DIMM4: 0T
Burst Length (BL)	8

Error Correction:

ECC	Not Supported
ChipKill ECC	Not Supported
RAID	Not Supported
ECC Scrubbing	Not Supported

Memory Slots:

DRAM Slot #1	8 GB (DDR3-1600 DDR3 SDRAM)
DRAM Slot #2	8 GB (DDR3-1600 DDR3 SDRAM)

Integrated Graphics Controller:

Graphics Controller Type	Intel HD Graphics 4000
Graphics Controller Status	Enabled
Graphics Frame Buffer Size	64 MB

Chipset Manufacturer:

Company Name	Intel Corporation
Product Information	http://www.intel.com/products/chipsets
Driver Download	http://support.intel.com/support/chipsets
BIOS Upgrades	http://www.aida64.com/bios-updates
Driver Update	http://www.aida64.com/driver-updates

[South Bridge: Intel Panther Point HM70]

South Bridge Properties:

South Bridge	Intel Panther Point HM70
Intel Platform	Chief River
Revision / Stepping	04 / C1
Package Type	989 Pin FC-BGA
Package Size	25 mm x 25 mm
Process Technology	65 nm
Die Size	100.73 mm2
Core Voltage	1.05 V
TDP	4.1 W

High Definition Audio:

Codec Name	Realtek ALC269
Codec ID	10EC0269h / 10250649h
Codec Revision	1001h

Codec Type	Audio

High Definition Audio:

Codec Name	Intel Panther Point HDMI
Codec ID	80862806h / 80860101h
Codec Revision	1000h
Codec Type	Audio

PCI Express Controller:

PCI-E 2.0 x1 port #1	In Use @ x1 (Broadcom NetLink BCM57785 PCI-E Gigabit Ethernet Controller, Broadcom SD Card Reader)
PCI-E 2.0 x1 port #2	In Use @ x1 (Intel Dual Band Wireless-AC 7260 AC 2x2 HMC WiFi Adapter)

Chipset Manufacturer:

Company Name	Intel Corporation
Product Information	http://www.intel.com/products/chipsets
Driver Download	http://support.intel.com/support/chipsets
BIOS Upgrades	http://www.aida64.com/bios-updates
Driver Update	http://www.aida64.com/driver-updates

BIOS

BIOS Properties:

BIOS Type	Insyde EFI
BIOS Version	V2.21
System BIOS Date	12/16/2013
Video BIOS Date	03/14/12

BIOS Manufacturer:

Company Name	Insyde Software Corp.
Product Information	http://www.insydesw.com/products
BIOS Upgrades	http://www.aida64.com/bios-updates

ACPI

[APIC: Multiple APIC Description Table]

ACPI Table Properties:

ACPI Signature	APIC
Table Description	Multiple APIC Description Table
Memory Address	AAFF9000h
Table Length	140 bytes
OEM ID	ACRSYS
OEM Table ID	ACRPRDCT
OEM Revision	00000001h
Creator ID	1025
Creator Revision	00040000h
Local APIC Address	FEE00000h

Processor Local APIC:

ACPI Processor ID	01h
APIC ID	00h
Status	Enabled

Processor Local APIC:

ACPI Processor ID	02h
APIC ID	01h
Status	Enabled

Processor Local APIC:

ACPI Processor ID	03h
APIC ID	02h
Status	Enabled

Processor Local APIC:

ACPI Processor ID	04h
APIC ID	03h
Status	Enabled

Processor Local APIC:

ACPI Processor ID	05h
APIC ID	00h
Status	Disabled

Processor Local APIC:

ACPI Processor ID	06h
APIC ID	00h
Status	Disabled

Processor Local APIC:

ACPI Processor ID	07h
APIC ID	00h
Status	Disabled

Processor Local APIC:

ACPI Processor ID	08h
APIC ID	00h
Status	Disabled

I/O APIC:

I/O APIC ID	00h
I/O APIC Address	FEC00000h
Global System Interrupt Base	00000000h

Interrupt Source Override:

Bus	ISA
Source	IRQ0
Global System Interrupt	00000002h
Polarity	Conforms to the specifications of the bus
Trigger Mode	Conforms to the specifications of the bus

Interrupt Source Override:

Bus	ISA
Source	IRQ9

Global System Interrupt	00000009h
Polarity	Active High
Trigger Mode	Level-Triggered

[ASF!: Alert Standard Format Table]

ACPI Table Properties:

ACPI Signature	ASF!
Table Description	Alert Standard Format Table
Memory Address	AAFFC000h
Table Length	165 bytes
OEM ID	ACRSYS
OEM Table ID	ACRPRDCT
OEM Revision	00000001h
Creator ID	1025
Creator Revision	00040000h

ASF_INFO:

Min Watchdog Reset Value	5 sec
Min ASF Sensor Interpoll Wait Time	1275 msec
System ID	0001h
IANA Manufacturer ID	00-00-01-57h

ASF_ALRT:

Numer of Alerts	3
Array Element Length	12

ASF_RCTL:

Numer of Controls	4
Array Element Length	4

ASF_RMCP:

Remote Control Capabilities	20-F8-00-00-00-13-F0h
RMCP Boot Options Completion Code	00h (Successful)
RMCP IANA Enterprise ID	00-00-00-00h
RMCP Special Command	00h
RMCP Special Command Parameter	0000h
RMCP Boot Options	0000h
RMCP OEM Parameters	0000h

[ASPT: ACPI System Performance Tuning Table]

ACPI Table Properties:

ACPI Signature	ASPT
Table Description	ACPI System Performance Tuning Table
Memory Address	AAFE3000h
Table Length	52 bytes
OEM ID	ACRSYS
OEM Table ID	ACRPRDCT
OEM Revision	00000001h
Creator ID	1025
Creator Revision	00040000h
SPTT Address	00000000-00000000h
AMRT Address	00000000-00000000h

[BOOT: Simple Boot Flag Table]

ACPI Table Properties:

ACPI Signature	BOOT
Table Description	Simple Boot Flag Table
Memory Address	AAFE8000h
Table Length	40 bytes
OEM ID	ACRSYS
OEM Table ID	ACRPRDCT
OEM Revision	00000001h
Creator ID	1025
Creator Revision	00040000h

[DBGP: Debug Port Table]

ACPI Table Properties:

ACPI Signature	DBGP
Table Description	Debug Port Table
Memory Address	AAFE2000h
Table Length	52 bytes
OEM ID	ACRSYS
OEM Table ID	ACRPRDCT
OEM Revision	00000001h
Creator ID	1025
Creator Revision	00040000h

[DMAR: DMA Remapping Table]

ACPI Table Properties:

ACPI Signature	DMAR
Table Description	DMA Remapping Table
Memory Address	AAFDC000h
Table Length	176 bytes
OEM ID	ACRSYS
OEM Table ID	ACRPRDCT
OEM Revision	00000001h
Creator ID	1025
Creator Revision	00040000h

[DSDT: Differentiated System Description Table]

ACPI Table Properties:

ACPI Signature	DSDT
Table Description	Differentiated System Description Table
Memory Address	00000000-AAFEC000h
Table Length	48130 bytes
OEM ID	ACRSYS
OEM Table ID	ACRPRDCT
OEM Revision	00000000h
Creator ID	1025
Creator Revision	00040000h

nVIDIA SLI:

SLI Certification	Not Present
PCI 0-0-0-0 (Direct I/O)	8086-0154 (Intel)
PCI 0-0-0-0 (HAL)	8086-0154 (Intel)

Lucid Virtu:

Virtu Certification	Not Present

[FACP: Fixed ACPI Description Table]

ACPI Table Properties:

ACPI Signature	FACP
Table Description	Fixed ACPI Description Table
Memory Address	AAFFB000h
Table Length	268 bytes
OEM ID	ACRSYS
OEM Table ID	ACRPRDCT
OEM Revision	00000001h
Creator ID	1025
Creator Revision	00040000h
FACS Address	AAFBA000h / 00000000-00000000h
DSDT Address	AAFEC000h / 00000000-AAFEC000h
SMI Command Port	000000B2h
PM Timer	00000408h

[FACS: Firmware ACPI Control Structure]

ACPI Table Properties:

ACPI Signature	FACS
Table Description	Firmware ACPI Control Structure
Memory Address	AAFBA000h
Table Length	64 bytes
Hardware Signature	00000000h
Waking Vector	00000000h
Global Lock	00000000h

[FBPT: Firmware Basic Boot Performance Table]

ACPI Table Properties:

ACPI Signature	FBPT
Table Description	Firmware Basic Boot Performance Table
Memory Address	00000000-AAFE1F98h
Table Length	56 bytes

[FPDT: Firmware Performance Data Table]

ACPI Table Properties:

ACPI Signature	FPDT
Table Description	Firmware Performance Data Table
Memory Address	AAFE0000h
Table Length	68 bytes
OEM ID	ACRSYS
OEM Table ID	ACRPRDCT

OEM Revision	00000001h
Creator ID	1025
Creator Revision	00040000h
FBPT Address	00000000-AAFE1F98h
S3PT Address	00000000-AAFE1F18h

[HPET: IA-PC High Precision Event Timer Table]

ACPI Table Properties:

ACPI Signature	HPET
Table Description	IA-PC High Precision Event Timer Table
Memory Address	AAFFA000h
Table Length	56 bytes
OEM ID	ACRSYS
OEM Table ID	ACRPRDCT
OEM Revision	00000001h
Creator ID	1025
Creator Revision	00040000h
HPET Address	00000000-FED00000h
Vendor ID	8086h
Revision ID	01h
Number of Timers	3
Counter Size	64-bit
Minimum Clock Ticks	128
Page Protection	No Guarantee
OEM Attribute	0h
LegacyReplacement IRQ Routing	Supported

[MCFG: Memory Mapped Configuration Space Base Address Description Table]

ACPI Table Properties:

ACPI Signature	MCFG
Table Description	Memory Mapped Configuration Space Base Address Description Table
Memory Address	AAFF8000h
Table Length	60 bytes
OEM ID	ACRSYS
OEM Table ID	ACRPRDCT
OEM Revision	00000001h
Creator ID	1025
Creator Revision	00040000h
Config Space Address	00000000-F0000000h
PCI Segment	0000h
Start Bus Number	00h
End Bus Number	3Fh

[RSD PTR: Root System Description Pointer]

ACPI Table Properties:

ACPI Signature	RSD PTR
Table Description	Root System Description Pointer
Memory Address	000FE020h
Table Length	36 bytes
OEM ID	ACRSYS

RSDP Revision	2 (ACPI 2.0+)
RSDT Address	AAFFE124h
XSDT Address	00000000-AAFFE210h

[RSDT: Root System Description Table]

ACPI Table Properties:

ACPI Signature	RSDT
Table Description	Root System Description Table
Memory Address	AAFFE124h
Table Length	96 bytes
OEM ID	ACRSYS
OEM Table ID	ACRPRDCT
OEM Revision	00000001h
Creator Revision	01000013h
RSDT Entry #0	AAFFB000h (FACP)
RSDT Entry #1	AAFFD000h (UEFI)
RSDT Entry #2	AAFFC000h (ASF!)
RSDT Entry #3	AAFFA000h (HPET)
RSDT Entry #4	AAFF9000h (APIC)
RSDT Entry #5	AAFF8000h (MCFG)
RSDT Entry #6	AAFEB000h (SLIC)
RSDT Entry #7	AAFEA000h (SSDT)
RSDT Entry #8	AAFE8000h (BOOT)
RSDT Entry #9	AAFE3000h (ASPT)
RSDT Entry #10	AAFE2000h (DBGP)
RSDT Entry #11	AAFE0000h (FPDT)
RSDT Entry #12	AAFDE000h (SSDT)
RSDT Entry #13	AAFDD000h (SSDT)
RSDT Entry #14	AAFDC000h (DMAR)

[S3PT: S3 Performance Table]

ACPI Table Properties:

ACPI Signature	S3PT
Table Description	S3 Performance Table
Memory Address	00000000-AAFE1F18h
Table Length	32 bytes

[SLIC: Software Licensing Description Table]

ACPI Table Properties:

ACPI Signature	SLIC
Table Description	Software Licensing Description Table
Memory Address	AAFEB000h
Table Length	374 bytes
OEM ID	ACRSYS
OEM Table ID	ACRPRDCT
OEM Revision	00000001h
Creator ID	1025
Creator Revision	00040000h
SLIC Version	v2.1

OEM Public Key:

Key Type	06h
Version	02h
Algorithm	00002400h
Magic	RSA1
Bit Length	1024
Exponent	65537

SLIC Marker:

Version	00020001h
OEM ID	ACRSYS
OEM Table ID	ACRPRDCT
Windows Flag	WINDOWS

[SSDT: Secondary System Description Table]

ACPI Table Properties:

ACPI Signature	SSDT
Table Description	Secondary System Description Table
Memory Address	AAFDD000h
Table Length	2706 bytes
OEM ID	ACRSYS
OEM Table ID	ACRPRDCT
OEM Revision	00003000h
Creator ID	1025
Creator Revision	00040000h

[SSDT: Secondary System Description Table]

ACPI Table Properties:

ACPI Signature	SSDT
Table Description	Secondary System Description Table
Memory Address	AAFDE000h
Table Length	2474 bytes
OEM ID	ACRSYS
OEM Table ID	ACRPRDCT
OEM Revision	00003000h
Creator ID	1025
Creator Revision	00040000h

[SSDT: Secondary System Description Table]

ACPI Table Properties:

ACPI Signature	SSDT
Table Description	Secondary System Description Table
Memory Address	AAFEA000h
Table Length	1790 bytes
OEM ID	ACRSYS
OEM Table ID	ACRPRDCT
OEM Revision	00001000h
Creator ID	1025
Creator Revision	00040000h

[UEFI: UEFI ACPI Boot Optimization Table]

ACPI Table Properties:

ACPI Signature	UEFI
Table Description	UEFI ACPI Boot Optimization Table
Memory Address	AAFFD000h
Table Length	566 bytes
OEM ID	ACRSYS
OEM Table ID	ACRPRDCT
OEM Revision	00000001h
Creator ID	1025
Creator Revision	00040000h

[XSDT: Extended System Description Table]

ACPI Table Properties:

ACPI Signature	XSDT
Table Description	Extended System Description Table
Memory Address	00000000-AAFFE210h
Table Length	156 bytes
OEM ID	ACRSYS
OEM Table ID	ACRPRDCT
OEM Revision	00000001h
Creator Revision	01000013h
XSDT Entry #0	00000000-AAFFB000h (FACP)
XSDT Entry #1	00000000-AAFFD000h (UEFI)
XSDT Entry #2	00000000-AAFFC000h (ASF!)
XSDT Entry #3	00000000-AAFFA000h (HPET)
XSDT Entry #4	00000000-AAFF9000h (APIC)
XSDT Entry #5	00000000-AAFF8000h (MCFG)
XSDT Entry #6	00000000-AAFEB000h (SLIC)
XSDT Entry #7	00000000-AAFEA000h (SSDT)
XSDT Entry #8	00000000-AAFE8000h (BOOT)
XSDT Entry #9	00000000-AAFE3000h (ASPT)
XSDT Entry #10	00000000-AAFE2000h (DBGP)
XSDT Entry #11	00000000-AAFE0000h (FPDT)
XSDT Entry #12	00000000-AAFDE000h (SSDT)
XSDT Entry #13	00000000-AAFDD000h (SSDT)
XSDT Entry #14	00000000-AAFDC000h (DMAR)

Operating System

Operating System Properties:

OS Name	Microsoft Windows 8.1 Professional
OS Language	English (United States)
OS Installer Language	English (United States)
OS Kernel Type	Multiprocessor Free (64-bit)
OS Version	6.3.9600.17736 (Win8.1 RTM)
OS Service Pack	-
OS Installation Date	4/10/2015
OS Root	C:\Windows

License Information:

Registered Owner	Liem
Registered Organization	
Product ID	00260-00358-16728-AA747
Product Key	
Product Activation (WPA)	Required

Current Session:

Computer Name	LTRANPHD
User Name	Liem
Logon Domain	LTRANPHD
UpTime	261 sec (0 days, 0 hours, 4 min, 21 sec)

Components Version:

Common Controls	6.16
Windows Mail	6.3.9600.16384 (winblue_rtm.130821-1623)
Windows Media Player	12.0.9600.16384 (winblue_rtm.130821-1623)
Windows Messenger	-
MSN Messenger	-
Internet Information Services (IIS)	-
.NET Framework	4.0.30319.33440 built by: FX45W81RTMREL
Novell Client	-
DirectX	DirectX 11.2
OpenGL	6.3.9600.17415 (winblue_r4.141028-1500)
ASPI	-

Operating System Features:

Debug Version	No
DBCS Version	No
Domain Controller	No
Security Present	No
Network Present	Yes
Remote Session	No
Safe Mode	No
Slow Processor	No
Terminal Services	Yes

Processes

Process Name	Process File Name	Type	Used Memory	Used Swap
aida64.exe	B:\Downloads\aida64.exe	32-bit	75256 KB	62 KB
ASCService.exe	C:\Program Files (x86)\IObit\Advanced SystemCare 8\ASCService.exe	32-bit	5292 KB	6 KB
audiodg.exe		64-bit	8572 KB	5 KB
chrome.exe	C:\Program Files (x86)\Google\Chrome\Application\chrome.exe	32-bit	37464 KB	33 KB
chrome.exe	C:\Program Files (x86)\Google\Chrome\Application\chrome.exe	32-bit	109 MB	104 KB
chrome.exe	C:\Program Files (x86)\Google\Chrome\Application\chrome.exe	32-bit	49172 KB	45 KB
chrome.exe	C:\Program Files (x86)\Google\Chrome\Application\chrome.exe	32-bit	79120 KB	68 KB
chrome.exe	C:\Program Files (x86)\Google\Chrome\Application\chrome.exe	32-bit	72516 KB	58 KB
chrome.exe	C:\Program Files (x86)\Google\Chrome\Application\chrome.exe	32-bit	137 MB	123 KB
chrome.exe	C:\Program Files (x86)\Google\Chrome\Application\chrome.exe	32-bit	98 MB	67 KB
chrome.exe	C:\Program Files (x86)\Google\Chrome\Application\chrome.exe	32-bit	38916 KB	23 KB

chrome.exe	C:\Program Files (x86)\Google\Chrome\Application\chrome.exe	32-bit	39672 KB	34 KB
chrome.exe	C:\Program Files (x86)\Google\Chrome\Application\chrome.exe	32-bit	93 MB	86 KB
chrome.exe	C:\Program Files (x86)\Google\Chrome\Application\chrome.exe	32-bit	43276 KB	33 KB
csrss.exe		64-bit	3776 KB	1 KB
csrss.exe		64-bit	21284 KB	2 KB
dasHost.exe	C:\Windows\system32\dashost.exe	64-bit	9548 KB	2 KB
devmonsrv.exe	C:\Program Files (x86)\Intel\Bluetooth\devmonsrv.exe	32-bit	7444 KB	2 KB
dwm.exe	C:\Windows\system32\dwm.exe	32-bit	19408 KB	13 KB
explorer.exe	C:\Windows\Explorer.EXE	64-bit	101 MB	56 KB
igfxCUIService.exe	C:\Windows\system32\igfxCUIService.exe	64-bit	6128 KB	1 KB
igfxEM.exe	C:\Windows\system32\igfxEM.exe	64-bit	13120 KB	6 KB
igfxHK.exe	C:\Windows\system32\igfxHK.exe	64-bit	9776 KB	4 KB
igfxTray.exe	C:\Windows\system32\igfxTray.exe	64-bit	17932 KB	12 KB
InstallServices.exe	C:\Program Files (x86)\IObit\Start Menu 8\InstallServices.exe	64-bit	17544 KB	10 KB
LiveUpdate.exe	C:\Program Files (x86)\IObit\LiveUpdate\LiveUpdate.exe	32-bit	7720 KB	5 KB
lsass.exe	C:\Windows\system32\lsass.exe	64-bit	10048 KB	3 KB
MsMpEng.exe		64-bit	99 MB	103 KB
NisSrv.exe		64-bit	6008 KB	8 KB
obexsrv.exe	C:\Program Files (x86)\Intel\Bluetooth\obexsrv.exe	32-bit	6828 KB	2 KB
ONENOTEM.EXE	C:\Program Files\Microsoft Office\Office15\ONENOTEM.EXE	64-bit	1004 KB	1 KB
PresentationFontCache.exe	C:\Windows\Microsoft.Net\Framework64\v3.0\WPF\PresentationFontCache.exe	64-bit	15840 KB	25 KB
rundll32.exe	C:\Windows\System32\rundll32.exe	64-bit	11732 KB	2 KB
SearchIndexer.exe	C:\Windows\system32\SearchIndexer.exe	64-bit	10200 KB	13 KB
services.exe		64-bit	5868 KB	2 KB
smss.exe		64-bit	1044 KB	0 KB
splwow64.exe	C:\Windows\splwow64.exe	64-bit	4680 KB	1 KB
spoolsv.exe	C:\Windows\System32\spoolsv.exe	64-bit	11640 KB	5 KB
sppsvc.exe		64-bit	14928 KB	6 KB
ss_conn_service.exe	C:\Program Files\SAMSUNG\USB Drivers\25_escape\conn\ss_conn_service.exe	32-bit	4576 KB	1 KB
StartMenu_Hook.exe	C:\Program Files (x86)\IObit\Start Menu 8\StartMenu_Hook.exe	32-bit	8036 KB	5 KB
StartMenu8.exe	C:\Program Files (x86)\IObit\Start Menu 8\StartMenu8.exe	32-bit	32744 KB	23 KB
StartMenuServices.exe	C:\Program Files (x86)\IObit\Start Menu 8\StartMenuServices.exe	32-bit	7188 KB	5 KB
svchost.exe	C:\Windows\system32\svchost.exe	64-bit	19676 KB	13 KB
svchost.exe	C:\Windows\System32\svchost.exe	64-bit	10372 KB	3 KB
svchost.exe	C:\Windows\system32\svchost.exe	64-bit	6272 KB	1 KB
svchost.exe	C:\Windows\system32\svchost.exe	64-bit	13288 KB	5 KB
svchost.exe	C:\Windows\system32\svchost.exe	64-bit	4592 KB	1 KB
svchost.exe	C:\Windows\System32\svchost.exe	64-bit	22624 KB	9 KB
svchost.exe	C:\Windows\system32\svchost.exe	64-bit	13864 KB	6 KB
svchost.exe	C:\Windows\system32\svchost.exe	64-bit	10224 KB	4 KB
svchost.exe	C:\Windows\system32\svchost.exe	64-bit	6280 KB	2 KB
svchost.exe	C:\Windows\System32\svchost.exe	64-bit	25360 KB	17 KB
svchost.exe	C:\Windows\system32\svchost.exe	64-bit	27976 KB	14 KB
svchost.exe	C:\Windows\system32\svchost.exe	64-bit	18336 KB	7 KB
System Idle Process			4 KB	0 KB
System		64-bit	2044 KB	0 KB
taskhostex.exe	C:\Windows\system32\taskhostex.exe	64-bit	9676 KB	3 KB
wininit.exe	C:\Windows\system32\wininit.exe	64-bit	3760 KB	0 KB
winlogon.exe	C:\Windows\system32\winlogon.exe	64-bit	8120 KB	1 KB
WMIADAP.exe	\\?\C:\Windows\system32\wbem\WMIADAP.EXE	64-bit	5232 KB	1 KB
WmiPrvSE.exe	C:\Windows\sysWOW64\wbem\wmiprvse.exe	64-bit	6880 KB	2 KB
WmiPrvSE.exe	C:\Windows\system32\wbem\wmiprvse.exe	64-bit	5444 KB	1 KB
WmiPrvSE.exe	C:\Windows\system32\wbem\wmiprvse.exe	64-bit	8292 KB	3 KB

System Drivers

Driver Name	Driver Description	File Name	Version	Type	State
1394ohci	1394 OHCI Compliant Host Controller	1394ohci.sys	6.3.9600.16384	Kernel Driver	Stopped
3ware	3ware	3ware.sys	5.1.0.51	Kernel Driver	Stopped
ACPI	Microsoft ACPI Driver	ACPI.sys	6.3.9600.17393	Kernel Driver	Running
acpiex	Microsoft ACPIEx Driver	acpiex.sys	6.3.9600.16384	Kernel Driver	Running
acpipagr	ACPI Processor Aggregator Driver	acpipagr.sys	6.3.9600.16384	Kernel Driver	Stopped
AcpiPmi	ACPI Power Meter Driver	acpipmi.sys	6.3.9600.16384	Kernel Driver	Stopped
acpitime	ACPI Wake Alarm Driver	acpitime.sys	6.3.9600.16384	Kernel Driver	Stopped
ADP80XX	ADP80XX	ADP80XX.SYS	1.0.0.254	Kernel Driver	Stopped
AFD	Ancillary Function Driver for Winsock	afd.sys	6.3.9600.17194	Kernel Driver	Running
agp440	Intel AGP Bus Filter	agp440.sys	6.3.9600.16384	Kernel Driver	Stopped
ahcache	Application Compatibility Cache	ahcache.sys	6.3.9600.17555	Kernel Driver	Running
AIDA64Driver	FinalWire AIDA64 Kernel Driver	kerneld.x64		Kernel Driver	Running
AmdK8	AMD K8 Processor Driver	amdk8.sys	6.3.9600.16384	Kernel Driver	Stopped
AmdPPM	AMD Processor Driver	amdppm.sys	6.3.9600.16384	Kernel Driver	Stopped
amdsata	amdsata	amdsata.sys	1.1.4.14	Kernel Driver	Stopped
amdsbs	amdsbs	amdsbs.sys	3.7.1540.43	Kernel Driver	Stopped
amdxata	amdxata	amdxata.sys	1.1.4.14	Kernel Driver	Stopped
ApfiltrService	Alps Pointing-device Filter Driver	Apfiltr.sys		Kernel Driver	Stopped
AppID	AppID Driver	appid.sys	6.3.9600.17415	Kernel Driver	Stopped
arcsas	Adaptec SAS/SATA-II RAID Storport's Miniport Driver	arcsas.sys	7.2.0.30261	Kernel Driver	Stopped
atapi	IDE Channel	atapi.sys	6.3.9600.16384	Kernel Driver	Stopped
athr	Qualcomm Atheros Extensible Wireless LAN device driver	athwbx.sys	10.0.0.276	Kernel Driver	Stopped
b06bdrv	Broadcom NetXtreme II VBD	bxvbda.sys	7.4.14.0	Kernel Driver	Stopped
BasicDisplay	BasicDisplay	BasicDisplay.sys	6.3.9600.16384	Kernel Driver	Running
BasicRender	BasicRender	BasicRender.sys	6.3.9600.17031	Kernel Driver	Running
bcmfn2	bcmfn2 Service	bcmfn2.sys	6.3.9391.6	Kernel Driver	Stopped
Beep	Beep			Kernel Driver	Running

bowser	Browser Support Driver	bowser.sys	6.3.9600.16384	File System Driver	Running
bScsiMSa	bScsiMSa	bScsiMSa.sys	1.0.8.0	Kernel Driver	Running
bScsiSDa	bScsiSDa	bScsiSDa.sys	1.0.0.254	Kernel Driver	Running
BthA2DP	Bluetooth Stereo	BthA2DP.sys	6.3.9600.17670	Kernel Driver	Running
BthAvrcpTg	Bluetooth Audio/Video Remote Control HID	BthAvrcpTg.sys	6.3.9600.16384	Kernel Driver	Running
BthEnum	Bluetooth Enumerator Service	BthEnum.sys	6.3.9600.17415	Kernel Driver	Running
BthHFEnum	Bluetooth Hands-Free Audio and Call Control HID Enumerator	bthhfenum.sys	6.3.9600.17723	Kernel Driver	Stopped
bthhfhid	Bluetooth Hands-Free Call Control HID	BthHFHid.sys	6.3.9600.16384	Kernel Driver	Stopped
BTHMODEM	Bluetooth Serial Communications Driver	bthmodem.sys	6.3.9600.16520	Kernel Driver	Stopped
BthPan	Bluetooth Device (Personal Area Network)	bthpan.sys	6.3.9600.17238	Kernel Driver	Running
BTHPORT	Bluetooth Port Driver	BTHport.sys	6.3.9600.17415	Kernel Driver	Stopped
BTHUSB	Bluetooth Radio USB Driver	BTHUSB.sys	6.3.9600.17415	Kernel Driver	Running
btmaux	Intel Bluetooth Auxiliary Service	btmaux.sys	17.1.1501.510	Kernel Driver	Running
cdfs	CD/DVD File System Reader	cdfs.sys	6.3.9600.16384	File System Driver	Stopped
cdrom	CD-ROM Driver	cdrom.sys	6.3.9600.16384	Kernel Driver	Running
circlass	Consumer IR Devices	circlass.sys	6.3.9600.16384	Kernel Driver	Stopped
CLFS	Common Log (CLFS)	CLFS.sys	6.3.9600.17719	Kernel Driver	Running
CmBatt	Microsoft ACPI Control Method Battery Driver	CmBatt.sys	6.3.9600.16384	Kernel Driver	Running
CNG	CNG	cng.sys	6.3.9600.17633	Kernel Driver	Running
CompositeBus	Composite Bus Enumerator Driver	CompositeBus.sys	6.3.9600.16384	Kernel Driver	Running
condrv	Console Driver	condrv.sys	6.3.9600.16384	Kernel Driver	Running
CSC	Offline Files Driver	csc.sys	6.3.9600.17415	Kernel Driver	Running
dam	Desktop Activity Moderator Driver	dam.sys	6.3.9600.17480	Kernel Driver	Stopped
Dfsc	DFS Namespace Client Driver	dfsc.sys	6.3.9600.17041	File System Driver	Running
dg_ssudbus	SAMSUNG Mobile USB Composite Device Driver (DEVGURU Ver.)	ssudbus.sys	2.11.10.0	Kernel Driver	Stopped
DIRECTIO	DIRECTIO	DirectIo64.sys		Kernel Driver	Stopped
disk	Disk Driver	disk.sys	6.3.9600.16384	Kernel Driver	Running
dmvsc	dmvsc	dmvsc.sys	6.3.9600.16384	Kernel Driver	Stopped
drmkaud	Microsoft Trusted Audio Drivers	drmkaud.sys	6.3.9600.17415	Kernel Driver	Stopped

DXGKrnl	LDDM Graphics Subsystem	dxgkrnl.sys	6.3.9600.17415	Kernel Driver	Running
ebdrv	Broadcom NetXtreme II 10 GigE VBD	evbda.sys	7.4.33.1	Kernel Driver	Stopped
EhStorClass	Enhanced Storage Filter Driver	EhStorClass.sys	6.3.9600.16384	Kernel Driver	Running
EhStorTcgDrv	Microsoft driver for storage devices supporting IEEE 1667 and TCG protocols	EhStorTcgDrv.sys	6.3.9600.16384	Kernel Driver	Stopped
ErrDev	Microsoft Hardware Error Device Driver	errdev.sys	6.3.9600.16384	Kernel Driver	Stopped
ETD	ELAN PS/2 Port Input Device	ETD.sys	11.116.0.0	Kernel Driver	Stopped
exfat	exFAT File System Driver			File System Driver	Stopped
fastfat	FAT12/16/32 File System Driver			File System Driver	Stopped
fdc	Floppy Disk Controller Driver	fdc.sys	6.3.9600.16384	Kernel Driver	Stopped
FileInfo	File Information FS MiniFilter	fileinfo.sys	6.3.9600.17031	File System Driver	Running
Filetrace	Filetrace	filetrace.sys	6.3.9600.16384	File System Driver	Stopped
flpydisk	Floppy Disk Driver	flpydisk.sys	6.3.9600.16384	Kernel Driver	Stopped
FltMgr	FltMgr	fltmgr.sys	6.3.9600.17326	File System Driver	Running
FsDepends	File System Dependency Minifilter	FsDepends.sys	6.3.9600.17396	File System Driver	Stopped
fvevol	BitLocker Drive Encryption Filter Driver	fvevol.sys	6.3.9600.17091	Kernel Driver	Running
FxPPM	Power Framework Processor Driver	fxppm.sys	6.3.9600.16384	Kernel Driver	Stopped
gagp30kx	Microsoft Generic AGPv3.0 Filter for K8 Processor Platforms	gagp30kx.sys	6.3.9600.16384	Kernel Driver	Stopped
gencounter	Microsoft Hyper-V Generation Counter	vmgencounter.sys	6.3.9600.16384	Kernel Driver	Stopped
GPIOClx0101	Microsoft GPIO Class Extension Driver	msgpioclx.sys	6.3.9600.17253	Kernel Driver	Stopped
GUBootStartup	GUBootStartup	GUBootStartup.sys	1.1.0.261	Kernel Driver	Running
HdAudAddService	Microsoft 1.1 UAA Function Driver for High Definition Audio Service	HdAudio.sys	6.3.9600.16384	Kernel Driver	Running
HDAudBus	Microsoft UAA Bus Driver for High Definition Audio	HDAudBus.sys	6.3.9600.17238	Kernel Driver	Running
HidBatt	HID UPS Battery Driver	HidBatt.sys	6.3.9600.16384	Kernel Driver	Stopped
HidBth	Microsoft Bluetooth HID Miniport	hidbth.sys	6.3.9600.17670	Kernel Driver	Stopped
hidi2c	Microsoft I2C HID Miniport Driver	hidi2c.sys	6.3.9600.16384	Kernel Driver	Stopped
HidIr	Microsoft Infrared HID Driver	hidir.sys	6.3.9600.16384	Kernel Driver	Stopped
HidUsb	Microsoft HID Class Driver	hidusb.sys	6.3.9600.17041	Kernel Driver	Running
				Kernel	

HpSAMD	HpSAMD	HpSAMD.sys	8.0.4.0	Kernel Driver	Stopped
HTTP	HTTP Service	HTTP.sys	6.3.9600.17712	Kernel Driver	Running
HWiNFO32	HWiNFO32/64 Kernel Driver	HWiNFO64A.SYS		Kernel Driver	Stopped
hwpolicy	Hardware Policy Driver	hwpolicy.sys	6.3.9600.16384	Kernel Driver	Stopped
hyperkbd	hyperkbd	hyperkbd.sys	6.3.9600.16384	Kernel Driver	Stopped
HyperVideo	HyperVideo	HyperVideo.sys	6.3.9600.16384	Kernel Driver	Stopped
i8042prt	PS/2 Keyboard and Mouse Port Driver	i8042prt.sys	6.3.9600.17480	Kernel Driver	Running
iaLPSSi_GPIO	Intel(R) Serial IO GPIO Controller Driver	iaLPSSi_GPIO.sys	1.1.163.0	Kernel Driver	Stopped
iaLPSSi_I2C	Intel(R) Serial IO I2C Controller Driver	iaLPSSi_I2C.sys	1.1.163.0	Kernel Driver	Stopped
iaStorAV	Intel(R) SATA RAID Controller Windows	iaStorAV.sys	12.0.1.1018	Kernel Driver	Stopped
iaStorV	Intel RAID Controller Windows 7	iaStorV.sys	8.6.2.1019	Kernel Driver	Stopped
igfx	igfx	igdkmd64.sys	10.18.10.3958	Kernel Driver	Running
intaud_WaveExtensible	Intel WiDi Audio Device	intelaud.sys	4.5.52.0	Kernel Driver	Stopped
intelide	intelide	intelide.sys	6.3.9600.16384	Kernel Driver	Stopped
intelpep	Intel(R) Power Engine Plug-in Driver	intelpep.sys	6.3.9600.17254	Kernel Driver	Running
intelppm	Intel Processor Driver	intelppm.sys	6.3.9600.16384	Kernel Driver	Running
IpFilterDriver	IP Traffic Filter Driver	ipfltdrv.sys	6.3.9600.16384	Kernel Driver	Stopped
IPMIDRV	IPMIDRV	IPMIDrv.sys	6.3.9600.17238	Kernel Driver	Stopped
IPNAT	IP Network Address Translator	ipnat.sys	6.3.9600.16477	Kernel Driver	Stopped
IRENUM	IR Bus Enumerator	irenum.sys	6.3.9600.16384	Kernel Driver	Stopped
isapnp	isapnp	isapnp.sys	6.3.9600.16384	Kernel Driver	Stopped
iScsiPrt	iScsiPort Driver	msiscsi.sys	6.3.9600.17090	Kernel Driver	Stopped
iwdbus	IWD Bus Enumerator	iwdbus.sys	4.5.52.0	Kernel Driver	Running
k57nd60a	Broadcom NetLink (TM) Gigabit Ethernet - NDIS 6.0	k57nd60a.sys	15.6.0.14	Kernel Driver	Running
kbdclass	Keyboard Class Driver	kbdclass.sys	6.3.9600.17480	Kernel Driver	Running
kbdhid	Keyboard HID Driver	kbdhid.sys	6.3.9600.17480	Kernel Driver	Stopped
kbldfltr	kbldfltr	kbldfltr.sys	6.3.9600.16384	Kernel Driver	Stopped
kdnic	Microsoft Kernel Debug Network Miniport (NDIS 6.20)	kdnic.sys	6.1.0.0	Kernel Driver	Running
KSecDD	KSecDD	ksecdd.sys	6.3.9600.17415	Kernel Driver	Running
KSecPkg	KSecPkg	ksecpkg.sys	6.3.9600.17631	Kernel Driver	Running
				Kernel	

ksthunk	Kernel Streaming Thunks	ksthunk.sys	6.3.9600.16384	Driver	Running
lltdio	Link-Layer Topology Discovery Mapper I/O Driver	lltdio.sys	6.3.9600.16384	Kernel Driver	Running
LSI_SAS	LSI_SAS	lsi_sas.sys	1.34.3.82	Kernel Driver	Stopped
LSI_SAS2	LSI_SAS2	lsi_sas2.sys	2.0.60.82	Kernel Driver	Stopped
LSI_SAS3	LSI_SAS3	lsi_sas3.sys	2.50.65.1	Kernel Driver	Stopped
LSI_SSS	LSI_SSS	lsi_sss.sys	2.10.61.81	Kernel Driver	Stopped
luafv	UAC File Virtualization	luafv.sys	6.3.9600.17031	File System Driver	Running
megasas	megasas	megasas.sys	6.3.9466.0	Kernel Driver	Stopped
megasr	megasr	megasr.sys	15.2.2013.129	Kernel Driver	Stopped
MEIx64	Intel(R) Management Engine Interface	TeeDriverx64.sys	10.0.30.1054	Kernel Driver	Stopped
Modem	Modem	modem.sys	6.3.9600.16384	Kernel Driver	Stopped
monitor	Microsoft Monitor Class Function Driver Service	monitor.sys	6.3.9600.16384	Kernel Driver	Running
mouclass	Mouse Class Driver	mouclass.sys	6.3.9600.17480	Kernel Driver	Running
mouhid	Mouse HID Driver	mouhid.sys	6.3.9600.17480	Kernel Driver	Running
mountmgr	Mount Point Manager	mountmgr.sys	6.3.9600.17393	Kernel Driver	Running
mpsdrv	Windows Firewall Authorization Driver	mpsdrv.sys	6.3.9600.17415	Kernel Driver	Running
MRxDAV	WebDav Client Redirector Driver	mrxdav.sys	6.3.9600.17560	File System Driver	Stopped
mrxsmb	SMB MiniRedirector Wrapper and Engine	mrxsmb.sys	6.3.9600.17396	File System Driver	Running
mrxsmb10	SMB 1.x MiniRedirector	mrxsmb10.sys	6.3.9600.17041	File System Driver	Running
mrxsmb20	SMB 2.0 MiniRedirector	mrxsmb20.sys	6.3.9600.17385	File System Driver	Running
MsBridge	Microsoft MAC Bridge	bridge.sys	6.3.9600.17415	Kernel Driver	Stopped
Msfs	Msfs			File System Driver	Running
msgpiowin32	Common Driver for Buttons, DockMode and Laptop/Slate Indicator	msgpiowin32.sys	6.3.9600.16384	Kernel Driver	Stopped
mshidkmdf	Pass-through HID to KMDF Filter Driver	mshidkmdf.sys	6.3.9600.16384	Kernel Driver	Stopped
mshidumdf	Pass-through HID to UMDF Driver	mshidumdf.sys	6.3.9600.16384	Kernel Driver	Stopped
msisadrv	msisadrv	msisadrv.sys	6.3.9600.16384	Kernel Driver	Running
MSKSSRV	Microsoft Streaming Service Proxy	MSKSSRV.sys	6.3.9600.16384	Kernel Driver	Stopped
MsLldp	Microsoft Link-Layer Discovery Protocol	mslldp.sys	6.3.9600.17415	Kernel	Stopped

				Driver	
MSPCLOCK	Microsoft Streaming Clock Proxy	MSPCLOCK.sys	6.3.9600.16384	Kernel Driver	Stopped
MSPQM	Microsoft Streaming Quality Manager Proxy	MSPQM.sys	6.3.9600.16384	Kernel Driver	Stopped
MsRPC	MsRPC			Kernel Driver	Stopped
mssmbios	Microsoft System Management BIOS Driver	mssmbios.sys	6.3.9600.16384	Kernel Driver	Running
MSTEE	Microsoft Streaming Tee/Sink-to-Sink Converter	MSTEE.sys	6.3.9600.16384	Kernel Driver	Stopped
MTConfig	Microsoft Input Configuration Driver	MTConfig.sys	6.3.9600.16384	Kernel Driver	Stopped
Mup	Mup	mup.sys	6.3.9600.16384	File System Driver	Running
mvumis	mvumis	mvumis.sys	1.0.5.1015	Kernel Driver	Stopped
NativeWifiP	NativeWiFi Filter	nwifi.sys	6.3.9600.17415	Kernel Driver	Running
NDIS	NDIS System Driver	ndis.sys	6.3.9600.17672	Kernel Driver	Running
NdisCap	Microsoft NDIS Capture	ndiscap.sys	6.3.9600.17415	Kernel Driver	Stopped
NdisImPlatform	Microsoft Network Adapter Multiplexor Protocol	NdisImPlatform.sys	6.3.9600.17415	Kernel Driver	Stopped
NdisTapi	Remote Access NDIS TAPI Driver	ndistapi.sys	6.3.9600.17484	Kernel Driver	Stopped
Ndisuio	NDIS Usermode I/O Protocol	ndisuio.sys	6.3.9600.16384	Kernel Driver	Running
NdisVirtualBus	Microsoft Virtual Network Adapter Enumerator	NdisVirtualBus.sys	6.3.9600.16384	Kernel Driver	Running
NdisWan	Remote Access NDIS WAN Driver	ndiswan.sys	6.3.9600.16384	Kernel Driver	Stopped
NdisWanLegacy	Remote Access LEGACY NDIS WAN Driver	ndiswan.sys	6.3.9600.16384	Kernel Driver	Stopped
NDProxy	NDIS Proxy			Kernel Driver	Stopped
Ndu	Windows Network Data Usage Monitoring Driver	Ndu.sys	6.3.9600.17415	Kernel Driver	Running
NetBIOS	NetBIOS Interface	netbios.sys	6.3.9600.17415	File System Driver	Running
NetBT	NetBT	netbt.sys	6.3.9600.16384	Kernel Driver	Running
netvsc	netvsc	netvsc63.sys	6.3.9600.17415	Kernel Driver	Stopped
NETwNb64	@oem57.inf,___ %NIC_Service_DispName_WINB_64%;___ Intel(R) Wireless Adapter Driver for Windows 8.1 - 64 Bit	NETwbw02.sys	16.5.3.6	Kernel Driver	Running
NETwNe64	@netwew02.inf,___ %NIC_Service_DispName_WIN8_64%;___ Intel(R) Wireless WiFi Link 5000 Series Adapter Driver for Windows 8 - 64 Bit	NETwew02.sys	16.0.0.61	Kernel Driver	Stopped
Npfs	Npfs			File System Driver	Running
npsvctrig	Named pipe service trigger provider	npsvctrig.sys	6.3.9600.16384	Kernel Driver	Running
nsiproxy	NSI Proxy Service Driver	nsiproxy.sys	6.3.9600.17415	Kernel Driver	Running
Ntfs	Ntfs			File System Driver	Running

Null	Null			Kernel Driver	Running
nv_agp	NVIDIA nForce AGP Bus Filter	nv_agp.sys	6.3.9600.16384	Kernel Driver	Stopped
nvraid	nvraid	nvraid.sys	10.6.0.22	Kernel Driver	Stopped
nvstor	nvstor	nvstor.sys	10.6.0.22	Kernel Driver	Stopped
Parport	Parallel port driver	parport.sys	6.3.9600.16384	Kernel Driver	Stopped
partmgr	Partition Manager	partmgr.sys	6.3.9600.17396	Kernel Driver	Running
pci	PCI Bus Driver	pci.sys	6.3.9600.17238	Kernel Driver	Running
pciide	pciide	pciide.sys	6.3.9600.16384	Kernel Driver	Stopped
pcmcia	pcmcia	pcmcia.sys	6.3.9600.16384	Kernel Driver	Stopped
pcw	Performance Counters for Windows Driver	pcw.sys	6.3.9600.16384	Kernel Driver	Running
pdc	pdc	pdc.sys	6.3.9600.17254	Kernel Driver	Running
PEAUTH	PEAUTH	peauth.sys	6.3.9600.17031	Kernel Driver	Running
Processor	Processor Driver	processr.sys	6.3.9600.16384	Kernel Driver	Stopped
Psched	QoS Packet Scheduler	pacer.sys	6.3.9600.17415	Kernel Driver	Running
QWAVEdrv	QWAVE driver	qwavedrv.sys	6.3.9600.17415	Kernel Driver	Stopped
RasAcd	Remote Access Auto Connection Driver	rasacd.sys	6.3.9600.17415	Kernel Driver	Stopped
RasPppoe	Remote Access PPPOE Driver	raspppoe.sys	6.3.9600.16384	Kernel Driver	Stopped
rdbss	Redirected Buffering Sub System	rdbss.sys	6.3.9600.16493	File System Driver	Running
rdpbus	Remote Desktop Device Redirector Bus Driver	rdpbus.sys	6.3.9600.16384	Kernel Driver	Running
RDPDR	Remote Desktop Device Redirector Driver	rdpdr.sys	6.3.9600.16384	Kernel Driver	Stopped
RdpVideoMiniport	Remote Desktop Video Miniport Driver	rdpvideominiport.sys	6.3.9600.17415	Kernel Driver	Stopped
rdyboost	ReadyBoost	rdyboost.sys	6.3.9600.17031	Kernel Driver	Running
ReFS	ReFS			File System Driver	Stopped
RFCOMM	Bluetooth Device (RFCOMM Protocol TDI)	rfcomm.sys	6.3.9600.17670	Kernel Driver	Running
rspndr	Link-Layer Topology Discovery Responder	rspndr.sys	6.3.9600.16384	Kernel Driver	Running
s3cap	s3cap	vms3cap.sys	6.3.9600.16384	Kernel Driver	Stopped
sbp2port	SBP-2 Transport/Protocol Bus Driver	sbp2port.sys	6.3.9600.16384	Kernel Driver	Stopped
scfilter	Smart card PnP Class Filter Driver	scfilter.sys	6.3.9600.17415	Kernel Driver	Stopped
sdbus	sdbus	sdbus.sys	6.3.9600.17705	Kernel Driver	Stopped

sdstor	SD Storage Port Driver	sdstor.sys	6.3.9600.17031	Kernel Driver	Stopped
secdrv	Security Driver			Kernel Driver	Running
SerCx	Serial UART Support Library	SerCx.sys	6.3.9600.16384	Kernel Driver	Stopped
SerCx2	Serial UART Support Library	SerCx2.sys	6.3.9600.16444	Kernel Driver	Stopped
Serenum	Serenum Filter Driver	serenum.sys	6.3.9600.16384	Kernel Driver	Stopped
Serial	Serial port driver	serial.sys	6.3.9600.16384	Kernel Driver	Stopped
sermouse	Serial Mouse Driver	sermouse.sys	6.3.9600.17480	Kernel Driver	Stopped
sfloppy	High-Capacity Floppy Disk Drive	sfloppy.sys	6.3.9600.16384	Kernel Driver	Stopped
SiSRaid2	SiSRaid2	SiSRaid2.sys	5.1.1039.2600	Kernel Driver	Stopped
SiSRaid4	SiSRaid4	sisraid4.sys	5.1.1039.3600	Kernel Driver	Stopped
spaceport	Storage Spaces Driver	spaceport.sys	6.3.9600.17415	Kernel Driver	Running
SpbCx	Simple Peripheral Bus Support Library	SpbCx.sys	6.3.9600.16384	Kernel Driver	Stopped
srv	Server SMB 1.xxx Driver	srv.sys	6.3.9600.17238	File System Driver	Running
srv2	Server SMB 2.xxx Driver	srv2.sys	6.3.9600.17396	File System Driver	Running
srvnet	srvnet	srvnet.sys	6.3.9600.17222	File System Driver	Running
ssudmdm	SAMSUNG Mobile USB Modem Drivers (DEVGURU Ver.)	ssudmdm.sys	2.11.10.0	Kernel Driver	Stopped
stexstor	stexstor	stexstor.sys	5.1.0.10	Kernel Driver	Stopped
storahci	Microsoft Standard SATA AHCI Driver	storahci.sys	6.3.9600.16384	Kernel Driver	Running
storflt	Hyper-V Storage Accelerator	vmstorfl.sys	6.3.9600.17415	Kernel Driver	Stopped
stornvme	Microsoft Standard NVM Express Driver	stornvme.sys	6.3.9600.16421	Kernel Driver	Stopped
storvsc	storvsc	storvsc.sys	6.3.9600.16384	Kernel Driver	Stopped
storvsp	storvsp	storvsp.sys	6.3.9600.16384	Kernel Driver	Stopped
swenum	Software Bus Driver	swenum.sys	6.3.9600.17415	Kernel Driver	Running
Tcpip	TCP/IP Protocol Driver	tcpip.sys	6.3.9600.17485	Kernel Driver	Running
TCPIP6	Microsoft IPv6 Protocol Driver	tcpip.sys	6.3.9600.17485	Kernel Driver	Stopped
tcpipreg	TCP/IP Registry Compatibility	tcpipreg.sys	6.3.9600.17041	Kernel Driver	Running
tdx	NetIO Legacy TDI Support Driver	tdx.sys	6.3.9600.16384	Kernel Driver	Running
terminpt	Microsoft Remote Desktop Input Driver	terminpt.sys	6.3.9600.16384	Kernel Driver	Stopped
TPM	TPM	tpm.sys	6.3.9600.16384	Kernel Driver	Stopped

TsUsbFlt	TsUsbFlt	tsusbflt.sys	6.3.9600.16384	Kernel Driver	Stopped
TsUsbGD	Remote Desktop Generic USB Device	TsUsbGD.sys	6.3.9600.17415	Kernel Driver	Stopped
tunnel	Microsoft Tunnel Miniport Adapter Driver	tunnel.sys	6.3.9600.16384	Kernel Driver	Stopped
uagp35	Microsoft AGPv3.5 Filter	uagp35.sys	6.3.9600.16384	Kernel Driver	Stopped
UASPStor	USB Attached SCSI (UAS) Driver	uaspstor.sys	6.3.9600.16384	Kernel Driver	Stopped
UCX01000	USB Controller Extension	ucx01000.sys	6.3.9600.17393	Kernel Driver	Stopped
udfs	udfs	udfs.sys	6.3.9600.17705	File System Driver	Stopped
UEFI	Microsoft UEFI Driver	UEFI.sys	6.3.9600.16384	Kernel Driver	Stopped
uliagpkx	Uli AGP Bus Filter	uliagpkx.sys	6.3.9600.16384	Kernel Driver	Stopped
umbus	UMBus Enumerator Driver	umbus.sys	6.3.9600.16384	Kernel Driver	Running
UmPass	Microsoft UMPass Driver	umpass.sys	6.3.9600.16384	Kernel Driver	Running
usbccgp	Microsoft USB Generic Parent Driver	usbccgp.sys	6.3.9600.17238	Kernel Driver	Running
usbcir	eHome Infrared Receiver (USBCIR)	usbcir.sys	6.3.9600.17415	Kernel Driver	Stopped
usbehci	Microsoft USB 2.0 Enhanced Host Controller Miniport Driver	usbehci.sys	6.3.9600.17195	Kernel Driver	Running
usbhub	Microsoft USB Standard Hub Driver	usbhub.sys	6.3.9600.17238	Kernel Driver	Running
USBHUB3	SuperSpeed Hub	UsbHub3.sys	6.3.9600.17731	Kernel Driver	Stopped
usbohci	Microsoft USB Open Host Controller Miniport Driver	usbohci.sys	6.3.9600.16384	Kernel Driver	Stopped
usbprint	Microsoft USB PRINTER Class	usbprint.sys	6.3.9600.16384	Kernel Driver	Stopped
USBSTOR	USB Mass Storage Driver	USBSTOR.SYS	6.3.9600.17331	Kernel Driver	Stopped
usbuhci	Microsoft USB Universal Host Controller Miniport Driver	usbuhci.sys	6.3.9600.17195	Kernel Driver	Stopped
usbvideo	USB Video Device (WDM)	usbvideo.sys	6.3.9600.17217	Kernel Driver	Running
USBXHCI	USB xHCI Compliant Host Controller	USBXHCI.SYS	6.3.9600.17393	Kernel Driver	Stopped
vdrvroot	Microsoft Virtual Drive Enumerator	vdrvroot.sys	6.3.9600.16384	Kernel Driver	Running
VerifierExt	VerifierExt	VerifierExt.sys	6.3.9600.16404	Kernel Driver	Stopped
vhdmp	vhdmp	vhdmp.sys	6.3.9600.17475	Kernel Driver	Stopped
viaide	viaide	viaide.sys	6.0.6000.170	Kernel Driver	Stopped
Vid	Vid	Vid.sys	6.3.9600.16384	Kernel Driver	Stopped
vmbus	Virtual Machine Bus	vmbus.sys	6.3.9600.17415	Kernel Driver	Stopped
VMBusHID	VMBusHID	VMBusHID.sys	6.3.9600.16384	Kernel Driver	Stopped
vmbusr	Virtual Machine Bus Provider	vmbusr.sys	6.3.9600.16384	Kernel	Stopped

				Driver	
volmgr	Volume Manager Driver	volmgr.sys	6.3.9600.16384	Kernel Driver	Running
volmgrx	Dynamic Volume Manager	volmgrx.sys	6.3.9600.16384	Kernel Driver	Running
volsnap	Storage volumes	volsnap.sys	6.3.9600.17215	Kernel Driver	Running
vpci	Microsoft Hyper-V Virtual PCI Bus	vpci.sys	6.3.9600.17393	Kernel Driver	Stopped
vpcivsp	Microsoft Hyper-V PCI Server	vpcivsp.sys	6.3.9600.16384	Kernel Driver	Stopped
vsmraid	vsmraid	vsmraid.sys	7.0.9200.6320	Kernel Driver	Stopped
VSTXRAID	VIA StorX Storage RAID Controller Windows Driver	vstxraid.sys	8.0.9200.8110	Kernel Driver	Stopped
vwifibus	Virtual WiFi Bus Driver	vwifibus.sys	6.3.9600.16384	Kernel Driver	Running
vwififlt	Virtual WiFi Filter Driver	vwififlt.sys	6.3.9600.17111	Kernel Driver	Running
vwifimp	Virtual WiFi Miniport Service	vwifimp.sys	6.3.9600.17111	Kernel Driver	Running
WacomPen	Wacom Serial Pen HID Driver	wacompen.sys	6.3.9600.16384	Kernel Driver	Stopped
WdBoot	Windows Defender Boot Driver	WdBoot.sys	4.7.205.0	Kernel Driver	Stopped
Wdf01000	Kernel Mode Driver Frameworks service	Wdf01000.sys	1.13.9600.16384	Kernel Driver	Running
WdFilter	Windows Defender Mini-Filter Driver	WdFilter.sys	4.7.205.0	File System Driver	Running
WdNisDrv	Windows Defender Network Inspection System Driver	WdNisDrv.sys	4.7.205.0	Kernel Driver	Running
WFPLWFS	Microsoft Windows Filtering Platform	wfplwfs.sys	6.3.9600.17485	Kernel Driver	Running
WIMMount	WIMMount	wimmount.sys	6.3.9600.17415	File System Driver	Stopped
WinUsb	WinUsb	WinUsb.sys	6.3.9600.16384	Kernel Driver	Stopped
WmiAcpi	Microsoft Windows Management Interface for ACPI	wmiacpi.sys	6.3.9600.16384	Kernel Driver	Running
Wof	Windows Overlay File System Filter Driver			File System Driver	Running
wpcfltr	Family Safety Filter Driver	wpcfltr.sys	6.3.9600.17415	Kernel Driver	Stopped
WpdUpFltr	WPD Upper Class Filter Driver	WpdUpFltr.sys	6.3.9600.16384	Kernel Driver	Stopped
ws2ifsl	Winsock IFS Driver	ws2ifsl.sys	6.3.9600.16384	Kernel Driver	Stopped
WudfPf	User Mode Driver Frameworks Platform Driver	WudfPf.sys	6.3.9600.17415	Kernel Driver	Stopped
WUDFRd	Windows Driver Foundation - User-mode Driver Framework Reflector	WUDFRd.sys	6.3.9600.17415	Kernel Driver	Stopped
WUDFWpdFs	WUDFWpdFs	WUDFRd.sys	6.3.9600.17415	Kernel Driver	Stopped
WUDFWpdMtp	WUDFWpdMtp	WUDFRd.sys	6.3.9600.17415	Kernel Driver	Stopped

Services

Service Name	Service Description	File Name	Version	Type	State	Account
AdvancedSystemCareService8	Advanced SystemCare Service 8	ASCService.exe	8.0.0.20	Own Process	Running	LocalSystem
AeLookupSvc	Application Experience	svchost.exe	6.3.9600.17415	Share Process	Running	localSystem
ALG	Application Layer Gateway Service	alg.exe	6.3.9600.17415	Own Process	Stopped	NT AUTHORITY\LocalService
AppIDSvc	Application Identity	svchost.exe	6.3.9600.17415	Share Process	Stopped	NT Authority\LocalService
Appinfo	Application Information	svchost.exe	6.3.9600.17415	Share Process	Running	LocalSystem
AppMgmt	Application Management	svchost.exe	6.3.9600.17415	Share Process	Stopped	LocalSystem
AppReadiness	App Readiness	svchost.exe	6.3.9600.17415	Share Process	Stopped	LocalSystem
AppXSvc	AppX Deployment Service (AppXSVC)	svchost.exe	6.3.9600.17415	Share Process	Stopped	LocalSystem
AudioEndpointBuilder	Windows Audio Endpoint Builder	svchost.exe	6.3.9600.17415	Share Process	Running	LocalSystem
Audiosrv	Windows Audio	svchost.exe	6.3.9600.17415	Share Process	Running	NT AUTHORITY\LocalService
AxInstSV	ActiveX Installer (AxInstSV)	svchost.exe	6.3.9600.17415	Share Process	Stopped	LocalSystem
BDESVC	BitLocker Drive Encryption Service	svchost.exe	6.3.9600.17415	Share Process	Stopped	localSystem
BFE	Base Filtering Engine	svchost.exe	6.3.9600.17415	Share Process	Running	NT AUTHORITY\LocalService
BITS	Background Intelligent Transfer Service	svchost.exe	6.3.9600.17415	Share Process	Running	LocalSystem
Bluetooth Device Monitor	Bluetooth Device Monitor	devmonsrv.exe	17.1.1411.506	Own Process	Running	LocalSystem
Bluetooth OBEX Service	Bluetooth OBEX Service	obexsrv.exe	17.1.1411.496	Own Process	Running	LocalSystem
BrokerInfrastructure	Background Tasks Infrastructure Service	svchost.exe	6.3.9600.17415	Share Process	Running	LocalSystem
Browser	Computer Browser	svchost.exe	6.3.9600.17415	Share Process	Running	LocalSystem
BthHFSrv	Bluetooth Handsfree Service	svchost.exe	6.3.9600.17415	Share Process	Stopped	NT AUTHORITY\LocalService
bthserv	Bluetooth Support Service	svchost.exe	6.3.9600.17415	Share Process	Running	NT AUTHORITY\LocalService
CertPropSvc	Certificate Propagation	svchost.exe	6.3.9600.17415	Share Process	Stopped	LocalSystem
COMSysApp	COM+ System Application	dllhost.exe	6.3.9600.17415	Own Process	Stopped	LocalSystem
cphs	Intel(R) Content Protection HECI Service	IntelCpHeciSvc.exe	9.0.20.9000	Own Process	Stopped	LocalSystem
CryptSvc	Cryptographic Services	svchost.exe	6.3.9600.17415	Share Process	Running	NT Authority\NetworkService
CscService	Offline Files	svchost.exe	6.3.9600.17415	Share Process	Stopped	LocalSystem
DcomLaunch	DCOM Server Process Launcher	svchost.exe	6.3.9600.17415	Share Process	Running	LocalSystem
defragsvc	Optimize drives	svchost.exe	6.3.9600.17415	Own Process	Stopped	localSystem
DeviceAssociationService	Device Association Service	svchost.exe	6.3.9600.17415	Share Process	Running	LocalSystem
DeviceInstall	Device Install Service	svchost.exe	6.3.9600.17415	Share Process	Stopped	LocalSystem
Dhcp	DHCP Client	svchost.exe	6.3.9600.17415	Share Process	Running	NT Authority\LocalService
DiagTrack	Diagnostics Tracking Service	svchost.exe	6.3.9600.17415	Own Process	Running	LocalSystem

Dnscache	DNS Client	svchost.exe	6.3.9600.17415	Share Process	Running	NT AUTHORITY\NetworkService
dot3svc	Wired AutoConfig	svchost.exe	6.3.9600.17415	Share Process	Stopped	localSystem
DPS	Diagnostic Policy Service	svchost.exe	6.3.9600.17415	Share Process	Running	NT AUTHORITY\LocalService
DsmSvc	Device Setup Manager	svchost.exe	6.3.9600.17415	Share Process	Stopped	LocalSystem
Eaphost	Extensible Authentication Protocol	svchost.exe	6.3.9600.17415	Share Process	Stopped	localSystem
EFS	Encrypting File System (EFS)	lsass.exe	6.3.9600.17415	Share Process	Stopped	LocalSystem
EventLog	Windows Event Log	svchost.exe	6.3.9600.17415	Share Process	Running	NT AUTHORITY\LocalService
EventSystem	COM+ Event System	svchost.exe	6.3.9600.17415	Share Process	Running	NT AUTHORITY\LocalService
Fax	Fax	fxssvc.exe	6.3.9600.17415	Own Process	Stopped	NT AUTHORITY\NetworkService
fdPHost	Function Discovery Provider Host	svchost.exe	6.3.9600.17415	Share Process	Running	NT AUTHORITY\LocalService
FDResPub	Function Discovery Resource Publication	svchost.exe	6.3.9600.17415	Share Process	Running	NT AUTHORITY\LocalService
fhsvc	File History Service	svchost.exe	6.3.9600.17415	Share Process	Stopped	LocalSystem
FontCache	Windows Font Cache Service	svchost.exe	6.3.9600.17415	Share Process	Running	NT AUTHORITY\LocalService
FontCache3.0.0.0	Windows Presentation Foundation Font Cache 3.0.0.0	PresentationFontCache.exe	3.0.6920.7903	Own Process	Running	NT Authority\LocalService
gpsvc	Group Policy Client	svchost.exe	6.3.9600.17415	Share Process	Running	LocalSystem
gupdate	Google Update Service (gupdate)	GoogleUpdate.exe	1.3.26.9	Own Process	Stopped	LocalSystem
gupdatem	Google Update Service (gupdatem)	GoogleUpdate.exe	1.3.26.9	Own Process	Stopped	LocalSystem
hidserv	Human Interface Device Service	svchost.exe	6.3.9600.17415	Share Process	Stopped	LocalSystem
hkmsvc	Health Key and Certificate Management	svchost.exe	6.3.9600.17415	Share Process	Stopped	localSystem
HomeGroupListener	HomeGroup Listener	svchost.exe	6.3.9600.17415	Share Process	Stopped	LocalSystem
HomeGroupProvider	HomeGroup Provider	svchost.exe	6.3.9600.17415	Share Process	Running	NT AUTHORITY\LocalService
iBtSiva	Intel Bluetooth Service	ibtsiva.exe	17.1.1512.771	Own Process	Stopped	LocalSystem
IEEtwCollectorService	Internet Explorer ETW Collector Service	IEEtwCollector.exe	11.0.9600.17416	Own Process	Stopped	LocalSystem
igfxCUIService1.0.0.0	Intel(R) HD Graphics Control Panel Service	igfxCUIService.exe	6.15.10.3958	Own Process	Running	LocalSystem
IKEEXT	IKE and AuthIP IPsec Keying Modules	svchost.exe	6.3.9600.17415	Share Process	Stopped	LocalSystem
iphlpsvc	IP Helper	svchost.exe	6.3.9600.17415	Share Process	Stopped	LocalSystem
KeyIso	CNG Key Isolation	lsass.exe	6.3.9600.17415	Share Process	Stopped	LocalSystem
KtmRm	KtmRm for Distributed Transaction Coordinator	svchost.exe	6.3.9600.17415	Share Process	Stopped	NT AUTHORITY\NetworkService
LanmanServer	Server	svchost.exe	6.3.9600.17415	Share Process	Running	LocalSystem
LanmanWorkstation	Workstation	svchost.exe	6.3.9600.17415	Share Process	Running	NT AUTHORITY\NetworkService
lfsvc	Windows Location Framework Service	svchost.exe	6.3.9600.17415	Share Process	Stopped	LocalSystem
LiveUpdateSvc	LiveUpdate	LiveUpdate.exe	2.1.3.569	Own Process	Running	LocalSystem
lltdsvc	Link-Layer Topology Discovery Mapper	svchost.exe	6.3.9600.17415	Share Process	Stopped	NT AUTHORITY\LocalService

lmhosts	TCP/IP NetBIOS Helper	svchost.exe	6.3.9600.17415	Share Process	Running	NT AUTHORITY\LocalService
LSM	Local Session Manager	svchost.exe	6.3.9600.17415	Share Process	Running	LocalSystem
MMCSS	Multimedia Class Scheduler	svchost.exe	6.3.9600.17415	Share Process	Running	LocalSystem
MpsSvc	Windows Firewall	svchost.exe	6.3.9600.17415	Share Process	Running	NT Authority\LocalService
MSDTC	Distributed Transaction Coordinator	msdtc.exe	2001.12.10530.17415	Own Process	Stopped	NT AUTHORITY\NetworkService
MSiSCSI	Microsoft iSCSI Initiator Service	svchost.exe	6.3.9600.17415	Share Process	Stopped	LocalSystem
msiserver	Windows Installer	msiexec.exe	5.0.9600.17415	Own Process	Stopped	LocalSystem
MsKeyboardFilter	Microsoft Keyboard Filter	svchost.exe	6.3.9600.17415	Share Process	Stopped	LocalSystem
napagent	Network Access Protection Agent	svchost.exe	6.3.9600.17415	Share Process	Stopped	NT AUTHORITY\NetworkService
NcaSvc	Network Connectivity Assistant	svchost.exe	6.3.9600.17415	Share Process	Stopped	LocalSystem
NcbService	Network Connection Broker	svchost.exe	6.3.9600.17415	Share Process	Running	LocalSystem
NcdAutoSetup	Network Connected Devices Auto-Setup	svchost.exe	6.3.9600.17415	Share Process	Running	NT AUTHORITY\LocalService
Netlogon	Netlogon	lsass.exe	6.3.9600.17415	Share Process	Stopped	LocalSystem
Netman	Network Connections	svchost.exe	6.3.9600.17415	Share Process	Stopped	LocalSystem
netprofm	Network List Service	svchost.exe	6.3.9600.17415	Share Process	Running	NT AUTHORITY\LocalService
NetTcpPortSharing	Net.Tcp Port Sharing Service	SMSvcHost.exe	4.0.30319.33440	Share Process	Stopped	NT AUTHORITY\LocalService
NlaSvc	Network Location Awareness	svchost.exe	6.3.9600.17415	Share Process	Running	NT AUTHORITY\NetworkService
nsi	Network Store Interface Service	svchost.exe	6.3.9600.17415	Share Process	Running	NT Authority\LocalService
ose64	Office 64 Source Engine	OSE.EXE	15.0.4454.1000	Own Process	Stopped	LocalSystem
p2pimsvc	Peer Networking Identity Manager	svchost.exe	6.3.9600.17415	Share Process	Stopped	NT AUTHORITY\LocalService
p2psvc	Peer Networking Grouping	svchost.exe	6.3.9600.17415	Share Process	Stopped	NT AUTHORITY\LocalService
PcaSvc	Program Compatibility Assistant Service	svchost.exe	6.3.9600.17415	Share Process	Running	LocalSystem
PeerDistSvc	BranchCache	svchost.exe	6.3.9600.17415	Share Process	Stopped	NT AUTHORITY\NetworkService
PerfHost	Performance Counter DLL Host	perfhost.exe	6.3.9600.16384	Own Process	Stopped	NT AUTHORITY\LocalService
pla	Performance Logs & Alerts	svchost.exe	6.3.9600.17415	Share Process	Stopped	NT AUTHORITY\LocalService
PlugPlay	Plug and Play	svchost.exe	6.3.9600.17415	Share Process	Running	LocalSystem
PNRPAutoReg	PNRP Machine Name Publication Service	svchost.exe	6.3.9600.17415	Share Process	Stopped	NT AUTHORITY\LocalService
PNRPsvc	Peer Name Resolution Protocol	svchost.exe	6.3.9600.17415	Share Process	Stopped	NT AUTHORITY\LocalService
PolicyAgent	IPsec Policy Agent	svchost.exe	6.3.9600.17415	Share Process	Running	NT Authority\NetworkService
Power	Power	svchost.exe	6.3.9600.17415	Share Process	Running	LocalSystem
PrintNotify	Printer Extensions and Notifications	svchost.exe	6.3.9600.17415	Share Process	Stopped	LocalSystem
				Share		

ProfSvc	User Profile Service	svchost.exe	6.3.9600.17415	Share Process	Running	LocalSystem
QWAVE	Quality Windows Audio Video Experience	svchost.exe	6.3.9600.17415	Share Process	Stopped	NT AUTHORITY\LocalService
RasAuto	Remote Access Auto Connection Manager	svchost.exe	6.3.9600.17415	Share Process	Stopped	localSystem
RasMan	Remote Access Connection Manager	svchost.exe	6.3.9600.17415	Share Process	Stopped	localSystem
RemoteAccess	Routing and Remote Access	svchost.exe	6.3.9600.17415	Share Process	Stopped	localSystem
RemoteRegistry	Remote Registry	svchost.exe	6.3.9600.17415	Share Process	Stopped	NT AUTHORITY\LocalService
RpcEptMapper	RPC Endpoint Mapper	svchost.exe	6.3.9600.17415	Share Process	Running	NT AUTHORITY\NetworkService
RpcLocator	Remote Procedure Call (RPC) Locator	locator.exe	6.3.9600.17415	Own Process	Stopped	NT AUTHORITY\NetworkService
RpcSs	Remote Procedure Call (RPC)	svchost.exe	6.3.9600.17415	Share Process	Running	NT AUTHORITY\NetworkService
SamSs	Security Accounts Manager	lsass.exe	6.3.9600.17415	Share Process	Running	LocalSystem
SCardSvr	Smart Card	svchost.exe	6.3.9600.17415	Share Process	Stopped	NT AUTHORITY\LocalService
ScDeviceEnum	Smart Card Device Enumeration Service	svchost.exe	6.3.9600.17415	Share Process	Stopped	LocalSystem
Schedule	Task Scheduler	svchost.exe	6.3.9600.17415	Share Process	Running	LocalSystem
SCPolicySvc	Smart Card Removal Policy	svchost.exe	6.3.9600.17415	Share Process	Stopped	LocalSystem
seclogon	Secondary Logon	svchost.exe	6.3.9600.17415	Share Process	Stopped	LocalSystem
SENS	System Event Notification Service	svchost.exe	6.3.9600.17415	Share Process	Running	LocalSystem
SensrSvc	Sensor Monitoring Service	svchost.exe	6.3.9600.17415	Share Process	Stopped	NT AUTHORITY\LocalService
SessionEnv	Remote Desktop Configuration	svchost.exe	6.3.9600.17415	Share Process	Stopped	localSystem
SharedAccess	Internet Connection Sharing (ICS)	svchost.exe	6.3.9600.17415	Share Process	Stopped	LocalSystem
ShellHWDetection	Shell Hardware Detection	svchost.exe	6.3.9600.17415	Share Process	Running	LocalSystem
smphost	Microsoft Storage Spaces SMP	svchost.exe	6.3.9600.17415	Own Process	Stopped	NT AUTHORITY\NetworkService
SNMPTRAP	SNMP Trap	snmptrap.exe	6.3.9600.17415	Own Process	Stopped	NT AUTHORITY\LocalService
Spooler	Print Spooler	spoolsv.exe	6.3.9600.17480	Own Process	Running	LocalSystem
sppsvc	Software Protection	sppsvc.exe	6.3.9600.16497	Own Process	Running	NT AUTHORITY\NetworkService
ss_conn_service	SAMSUNG Mobile Connectivity Service	ss_conn_service.exe	2.5.0.0	Own Process	Running	LocalSystem
SSDPSRV	SSDP Discovery	svchost.exe	6.3.9600.17415	Share Process	Running	NT AUTHORITY\LocalService
SstpSvc	Secure Socket Tunneling Protocol Service	svchost.exe	6.3.9600.17415	Share Process	Stopped	NT Authority\LocalService
StartMenuService	StartMenu8 Service	StartMenuServices.exe	1.0.0.0	Own Process	Running	LocalSystem
stisvc	Windows Image Acquisition (WIA)	svchost.exe	6.3.9600.17415	Own Process	Running	NT Authority\LocalService
StorSvc	Storage Service	svchost.exe	6.3.9600.17415	Share Process	Stopped	LocalSystem
svsvc	Spot Verifier	svchost.exe	6.3.9600.17415	Share Process	Stopped	LocalSystem
swprv	Microsoft Software Shadow Copy Provider	svchost.exe	6.3.9600.17415	Own Process	Stopped	LocalSystem
SysMain	Superfetch	svchost.exe	6.3.9600.17415	Share Process	Running	LocalSystem

SystemEventsBroker	System Events Broker	svchost.exe	6.3.9600.17415	Share Process	Running	LocalSystem
TabletInputService	Touch Keyboard and Handwriting Panel Service	svchost.exe	6.3.9600.17415	Share Process	Stopped	LocalSystem
TapiSrv	Telephony	svchost.exe	6.3.9600.17415	Share Process	Stopped	NT AUTHORITY\NetworkService
TermService	Remote Desktop Services	svchost.exe	6.3.9600.17415	Share Process	Stopped	NT Authority\NetworkService
Themes	Themes	svchost.exe	6.3.9600.17415	Share Process	Running	LocalSystem
THREADORDER	Thread Ordering Server	svchost.exe	6.3.9600.17415	Share Process	Stopped	NT AUTHORITY\LocalService
TimeBroker	Time Broker	svchost.exe	6.3.9600.17415	Share Process	Running	NT AUTHORITY\LocalService
TrkWks	Distributed Link Tracking Client	svchost.exe	6.3.9600.17415	Share Process	Running	LocalSystem
TrustedInstaller	Windows Modules Installer	TrustedInstaller.exe	6.3.9600.17415	Own Process	Stopped	localSystem
UI0Detect	Interactive Services Detection	UI0Detect.exe	6.3.9600.17415	Own Process	Stopped	LocalSystem
UmRdpService	Remote Desktop Services UserMode Port Redirector	svchost.exe	6.3.9600.17415	Share Process	Stopped	localSystem
upnphost	UPnP Device Host	svchost.exe	6.3.9600.17415	Share Process	Stopped	NT AUTHORITY\LocalService
VaultSvc	Credential Manager	lsass.exe	6.3.9600.17415	Share Process	Stopped	LocalSystem
vds	Virtual Disk	vds.exe	6.3.9600.17415	Own Process	Stopped	LocalSystem
vmicguestinterface	Hyper-V Guest Service Interface	svchost.exe	6.3.9600.17415	Share Process	Stopped	LocalSystem
vmicheartbeat	Hyper-V Heartbeat Service	svchost.exe	6.3.9600.17415	Share Process	Stopped	LocalSystem
vmickvpexchange	Hyper-V Data Exchange Service	svchost.exe	6.3.9600.17415	Share Process	Stopped	LocalSystem
vmicrdv	Hyper-V Remote Desktop Virtualization Service	svchost.exe	6.3.9600.17415	Share Process	Stopped	LocalSystem
vmicshutdown	Hyper-V Guest Shutdown Service	svchost.exe	6.3.9600.17415	Share Process	Stopped	LocalSystem
vmictimesync	Hyper-V Time Synchronization Service	svchost.exe	6.3.9600.17415	Share Process	Stopped	NT AUTHORITY\LocalService
vmicvss	Hyper-V Volume Shadow Copy Requestor	svchost.exe	6.3.9600.17415	Share Process	Stopped	LocalSystem
VSS	Volume Shadow Copy	vssvc.exe	6.3.9600.17466	Own Process	Stopped	LocalSystem
W32Time	Windows Time	svchost.exe	6.3.9600.17415	Share Process	Stopped	NT AUTHORITY\LocalService
wbengine	Block Level Backup Engine Service	wbengine.exe	6.3.9600.17415	Own Process	Stopped	localSystem
WbioSrvc	Windows Biometric Service	svchost.exe	6.3.9600.17415	Share Process	Stopped	LocalSystem
Wcmsvc	Windows Connection Manager	svchost.exe	6.3.9600.17415	Share Process	Running	NT Authority\LocalService
wcncsvc	Windows Connect Now - Config Registrar	svchost.exe	6.3.9600.17415	Share Process	Running	NT AUTHORITY\LocalService
WcsPlugInService	Windows Color System	svchost.exe	6.3.9600.17415	Share Process	Stopped	NT AUTHORITY\LocalService
WdiServiceHost	Diagnostic Service Host	svchost.exe	6.3.9600.17415	Share Process	Running	NT AUTHORITY\LocalService
WdiSystemHost	Diagnostic System Host	svchost.exe	6.3.9600.17415	Share Process	Running	LocalSystem
WdNisSvc	Windows Defender Network Inspection Service	NisSrv.exe		Own Process	Running	NT AUTHORITY\LocalService
WebClient	WebClient	svchost.exe	6.3.9600.17415	Share Process	Stopped	NT AUTHORITY\LocalService
Wecsvc	Windows Event Collector	svchost.exe	6.3.9600.17415	Share Process	Stopped	NT AUTHORITY\NetworkService

WEPHOSTSVC	Windows Encryption Provider Host Service	svchost.exe	6.3.9600.17415	Share Process	Stopped	NT AUTHORITY\LocalService
wercplsupport	Problem Reports and Solutions Control Panel Support	svchost.exe	6.3.9600.17415	Share Process	Stopped	localSystem
WerSvc	Windows Error Reporting Service	svchost.exe	6.3.9600.17415	Own Process	Stopped	localSystem
WiaRpc	Still Image Acquisition Events	svchost.exe	6.3.9600.17415	Share Process	Stopped	LocalSystem
WinDefend	Windows Defender Service	MsMpEng.exe		Own Process	Running	LocalSystem
WinHttpAutoProxySvc	WinHTTP Web Proxy Auto-Discovery Service	svchost.exe	6.3.9600.17415	Share Process	Stopped	NT AUTHORITY\LocalService
Winmgmt	Windows Management Instrumentation	svchost.exe	6.3.9600.17415	Share Process	Running	localSystem
WinRM	Windows Remote Management (WS-Management)	svchost.exe	6.3.9600.17415	Share Process	Stopped	NT AUTHORITY\NetworkService
WlanSvc	WLAN AutoConfig	svchost.exe	6.3.9600.17415	Share Process	Running	LocalSystem
wlidsvc	Microsoft Account Sign-in Assistant	svchost.exe	6.3.9600.17415	Share Process	Stopped	LocalSystem
wmiApSrv	WMI Performance Adapter	WmiApSrv.exe	6.3.9600.17415	Own Process	Stopped	localSystem
WMPNetworkSvc	Windows Media Player Network Sharing Service	wmpnetwk.exe		Own Process	Stopped	NT AUTHORITY\NetworkService
workfolderssvc	Work Folders	svchost.exe	6.3.9600.17415	Share Process	Stopped	NT AUTHORITY\LocalService
WPCSvc	Family Safety	svchost.exe	6.3.9600.17415	Share Process	Stopped	NT Authority\LocalService
WPDBusEnum	Portable Device Enumerator Service	svchost.exe	6.3.9600.17415	Share Process	Stopped	LocalSystem
wscsvc	Security Center	svchost.exe	6.3.9600.17415	Share Process	Running	NT AUTHORITY\LocalService
WSearch	Windows Search	SearchIndexer.exe	7.0.9600.17415	Own Process	Running	LocalSystem
WSService	Windows Store Service (WSService)	svchost.exe	6.3.9600.17415	Share Process	Stopped	LocalSystem
wuauserv	Windows Update	svchost.exe	6.3.9600.17415	Share Process	Stopped	LocalSystem
wudfsvc	Windows Driver Foundation - User-mode Driver Framework	svchost.exe	6.3.9600.17415	Share Process	Stopped	LocalSystem
WwanSvc	WWAN AutoConfig	svchost.exe	6.3.9600.17415	Share Process	Stopped	NT Authority\LocalService

AX Files

AX File	Version	Description
bdaplgin.ax	6.3.9600.17415	Microsoft BDA Device Control Plug-in for MPEG2 based networks.
g711codc.ax	6.3.9600.17415	Intel G711 CODEC
iac25_32.ax	2.0.5.53	Indeo® audio software
ir41_32.ax	6.3.9600.17415	IR41_32 WRAPPER DLL
ivfsrc.ax	5.10.2.51	Intel Indeo® video IVF Source Filter 5.10
ksproxy.ax	6.3.9600.17415	WDM Streaming ActiveMovie Proxy
kstvtune.ax	6.3.9600.17415	WDM Streaming TvTuner
kswdmcap.ax	6.3.9600.17415	WDM Streaming Video Capture
ksxbar.ax	6.3.9600.17415	WDM Streaming Crossbar
mpeg2data.ax	6.6.9600.17415	Microsoft MPEG-2 Section and Table Acquisition Module
mpg2splt.ax	6.6.9600.17415	DirectShow MPEG-2 Splitter.
msdvbnp.ax	6.6.9600.17415	Microsoft Network Provider for MPEG2 based networks.
msnp.ax	6.6.9600.17415	Microsoft Network Provider for MPEG2 based networks.

psisrndr.ax	6.6.9600.17415	Microsoft Transport Information Filter for MPEG2 based networks.
vbicodec.ax	6.6.9600.17415	Microsoft VBI Codec
vbisurf.ax	6.3.9600.17415	VBI Surface Allocator Filter
vidcap.ax	6.3.9600.17415	Video Capture Interface Server
wstpager.ax	6.6.9600.17415	Microsoft Teletext Server

DLL Files

DLL File	Version	Description
accessibilitycpl.dll	6.3.9600.17415	Ease of access control panel
acctres.dll	6.3.9600.16384	Microsoft Internet Account Manager Resources
acledit.dll	6.3.9600.17415	Access Control List Editor
aclui.dll	6.3.9600.17415	Security Descriptor Editor
acppage.dll	6.3.9600.17415	Compatibility Tab Shell Extension Library
actioncenter.dll	6.3.9600.17415	Action Center
actioncentercpl.dll	6.3.9600.17415	Action Center Control Panel
activeds.dll	6.3.9600.17415	ADs Router Layer DLL
actxprxy.dll	6.3.9600.17416	ActiveX Interface Marshaling Library
admtmpl.dll	6.3.9600.17415	Administrative Templates Extension
adprovider.dll	6.3.9600.17415	adprovider DLL
adrclient.dll	6.3.9600.17415	Microsoft® Access Denied Remediation Client
adsldp.dll	6.3.9600.17415	ADs LDAP Provider DLL
adsldpc.dll	6.3.9600.17415	ADs LDAP Provider C DLL
adsmsext.dll	6.3.9600.17415	ADs LDAP Provider DLL
adsnt.dll	6.3.9600.17415	ADs Windows NT Provider DLL
adtschema.dll	6.3.9600.17415	Security Audit Schema DLL
advapi32.dll	6.3.9600.17415	Advanced Windows 32 Base API
advapi32res.dll	6.3.9600.16384	Advanced Windows 32 Base API
advpack.dll	11.0.9600.17415	ADVPACK
aeevts.dll	6.3.9600.16384	Application Experience Event Resources
amstream.dll	6.6.9600.17415	DirectShow Runtime.
apds.dll	6.3.9600.17415	Microsoft® Help Data Services Module
api-ms-win-appmodel-identity-l1-1-0.dll	6.3.9600.16384	ApiSet Stub DLL
api-ms-win-appmodel-runtime-internal-l1-1-0.dll	6.3.9600.16384	ApiSet Stub DLL
api-ms-win-appmodel-runtime-l1-1-0.dll	6.3.9600.16384	ApiSet Stub DLL
api-ms-win-appmodel-runtime-l1-1-1.dll	6.3.9600.16384	ApiSet Stub DLL
api-ms-win-appmodel-state-l1-1-0.dll	6.3.9600.16384	ApiSet Stub DLL
api-ms-win-appmodel-state-l1-1-1.dll	6.3.9600.16384	ApiSet Stub DLL
api-ms-win-base-bootconfig-l1-1-0.dll	6.3.9600.16384	ApiSet Stub DLL
api-ms-win-base-util-l1-1-0.dll	6.3.9600.16384	ApiSet Stub DLL
api-ms-win-core-apiquery-l1-1-0.dll	6.3.9600.16384	ApiSet Stub DLL
api-ms-win-core-appcompat-l1-1-0.dll	6.3.9600.16384	ApiSet Stub DLL
api-ms-win-core-appcompat-l1-1-1.dll	6.3.9600.16384	ApiSet Stub DLL
api-ms-win-core-appinit-l1-1-0.dll	6.3.9600.16384	ApiSet Stub DLL
api-ms-win-core-atoms-l1-1-0.dll	6.3.9600.16384	ApiSet Stub DLL
api-ms-win-core-bem-l1-1-0.dll	6.3.9600.16384	ApiSet Stub DLL
api-ms-win-core-bicltapi-l1-1-0.dll	6.3.9600.16384	ApiSet Stub DLL
api-ms-win-core-bicltapi-l1-1-1.dll	6.3.9600.16384	ApiSet Stub DLL
api-ms-win-core-biplmapi-l1-1-0.dll	6.3.9600.16384	ApiSet Stub DLL
api-ms-win-core-biplmapi-l1-1-1.dll	6.3.9600.16384	ApiSet Stub DLL
api-ms-win-core-biptcltapi-l1-1-0.dll	6.3.9600.16384	ApiSet Stub DLL
api-ms-win-core-biptcltapi-l1-1-1.dll	6.3.9600.16384	ApiSet Stub DLL

api-ms-win-core-calendar-l1-1-0.dll	6.3.9600.16384	ApiSet Stub DLL
api-ms-win-core-com-l1-1-0.dll	6.3.9600.16384	ApiSet Stub DLL
api-ms-win-core-com-l1-1-1.dll	6.3.9600.16384	ApiSet Stub DLL
api-ms-win-core-comm-l1-1-0.dll	6.3.9600.16384	ApiSet Stub DLL
api-ms-win-core-com-private-l1-1-0.dll	6.3.9600.16384	ApiSet Stub DLL
api-ms-win-core-console-l1-1-0.dll	6.3.9600.16384	ApiSet Stub DLL
api-ms-win-core-console-l2-1-0.dll	6.3.9600.16384	ApiSet Stub DLL
api-ms-win-core-crt-l1-1-0.dll	6.3.9600.16384	ApiSet Stub DLL
api-ms-win-core-crt-l2-1-0.dll	6.3.9600.16384	ApiSet Stub DLL
api-ms-win-core-datetime-l1-1-0.dll	6.3.9600.16384	ApiSet Stub DLL
api-ms-win-core-datetime-l1-1-1.dll	6.3.9600.16384	ApiSet Stub DLL
api-ms-win-core-debug-l1-1-0.dll	6.3.9600.16384	ApiSet Stub DLL
api-ms-win-core-debug-l1-1-1.dll	6.3.9600.16384	ApiSet Stub DLL
api-ms-win-core-delayload-l1-1-0.dll	6.3.9600.16384	ApiSet Stub DLL
api-ms-win-core-delayload-l1-1-1.dll	6.3.9600.16384	ApiSet Stub DLL
api-ms-win-core-errorhandling-l1-1-0.dll	6.3.9600.16384	ApiSet Stub DLL
api-ms-win-core-errorhandling-l1-1-1.dll	6.3.9600.16384	ApiSet Stub DLL
api-ms-win-core-fibers-l1-1-0.dll	6.3.9600.16384	ApiSet Stub DLL
api-ms-win-core-fibers-l1-1-1.dll	6.3.9600.16384	ApiSet Stub DLL
api-ms-win-core-fibers-l2-1-0.dll	6.3.9600.16384	ApiSet Stub DLL
api-ms-win-core-fibers-l2-1-1.dll	6.3.9600.16384	ApiSet Stub DLL
api-ms-win-core-file-l1-1-0.dll	6.3.9600.16384	ApiSet Stub DLL
api-ms-win-core-file-l1-2-0.dll	6.3.9600.16384	ApiSet Stub DLL
api-ms-win-core-file-l1-2-1.dll	6.3.9600.16384	ApiSet Stub DLL
api-ms-win-core-file-l2-1-0.dll	6.3.9600.16384	ApiSet Stub DLL
api-ms-win-core-file-l2-1-1.dll	6.3.9600.16384	ApiSet Stub DLL
api-ms-win-core-firmware-l1-1-0.dll	6.3.9600.16384	ApiSet Stub DLL
api-ms-win-core-handle-l1-1-0.dll	6.3.9600.16384	ApiSet Stub DLL
api-ms-win-core-heap-l1-1-0.dll	6.3.9600.16384	ApiSet Stub DLL
api-ms-win-core-heap-l1-2-0.dll	6.3.9600.16384	ApiSet Stub DLL
api-ms-win-core-heap-obsolete-l1-1-0.dll	6.3.9600.16384	ApiSet Stub DLL
api-ms-win-core-interlocked-l1-1-0.dll	6.3.9600.16384	ApiSet Stub DLL
api-ms-win-core-interlocked-l1-2-0.dll	6.3.9600.16384	ApiSet Stub DLL
api-ms-win-core-io-l1-1-0.dll	6.3.9600.16384	ApiSet Stub DLL
api-ms-win-core-io-l1-1-1.dll	6.3.9600.16384	ApiSet Stub DLL
api-ms-win-core-job-l1-1-0.dll	6.3.9600.16384	ApiSet Stub DLL
api-ms-win-core-job-l2-1-0.dll	6.3.9600.16384	ApiSet Stub DLL
api-ms-win-core-kernel32-legacy-l1-1-0.dll	6.3.9600.16384	ApiSet Stub DLL
api-ms-win-core-kernel32-legacy-l1-1-1.dll	6.3.9600.16384	ApiSet Stub DLL
api-ms-win-core-kernel32-private-l1-1-0.dll	6.3.9600.16384	ApiSet Stub DLL
api-ms-win-core-libraryloader-l1-1-0.dll	6.3.9600.16384	ApiSet Stub DLL
api-ms-win-core-libraryloader-l1-1-1.dll	6.3.9600.16384	ApiSet Stub DLL
api-ms-win-core-libraryloader-l1-2-0.dll	6.3.9600.16384	ApiSet Stub DLL
api-ms-win-core-libraryloader-private-l1-1-0.dll	6.3.9600.16384	ApiSet Stub DLL
api-ms-win-core-localization-l1-1-0.dll	6.3.9600.16384	ApiSet Stub DLL
api-ms-win-core-localization-l1-2-0.dll	6.3.9600.16384	ApiSet Stub DLL
api-ms-win-core-localization-l1-2-1.dll	6.3.9600.16384	ApiSet Stub DLL
api-ms-win-core-localization-l2-1-0.dll	6.3.9600.16384	ApiSet Stub DLL
api-ms-win-core-localization-obsolete-l1-1-0.dll	6.3.9600.16384	ApiSet Stub DLL
api-ms-win-core-localization-obsolete-l1-2-0.dll	6.3.9600.16384	ApiSet Stub DLL
api-ms-win-core-localization-private-l1-1-0.dll	6.3.9600.16384	ApiSet Stub DLL
api-ms-win-core-localregistry-l1-1-0.dll	6.3.9600.16384	ApiSet Stub DLL
api-ms-win-core-memory-l1-1-0.dll	6.3.9600.16384	ApiSet Stub DLL
api-ms-win-core-memory-l1-1-1.dll	6.3.9600.16384	ApiSet Stub DLL

api-ms-win-core-memory-l1-1-2.dll	6.3.9600.16384	ApiSet Stub DLL
api-ms-win-core-multipleproviderrouter-l1-1-0.dll	6.3.9600.16384	ApiSet Stub DLL
api-ms-win-core-namedpipe-l1-1-0.dll	6.3.9600.16384	ApiSet Stub DLL
api-ms-win-core-namedpipe-l1-2-0.dll	6.3.9600.16384	ApiSet Stub DLL
api-ms-win-core-namespace-l1-1-0.dll	6.3.9600.16384	ApiSet Stub DLL
api-ms-win-core-normalization-l1-1-0.dll	6.3.9600.16384	ApiSet Stub DLL
api-ms-win-core-path-l1-1-0.dll	6.3.9600.16384	ApiSet Stub DLL
api-ms-win-core-privateprofile-l1-1-0.dll	6.3.9600.16384	ApiSet Stub DLL
api-ms-win-core-processenvironment-l1-1-0.dll	6.3.9600.16384	ApiSet Stub DLL
api-ms-win-core-processenvironment-l1-2-0.dll	6.3.9600.16384	ApiSet Stub DLL
api-ms-win-core-processsecurity-l1-1-0.dll	6.3.9600.16384	ApiSet Stub DLL
api-ms-win-core-processthreads-l1-1-0.dll	6.3.9600.16384	ApiSet Stub DLL
api-ms-win-core-processthreads-l1-1-1.dll	6.3.9600.16384	ApiSet Stub DLL
api-ms-win-core-processthreads-l1-1-2.dll	6.3.9600.16384	ApiSet Stub DLL
api-ms-win-core-processtopology-l1-1-0.dll	6.3.9600.16384	ApiSet Stub DLL
api-ms-win-core-processtopology-l1-2-0.dll	6.3.9600.16384	ApiSet Stub DLL
api-ms-win-core-processtopology-obsolete-l1-1-0.dll	6.3.9600.16384	ApiSet Stub DLL
api-ms-win-core-processtopology-private-l1-1-0.dll	6.3.9600.16384	ApiSet Stub DLL
api-ms-win-core-profile-l1-1-0.dll	6.3.9600.16384	ApiSet Stub DLL
api-ms-win-core-psapi-ansi-l1-1-0.dll	6.3.9600.16384	ApiSet Stub DLL
api-ms-win-core-psapi-l1-1-0.dll	6.3.9600.16384	ApiSet Stub DLL
api-ms-win-core-psapi-obsolete-l1-1-0.dll	6.3.9600.16384	ApiSet Stub DLL
api-ms-win-core-psm-app-l1-1-0.dll	6.3.9600.16384	ApiSet Stub DLL
api-ms-win-core-psm-appnotify-l1-1-0.dll	6.3.9600.16384	ApiSet Stub DLL
api-ms-win-core-psm-info-l1-1-0.dll	6.3.9600.16384	ApiSet Stub DLL
api-ms-win-core-psm-key-l1-1-0.dll	6.3.9600.16384	ApiSet Stub DLL
api-ms-win-core-psm-plm-l1-1-0.dll	6.3.9600.16384	ApiSet Stub DLL
api-ms-win-core-psm-plm-l1-1-1.dll	6.3.9600.16384	ApiSet Stub DLL
api-ms-win-core-quirks-l1-1-0.dll	6.3.9600.16384	ApiSet Stub DLL
api-ms-win-core-realtime-l1-1-0.dll	6.3.9600.16384	ApiSet Stub DLL
api-ms-win-core-registry-l1-1-0.dll	6.3.9600.16384	ApiSet Stub DLL
api-ms-win-core-registry-l2-1-0.dll	6.3.9600.16384	ApiSet Stub DLL
api-ms-win-core-registry-private-l1-1-0.dll	6.3.9600.16384	ApiSet Stub DLL
api-ms-win-core-registryuserspecific-l1-1-0.dll	6.3.9600.16384	ApiSet Stub DLL
api-ms-win-core-rtlsupport-l1-1-0.dll	6.3.9600.16384	ApiSet Stub DLL
api-ms-win-core-rtlsupport-l1-2-0.dll	6.3.9600.16384	ApiSet Stub DLL
api-ms-win-core-shlwapi-legacy-l1-1-0.dll	6.3.9600.16384	ApiSet Stub DLL
api-ms-win-core-shlwapi-obsolete-l1-1-0.dll	6.3.9600.16384	ApiSet Stub DLL
api-ms-win-core-shutdown-l1-1-0.dll	6.3.9600.16384	ApiSet Stub DLL
api-ms-win-core-sidebyside-l1-1-0.dll	6.3.9600.16384	ApiSet Stub DLL
api-ms-win-core-stringansi-l1-1-0.dll	6.3.9600.16384	ApiSet Stub DLL
api-ms-win-core-string-l1-1-0.dll	6.3.9600.16384	ApiSet Stub DLL
api-ms-win-core-string-l2-1-0.dll	6.3.9600.16384	ApiSet Stub DLL
api-ms-win-core-stringloader-l1-1-0.dll	6.3.9600.16384	ApiSet Stub DLL
api-ms-win-core-stringloader-l1-1-1.dll	6.3.9600.16384	ApiSet Stub DLL
api-ms-win-core-string-obsolete-l1-1-0.dll	6.3.9600.16384	ApiSet Stub DLL
api-ms-win-core-synch-l1-1-0.dll	6.3.9600.16384	ApiSet Stub DLL
api-ms-win-core-synch-l1-2-0.dll	6.3.9600.16384	ApiSet Stub DLL
api-ms-win-core-sysinfo-l1-1-0.dll	6.3.9600.16384	ApiSet Stub DLL
api-ms-win-core-sysinfo-l1-2-0.dll	6.3.9600.16384	ApiSet Stub DLL
api-ms-win-core-sysinfo-l1-2-1.dll	6.3.9600.16384	ApiSet Stub DLL
api-ms-win-core-systemtopology-l1-1-0.dll	6.3.9600.16384	ApiSet Stub DLL
api-ms-win-core-threadpool-l1-1-0.dll	6.3.9600.16384	ApiSet Stub DLL
api-ms-win-core-threadpool-l1-2-0.dll	6.3.9600.16384	ApiSet Stub DLL

api-ms-win-core-threadpool-legacy-l1-1-0.dll	6.3.9600.16384	ApiSet Stub DLL
api-ms-win-core-threadpool-private-l1-1-0.dll	6.3.9600.16384	ApiSet Stub DLL
api-ms-win-core-timezone-l1-1-0.dll	6.3.9600.16384	ApiSet Stub DLL
api-ms-win-core-timezone-private-l1-1-0.dll	6.3.9600.16384	ApiSet Stub DLL
api-ms-win-core-toolhelp-l1-1-0.dll	6.3.9600.16384	ApiSet Stub DLL
api-ms-win-core-url-l1-1-0.dll	6.3.9600.16384	ApiSet Stub DLL
api-ms-win-core-util-l1-1-0.dll	6.3.9600.16384	ApiSet Stub DLL
api-ms-win-core-versionansi-l1-1-0.dll	6.3.9600.16384	ApiSet Stub DLL
api-ms-win-core-version-l1-1-0.dll	6.3.9600.16384	ApiSet Stub DLL
api-ms-win-core-version-private-l1-1-0.dll	6.3.9600.16384	ApiSet Stub DLL
api-ms-win-core-windowserrorreporting-l1-1-0.dll	6.3.9600.16384	ApiSet Stub DLL
api-ms-win-core-winrt-error-l1-1-0.dll	6.3.9600.16384	ApiSet Stub DLL
api-ms-win-core-winrt-error-l1-1-1.dll	6.3.9600.16384	ApiSet Stub DLL
api-ms-win-core-winrt-errorprivate-l1-1-0.dll	6.3.9600.16384	ApiSet Stub DLL
api-ms-win-core-winrt-errorprivate-l1-1-1.dll	6.3.9600.16384	ApiSet Stub DLL
api-ms-win-core-winrt-l1-1-0.dll	6.3.9600.16384	ApiSet Stub DLL
api-ms-win-core-winrt-propertysetprivate-l1-1-0.dll	6.3.9600.16384	ApiSet Stub DLL
api-ms-win-core-winrt-registration-l1-1-0.dll	6.3.9600.16384	ApiSet Stub DLL
api-ms-win-core-winrt-robuffer-l1-1-0.dll	6.3.9600.16384	ApiSet Stub DLL
api-ms-win-core-winrt-roparameterizediid-l1-1-0.dll	6.3.9600.16384	ApiSet Stub DLL
api-ms-win-core-winrt-string-l1-1-0.dll	6.3.9600.16384	ApiSet Stub DLL
api-ms-win-core-wow64-l1-1-0.dll	6.3.9600.16384	ApiSet Stub DLL
api-ms-win-core-xstate-l1-1-0.dll	6.3.9600.16384	ApiSet Stub DLL
api-ms-win-core-xstate-l1-1-1.dll	6.3.9600.16384	ApiSet Stub DLL
api-ms-win-core-xstate-l2-1-0.dll	6.3.9600.16384	ApiSet Stub DLL
api-ms-win-devices-config-l1-1-0.dll	6.3.9600.16384	ApiSet Stub DLL
api-ms-win-devices-config-l1-1-1.dll	6.3.9600.16384	ApiSet Stub DLL
api-ms-win-devices-query-l1-1-0.dll	6.3.9600.16384	ApiSet Stub DLL
api-ms-win-devices-query-l1-1-1.dll	6.3.9600.16384	ApiSet Stub DLL
api-ms-win-devices-swdevice-l1-1-0.dll	6.3.9600.16384	ApiSet Stub DLL
api-ms-win-devices-swdevice-l1-1-1.dll	6.3.9600.16384	ApiSet Stub DLL
api-ms-win-downlevel-advapi32-l1-1-0.dll	6.3.9600.16384	ApiSet Stub DLL
api-ms-win-downlevel-advapi32-l1-1-1.dll	6.3.9600.16384	ApiSet Stub DLL
api-ms-win-downlevel-advapi32-l2-1-0.dll	6.3.9600.16384	ApiSet Stub DLL
api-ms-win-downlevel-advapi32-l2-1-1.dll	6.3.9600.16384	ApiSet Stub DLL
api-ms-win-downlevel-advapi32-l3-1-0.dll	6.3.9600.16384	ApiSet Stub DLL
api-ms-win-downlevel-advapi32-l4-1-0.dll	6.3.9600.16384	ApiSet Stub DLL
api-ms-win-downlevel-kernel32-l1-1-0.dll	6.3.9600.16384	ApiSet Stub DLL
api-ms-win-downlevel-kernel32-l2-1-0.dll	6.3.9600.16384	ApiSet Stub DLL
api-ms-win-downlevel-normaliz-l1-1-0.dll	6.3.9600.16384	ApiSet Stub DLL
api-ms-win-downlevel-ole32-l1-1-0.dll	6.3.9600.16384	ApiSet Stub DLL
api-ms-win-downlevel-ole32-l1-1-1.dll	6.3.9600.16384	ApiSet Stub DLL
api-ms-win-downlevel-shell32-l1-1-0.dll	6.3.9600.16384	ApiSet Stub DLL
api-ms-win-downlevel-shlwapi-l1-1-0.dll	6.3.9600.16384	ApiSet Stub DLL
api-ms-win-downlevel-shlwapi-l1-1-1.dll	6.3.9600.16384	ApiSet Stub DLL
api-ms-win-downlevel-shlwapi-l2-1-0.dll	6.3.9600.16384	ApiSet Stub DLL
api-ms-win-downlevel-shlwapi-l2-1-1.dll	6.3.9600.16384	ApiSet Stub DLL
api-ms-win-downlevel-user32-l1-1-0.dll	6.3.9600.16384	ApiSet Stub DLL
api-ms-win-downlevel-user32-l1-1-1.dll	6.3.9600.16384	ApiSet Stub DLL
api-ms-win-downlevel-version-l1-1-0.dll	6.3.9600.16384	ApiSet Stub DLL
api-ms-win-dx-d3dkmt-l1-1-0.dll	6.3.9600.16384	ApiSet Stub DLL
api-ms-win-eventing-classicprovider-l1-1-0.dll	6.3.9600.16384	ApiSet Stub DLL
api-ms-win-eventing-consumer-l1-1-0.dll	6.3.9600.16384	ApiSet Stub DLL
api-ms-win-eventing-controller-l1-1-0.dll	6.3.9600.16384	ApiSet Stub DLL

api-ms-win-eventing-legacy-l1-1-0.dll	6.3.9600.16384	ApiSet Stub DLL
api-ms-win-eventing-obsolete-l1-1-0.dll	6.3.9600.16384	ApiSet Stub DLL
api-ms-win-eventing-provider-l1-1-0.dll	6.3.9600.16384	ApiSet Stub DLL
api-ms-win-eventlog-legacy-l1-1-0.dll	6.3.9600.16384	ApiSet Stub DLL
api-ms-win-eventlog-private-l1-1-0.dll	6.3.9600.16384	ApiSet Stub DLL
api-ms-win-gdi-dpiinfo-l1-1-0.dll	6.3.9600.16384	ApiSet Stub DLL
api-ms-win-http-time-l1-1-0.dll	6.3.9600.16384	ApiSet Stub DLL
api-ms-win-input-ie-interactioncontext-l1-1-0.dll	6.3.9600.16384	ApiSet Stub DLL
api-ms-win-mm-joystick-l1-1-0.dll	6.3.9600.16384	ApiSet Stub DLL
api-ms-win-mm-mci-l1-1-0.dll	6.3.9600.16384	ApiSet Stub DLL
api-ms-win-mm-misc-l1-1-0.dll	6.3.9600.16384	ApiSet Stub DLL
api-ms-win-mm-misc-l1-1-1.dll	6.3.9600.16384	ApiSet Stub DLL
api-ms-win-mm-misc-l2-1-0.dll	6.3.9600.16384	ApiSet Stub DLL
api-ms-win-mm-mme-l1-1-0.dll	6.3.9600.16384	ApiSet Stub DLL
api-ms-win-mm-playsound-l1-1-0.dll	6.3.9600.16384	ApiSet Stub DLL
api-ms-win-mm-time-l1-1-0.dll	6.3.9600.16384	ApiSet Stub DLL
api-ms-win-net-isolation-l1-1-0.dll	6.3.9600.16384	ApiSet Stub DLL
api-ms-win-net-isolation-l1-1-1.dll	6.3.9600.16384	ApiSet Stub DLL
api-ms-win-ntuser-ie-message-l1-1-0.dll	6.3.9600.16384	ApiSet Stub DLL
api-ms-win-ntuser-ie-window-l1-1-0.dll	6.3.9600.16384	ApiSet Stub DLL
api-ms-win-ntuser-ie-wmpointer-l1-1-0.dll	6.3.9600.16384	ApiSet Stub DLL
api-ms-win-oobe-notification-l1-1-0.dll	6.3.9600.16384	ApiSet Stub DLL
api-ms-win-perf-legacy-l1-1-0.dll	6.3.9600.16384	ApiSet Stub DLL
api-ms-win-power-base-l1-1-0.dll	6.3.9600.16384	ApiSet Stub DLL
api-ms-win-power-setting-l1-1-0.dll	6.3.9600.16384	ApiSet Stub DLL
api-ms-win-ro-typeresolution-l1-1-0.dll	6.3.9600.16384	ApiSet Stub DLL
api-ms-win-rtcore-navigation-l1-1-0.dll	6.3.9600.16384	ApiSet Stub DLL
api-ms-win-rtcore-ntuser-clipboard-l1-1-0.dll	6.3.9600.16384	ApiSet Stub DLL
api-ms-win-rtcore-ntuser-private-l1-1-0.dll	6.3.9600.16384	ApiSet Stub DLL
api-ms-win-rtcore-ntuser-synch-l1-1-0.dll	6.3.9600.16384	ApiSet Stub DLL
api-ms-win-rtcore-ntuser-window-l1-1-0.dll	6.3.9600.16384	ApiSet Stub DLL
api-ms-win-rtcore-ntuser-windowstation-l1-1-0.dll	6.3.9600.16384	ApiSet Stub DLL
api-ms-win-rtcore-ntuser-winevent-l1-1-0.dll	6.3.9600.16384	ApiSet Stub DLL
api-ms-win-rtcore-ntuser-wmpointer-l1-1-0.dll	6.3.9600.16384	ApiSet Stub DLL
api-ms-win-rtcore-ole32-clipboard-l1-1-0.dll	6.3.9600.16384	ApiSet Stub DLL
api-ms-win-rtcore-session-l1-1-0.dll	6.3.9600.16384	ApiSet Stub DLL
api-ms-win-security-activedirectoryclient-l1-1-0.dll	6.3.9600.16384	ApiSet Stub DLL
api-ms-win-security-appcontainer-l1-1-0.dll	6.3.9600.16384	ApiSet Stub DLL
api-ms-win-security-audit-l1-1-0.dll	6.3.9600.16384	ApiSet Stub DLL
api-ms-win-security-audit-l1-1-1.dll	6.3.9600.16384	ApiSet Stub DLL
api-ms-win-security-base-l1-1-0.dll	6.3.9600.16384	ApiSet Stub DLL
api-ms-win-security-base-l1-2-0.dll	6.3.9600.16384	ApiSet Stub DLL
api-ms-win-security-base-private-l1-1-0.dll	6.3.9600.16384	ApiSet Stub DLL
api-ms-win-security-base-private-l1-1-1.dll	6.3.9600.16384	ApiSet Stub DLL
api-ms-win-security-credentials-l1-1-0.dll	6.3.9600.16384	ApiSet Stub DLL
api-ms-win-security-credentials-l2-1-0.dll	6.3.9600.16384	ApiSet Stub DLL
api-ms-win-security-cryptoapi-l1-1-0.dll	6.3.9600.16384	ApiSet Stub DLL
api-ms-win-security-grouppolicy-l1-1-0.dll	6.3.9600.16384	ApiSet Stub DLL
api-ms-win-security-logon-l1-1-0.dll	6.3.9600.16384	ApiSet Stub DLL
api-ms-win-security-lsalookup-l1-1-0.dll	6.3.9600.16384	ApiSet Stub DLL
api-ms-win-security-lsalookup-l1-1-1.dll	6.3.9600.16384	ApiSet Stub DLL
api-ms-win-security-lsalookup-l2-1-0.dll	6.3.9600.16384	ApiSet Stub DLL
api-ms-win-security-lsalookup-l2-1-1.dll	6.3.9600.16384	ApiSet Stub DLL
api-ms-win-security-lsapolicy-l1-1-0.dll	6.3.9600.16384	ApiSet Stub DLL

api-ms-win-security-provider-l1-1-0.dll	6.3.9600.16384	ApiSet Stub DLL
api-ms-win-security-sddl-ansi-l1-1-0.dll	6.3.9600.16384	ApiSet Stub DLL
api-ms-win-security-sddl-l1-1-0.dll	6.3.9600.16384	ApiSet Stub DLL
api-ms-win-security-sddlparsecond-l1-1-0.dll	6.3.9600.16384	ApiSet Stub DLL
api-ms-win-security-systemfunctions-l1-1-0.dll	6.3.9600.16384	ApiSet Stub DLL
api-ms-win-security-trustee-l1-1-0.dll	6.3.9600.16384	ApiSet Stub DLL
api-ms-win-security-trustee-l1-1-1.dll	6.3.9600.16384	ApiSet Stub DLL
api-ms-win-service-core-l1-1-0.dll	6.3.9600.16384	ApiSet Stub DLL
api-ms-win-service-core-l1-1-1.dll	6.3.9600.16384	ApiSet Stub DLL
api-ms-win-service-management-l1-1-0.dll	6.3.9600.16384	ApiSet Stub DLL
api-ms-win-service-management-l2-1-0.dll	6.3.9600.16384	ApiSet Stub DLL
api-ms-win-service-private-l1-1-0.dll	6.3.9600.16384	ApiSet Stub DLL
api-ms-win-service-winsvc-l1-1-0.dll	6.3.9600.16384	ApiSet Stub DLL
api-ms-win-service-winsvc-l1-2-0.dll	6.3.9600.16384	ApiSet Stub DLL
api-ms-win-shcore-comhelpers-l1-1-0.dll	6.3.9600.16384	ApiSet Stub DLL
api-ms-win-shcore-obsolete-l1-1-0.dll	6.3.9600.16384	ApiSet Stub DLL
api-ms-win-shcore-registry-l1-1-1.dll	6.3.9600.16384	ApiSet Stub DLL
api-ms-win-shcore-scaling-l1-1-0.dll	6.3.9600.16384	ApiSet Stub DLL
api-ms-win-shcore-scaling-l1-1-1.dll	6.3.9600.16384	ApiSet Stub DLL
api-ms-win-shcore-stream-l1-1-0.dll	6.3.9600.16384	ApiSet Stub DLL
api-ms-win-shcore-stream-winrt-l1-1-0.dll	6.3.9600.16384	ApiSet Stub DLL
api-ms-win-shcore-sysinfo-l1-1-0.dll	6.3.9600.16384	ApiSet Stub DLL
api-ms-win-shcore-thread-l1-1-0.dll	6.3.9600.16384	ApiSet Stub DLL
api-ms-win-shcore-unicodeansi-l1-1-0.dll	6.3.9600.16384	ApiSet Stub DLL
api-ms-win-shell-shellcom-l1-1-0.dll	6.3.9600.16384	ApiSet Stub DLL
api-ms-win-shell-shellfolders-l1-1-0.dll	6.3.9600.16384	ApiSet Stub DLL
apphelp.dll	6.3.9600.17415	Application Compatibility Client Library
apphlpdm.dll	6.3.9600.17415	Application Compatibility Help Module
appidapi.dll	6.3.9600.17415	Application Identity APIs Dll
appidpolicyengineapi.dll	6.3.9600.17415	AppId Policy Engine API Module
appmgmts.dll	6.3.9600.17415	Software installation Service
appmgr.dll	6.3.9600.17415	Software Installation Snapin Extenstion
apprepapi.dll	6.3.9600.17415	Application Reputation APIs Dll
apprepsync.dll	6.3.9600.17415	AppRepSync Task
appxalluserstore.dll	6.3.9600.17484	AppX All User Store DLL
appxapplicabilityengine.dll	6.3.9600.17415	AppX Applicability Engine
appxdeploymentclient.dll	6.3.9600.17415	AppX Deployment Client DLL
appxpackaging.dll	6.3.9600.17415	Native Code Appx Packaging Library
appxsip.dll	6.3.9600.17415	Appx Subject Interface Package
asferror.dll	12.0.9600.16384	ASF Error Definitions
aspnet_counters.dll	4.0.30319.33440	Microsoft ASP.NET Performance Counter Shim DLL
asycfilt.dll	6.3.9600.17415	
atl.dll	3.5.2284.0	ATL Module for Windows XP (Unicode)
atl100.dll	10.0.40219.325	ATL Module for Windows
atlthunk.dll	6.3.9600.17670	atlthunk.dll
atmfd.dll	5.1.2.241	Windows NT OpenType/Type 1 Font Driver
atmlib.dll	5.1.2.241	Windows NT OpenType/Type 1 API Library.
audiodev.dll	6.3.9600.17415	Portable Media Devices Shell Extension
audioeng.dll	6.3.9600.17415	Audio Engine
audiokse.dll	6.3.9600.17415	Audio Ks Endpoint
audioses.dll	6.3.9600.17415	Audio Session
auditnativesnapin.dll	6.3.9600.17415	Audit Policy Group Policy Editor Extension
auditpolicygpinterop.dll	6.3.9600.17415	Audit Policy GP Module
auditpolmsg.dll	6.3.9600.16384	Audit Policy MMC SnapIn Messages

authbroker.dll	6.3.9600.17415	Web Authentication WinRT API
authext.dll	6.3.9600.17415	Authentication Extensions
authfwcfg.dll	6.3.9600.17415	Windows Firewall with Advanced Security Configuration Helper
authfwgp.dll	6.3.9600.17415	Windows Firewall with Advanced Security Group Policy Editor Extension
authfwsnapin.dll	6.3.9600.17415	Microsoft.WindowsFirewall.SnapIn
authfwwizfwk.dll	6.3.9600.17415	Wizard Framework
authui.dll	6.3.9600.17669	Windows Authentication UI
authz.dll	6.3.9600.17415	Authorization Framework
autoplay.dll	6.3.9600.17415	AutoPlay Control Panel
avicap32.dll	6.3.9600.17415	AVI Capture window class
avifil32.dll	6.3.9600.17415	Microsoft AVI File support library
avrt.dll	6.3.9600.17415	Multimedia Realtime Runtime
azroles.dll	6.3.9600.17415	azroles Module
azroleui.dll	6.3.9600.17415	Authorization Manager
azsqlext.dll	6.3.9600.17415	AzMan Sql Audit Extended Stored Procedures Dll
basecsp.dll	6.3.9600.17415	Microsoft Base Smart Card Crypto Provider
batmeter.dll	6.3.9600.17415	Battery Meter Helper DLL
bcd.dll	6.3.9600.17415	BCD DLL
bcp47langs.dll	6.3.9600.17415	BCP47 Language Classes
bcrypt.dll	6.3.9600.17415	Windows Cryptographic Primitives Library
bcryptprimitives.dll	6.3.9600.17415	Windows Cryptographic Primitives Library
bidispl.dll	6.3.9600.17415	Bidispl DLL
biocredprov.dll	6.3.9600.17415	WinBio Credential Provider
bitsperf.dll	7.7.9600.17415	Perfmon Counter Access
bitsprx2.dll	7.7.9600.17415	Background Intelligent Transfer Service Proxy
bitsprx3.dll	7.7.9600.17415	Background Intelligent Transfer Service 2.0 Proxy
bitsprx4.dll	7.7.9600.17415	Background Intelligent Transfer Service 2.5 Proxy
bitsprx5.dll	7.7.9600.17415	Background Intelligent Transfer Service 3.0 Proxy
bitsprx6.dll	7.7.9600.17415	Background Intelligent Transfer Service 4.0 Proxy
bitsprx7.dll	7.7.9600.17415	Background Intelligent Transfer Service 5.0 Proxy
biwinrt.dll	6.3.9600.17415	Windows Background Broker Infrastructure
blackbox.dll	11.0.9600.17415	BlackBox DLL
bluetoothapis.dll	6.3.9600.17415	Bluetooth Usermode Api host
bootvid.dll	6.3.9600.16384	VGA Boot Driver
browcli.dll	6.3.9600.17415	Browser Service Client DLL
browseui.dll	6.3.9600.17415	Shell Browser UI Library
btpanui.dll	6.3.9600.17415	Bluetooth PAN User Interface
bwcontexthandler.dll	1.0.0.1	ContextH Application
c_g18030.dll	6.3.9600.17415	GB18030 DBCS-Unicode Conversion DLL
c_is2022.dll	6.3.9600.17415	ISO-2022 Code Page Translation DLL
c_iscii.dll	6.3.9600.17415	ISCII Code Page Translation DLL
cabinet.dll	6.3.9600.17415	Microsoft® Cabinet File API
cabview.dll	6.3.9600.17415	Cabinet File Viewer Shell Extension
callbuttons.dll	6.3.9600.17415	Windows Runtime CallButtonsServer DLL
callbuttons.proxystub.dll	6.3.9600.17415	Windows Runtime CallButtonsServer ProxyStub DLL
capiprovider.dll	6.3.9600.17415	capiprovider DLL
capisp.dll	6.3.9600.17415	Sysprep cleanup dll for CAPI
catsrv.dll	2001.12.10530.17415	COM+ Configuration Catalog Server
catsrvps.dll	2001.12.10530.17415	COM+ Configuration Catalog Server Proxy/Stub
catsrvut.dll	2001.12.10530.17415	COM+ Configuration Catalog Server Utilities
cca.dll	6.6.9600.17415	CCA DirectShow Filter.
cdosys.dll	6.6.9600.17415	Microsoft CDO for Windows Library
certca.dll	6.3.9600.17415	Microsoft® Active Directory Certificate Services CA
certcli.dll	6.3.9600.17704	Microsoft® Active Directory Certificate Services Client

certcredprovider.dll	6.3.9600.17415	Cert Credential Provider
certenc.dll	6.3.9600.17415	Active Directory Certificate Services Encoding
certenroll.dll	6.3.9600.17415	Microsoft® Active Directory Certificate Services Enrollment Client
certenrollui.dll	6.3.9600.17415	X509 Certificate Enrollment UI
certmgr.dll	6.3.9600.17415	Certificates snap-in
certpoleng.dll	6.3.9600.17415	Certificate Policy Engine
cewmdm.dll	12.0.9600.17415	Windows CE WMDM Service Provider
cfgbkend.dll	6.3.9600.17415	Configuration Backend Interface
cfgmgr32.dll	6.3.9600.17415	Configuration Manager DLL
cfmifs.dll	6.3.9600.17415	FmIfs Engine
cfmifsproxy.dll	6.3.9600.17415	Microsoft® FmIfs Proxy Library
chartv.dll	6.3.9600.17415	Chart View
chxreadingstringime.dll	6.3.9600.17415	CHxReadingStringIME
cic.dll	6.3.9600.17415	CIC - MMC controls for Taskpad
clb.dll	6.3.9600.17415	Column List Box
clbcatq.dll	2001.12.10530.17415	COM+ Configuration Catalog
clfsw32.dll	6.3.9600.17719	Common Log Marshalling Win32 DLL
cliconfg.dll	6.3.9600.17415	SQL Client Configuration Utility DLL
clrhost.dll	6.3.9600.17031	In Proc server for managed servers in the Windows Runtime
clusapi.dll	6.3.9600.17415	Cluster API Library
cmcfg32.dll	7.2.9600.17415	Microsoft Connection Manager Configuration Dll
cmdext.dll	6.3.9600.17415	cmd.exe Extension DLL
cmdial32.dll	7.2.9600.17415	Microsoft Connection Manager
cmifw.dll	6.3.9600.17415	Windows Firewall rule configuration plug-in
cmipnpinstall.dll	6.3.9600.16384	PNP plugin installer for CMI
cmlua.dll	7.2.9600.17415	Connection Manager Admin API Helper
cmpbk32.dll	7.2.9600.17415	Microsoft Connection Manager Phonebook
cmstplua.dll	7.2.9600.17415	Connection Manager Admin API Helper for Setup
cmutil.dll	7.2.9600.17415	Microsoft Connection Manager Utility Lib
cngcredui.dll	6.3.9600.17415	Microsoft CNG CredUI Provider
cngprovider.dll	6.3.9600.17415	cngprovider DLL
cnvfat.dll	6.3.9600.17415	FAT File System Conversion Utility DLL
colbact.dll	2001.12.10530.17415	COM+
colorcnv.dll	6.3.9600.17415	Windows Media Color Conversion
colorui.dll	6.3.9600.17415	Microsoft Color Control Panel
combase.dll	6.3.9600.17415	Microsoft COM for Windows
comcat.dll	6.3.9600.17415	Microsoft Component Category Manager Library
comctl32.dll	5.82.9600.17415	User Experience Controls Library
comdlg32.dll	6.3.9600.17415	Common Dialogs DLL
compobj.dll	3.10.0.103	Windows Win16 Application Launcher
comppkgsup.dll	12.0.9600.17415	Component Package Support DLL
compstui.dll	6.3.9600.17415	Common Property Sheet User Interface DLL
comrepl.dll	2001.12.10530.17415	COM+
comres.dll	2001.12.10530.16384	COM+ Resources
comsnap.dll	2001.12.10530.17415	COM+ Explorer MMC Snapin
comsvcs.dll	2001.12.10530.17415	COM+ Services
comuid.dll	2001.12.10530.17415	COM+ Explorer UI
configureexpandedstorage.dll	6.3.9600.17415	ConfigureExpandedStorage
connect.dll	6.3.9600.17415	Get Connected Wizards
connectedaccountstate.dll	6.3.9600.17415	ConnectedAccountState.dll
console.dll	6.3.9600.17415	Control Panel Console Applet
coremmres.dll	6.3.9600.16384	General Core Multimedia Resources
cpfilters.dll	6.6.9600.17415	PTFilter & Encypter/Decrypter Tagger Filters.
credentialmigrationhandler.dll	6.3.9600.17415	Credential Migration Handler

credssp.dll	6.3.9600.17415	Credential Delegation Security Package
credui.dll	6.3.9600.17415	Credential Manager User Interface
crtdll.dll	4.0.1183.1	Microsoft C Runtime Library
crypt32.dll	6.3.9600.17475	Crypto API32
cryptbase.dll	6.3.9600.17415	Base cryptographic API DLL
cryptdlg.dll	6.3.9600.17415	Microsoft Common Certificate Dialogs
cryptdll.dll	6.3.9600.17415	Cryptography Manager
cryptext.dll	6.3.9600.17415	Crypto Shell Extensions
cryptnet.dll	6.3.9600.17415	Crypto Network Related API
cryptowinrt.dll	6.3.9600.17415	Crypto WinRT Library
cryptsp.dll	6.3.9600.17415	Cryptographic Service Provider API
crypttpmeksvc.dll	6.3.9600.17415	Cryptographic TPM Endorsement Key Services
cryptui.dll	6.3.9600.17415	Microsoft Trust UI Provider
cryptuiwizard.dll	6.3.9600.17415	Microsoft Trust UI Provider
cryptxml.dll	6.3.9600.17415	XML DigSig API
cscapi.dll	6.3.9600.17415	Offline Files Win32 API
cscdll.dll	6.3.9600.17415	Offline Files Temporary Shim
cscobj.dll	6.3.9600.17415	In-proc COM object used by clients of CSC API
ctl3d32.dll	2.31.0.0	Ctl3D 3D Windows Controls
d2d1.dll	6.3.9600.17415	Microsoft D2D Library
d3d10.dll	6.3.9600.17415	Direct3D 10 Runtime
d3d10_1.dll	6.3.9600.17415	Direct3D 10.1 Runtime
d3d10_1core.dll	6.3.9600.17415	Direct3D 10.1 Runtime
d3d10core.dll	6.3.9600.17415	Direct3D 10 Runtime
d3d10level9.dll	6.3.9600.17415	Direct3D 10 to Direct3D9 Translation Runtime
d3d10warp.dll	6.3.9600.17415	Direct3D 10 Rasterizer
d3d11.dll	6.3.9600.17415	Direct3D 11 Runtime
d3d8.dll	6.3.9600.17415	Microsoft Direct3D
d3d8thk.dll	6.3.9600.17415	Microsoft Direct3D OS Thunk Layer
d3d9.dll	6.3.9600.17415	Direct3D 9 Runtime
d3dcompiler_33.dll	9.18.904.15	Microsoft Direct3D
d3dcompiler_34.dll	9.19.949.46	Microsoft Direct3D
d3dcompiler_35.dll	9.19.949.1104	Microsoft Direct3D
d3dcompiler_36.dll	9.19.949.2111	Microsoft Direct3D
d3dcompiler_37.dll	9.22.949.2248	Microsoft Direct3D
d3dcompiler_38.dll	9.23.949.2378	Microsoft Direct3D
d3dcompiler_39.dll	9.24.949.2307	Microsoft Direct3D
d3dcompiler_40.dll	9.24.950.2656	Direct3D HLSL Compiler
d3dcompiler_41.dll	9.26.952.2844	Direct3D HLSL Compiler
d3dcompiler_42.dll	9.27.952.3022	Direct3D HLSL Compiler
d3dcompiler_43.dll	9.29.952.3111	Direct3D HLSL Compiler
d3dcompiler_47.dll	6.3.9600.17672	Direct3D HLSL Compiler
d3dcsx_42.dll	9.27.952.3022	Direct3D 10.1 Extensions
d3dcsx_43.dll	9.29.952.3111	Direct3D 10.1 Extensions
d3dim.dll	6.3.9600.17415	Microsoft Direct3D
d3dim700.dll	6.3.9600.17415	Microsoft Direct3D
d3dramp.dll	6.3.9600.17415	Microsoft Direct3D
d3dx10.dll	9.16.843.0	Microsoft Direct3D
d3dx10_33.dll	9.18.904.21	Microsoft Direct3D
d3dx10_34.dll	9.19.949.46	Microsoft Direct3D
d3dx10_35.dll	9.19.949.1104	Microsoft Direct3D
d3dx10_36.dll	9.19.949.2009	Microsoft Direct3D
d3dx10_37.dll	9.19.949.2187	Microsoft Direct3D
d3dx10_38.dll	9.23.949.2378	Microsoft Direct3D

d3dx10_39.dll	9.24.949.2307	Microsoft Direct3D
d3dx10_40.dll	9.24.950.2656	Direct3D 10.1 Extensions
d3dx10_41.dll	9.26.952.2844	Direct3D 10.1 Extensions
d3dx10_42.dll	9.27.952.3001	Direct3D 10.1 Extensions
d3dx10_43.dll	9.29.952.3111	Direct3D 10.1 Extensions
d3dx11_42.dll	9.27.952.3022	Direct3D 10.1 Extensions
d3dx11_43.dll	9.29.952.3111	Direct3D 10.1 Extensions
d3dx9_24.dll	9.5.132.0	Microsoft® DirectX for Windows®
d3dx9_25.dll	9.6.168.0	Microsoft® DirectX for Windows®
d3dx9_26.dll	9.7.239.0	Microsoft® DirectX for Windows®
d3dx9_27.dll	9.8.299.0	Microsoft® DirectX for Windows®
d3dx9_28.dll	9.10.455.0	Microsoft® DirectX for Windows®
d3dx9_29.dll	9.11.519.0	Microsoft® DirectX for Windows®
d3dx9_30.dll	9.12.589.0	Microsoft® DirectX for Windows®
d3dx9_31.dll	9.15.779.0	Microsoft® DirectX for Windows®
d3dx9_32.dll	9.16.843.0	Microsoft® DirectX for Windows®
d3dx9_33.dll	9.18.904.15	Microsoft® DirectX for Windows®
d3dx9_34.dll	9.19.949.46	Microsoft® DirectX for Windows®
d3dx9_35.dll	9.19.949.1104	Microsoft® DirectX for Windows®
d3dx9_36.dll	9.19.949.2111	Microsoft® DirectX for Windows®
d3dx9_37.dll	9.22.949.2248	Microsoft® DirectX for Windows®
d3dx9_38.dll	9.23.949.2378	Microsoft® DirectX for Windows®
d3dx9_39.dll	9.24.949.2307	Microsoft® DirectX for Windows®
d3dx9_40.dll	9.24.950.2656	Direct3D 9 Extensions
d3dx9_41.dll	9.26.952.2844	Direct3D 9 Extensions
d3dx9_42.dll	9.27.952.3001	Direct3D 9 Extensions
d3dx9_43.dll	9.29.952.3111	Direct3D 9 Extensions
d3dxof.dll	6.3.9600.17415	DirectX Files DLL
dabapi.dll	6.3.9600.17415	Desktop Activity Broker API
dafprintprovider.dll	6.3.9600.17415	DAF Print Provider DLL
daotpcredentialprovider.dll	6.3.9600.17415	DirectAccess One-Time Password Credential Provider
dataclen.dll	6.3.9600.17415	Disk Space Cleaner for Windows
davclnt.dll	6.3.9600.17415	Web DAV Client DLL
davhlpr.dll	6.3.9600.17415	DAV Helper DLL
dbgeng.dll	6.3.9600.17415	Windows Symbolic Debugger Engine
dbghelp.dll	6.3.9600.17415	Windows Image Helper
dbnetlib.dll	6.3.9600.17415	Winsock Oriented Net DLL for SQL Clients
dbnmpntw.dll	6.3.9600.17415	Named Pipes Net DLL for SQL Clients
dciman32.dll	6.3.9600.17415	DCI Manager
dcomp.dll	6.3.9600.17415	Microsoft DirectComposition Library
ddaclsys.dll	6.3.9600.17415	SysPrep module for Resetting Data Drive ACL
ddoiproxy.dll	6.3.9600.17415	DDOI Interface Proxy
ddores.dll	6.3.9600.17415	Device Category information and resources
ddraw.dll	6.3.9600.17415	Microsoft DirectDraw
ddrawex.dll	6.3.9600.17415	Direct Draw Ex
defaultdevicemanager.dll	6.3.9600.17415	Default Device Manager
defaultprinterprovider.dll	6.3.9600.17415	Microsoft Windows Default Printer Provider
delegatorprovider.dll	6.3.9600.17415	WMI PassThru Provider for Storage Management
deskadp.dll	6.3.9600.17415	Advanced display adapter properties
deskmon.dll	6.3.9600.17415	Advanced display monitor properties
devdispitemprovider.dll	6.3.9600.17415	DeviceItem inproc devquery subsystem
devenum.dll	6.6.9600.17415	Device enumeration.
deviceaccess.dll	6.3.9600.17415	Device Broker And Policy COM Server
deviceassociation.dll	6.3.9600.17415	Device Association Client DLL

devicecenter.dll	6.3.9600.17415	Device Center
devicedisplaystatusmanager.dll	6.3.9600.17415	Device Display Status Manager
devicepairing.dll	6.3.9600.17481	Shell extensions for Device Pairing
devicepairingfolder.dll	6.3.9600.17415	Device Pairing Folder
devicepairingproxy.dll	6.3.9600.17415	Device Pairing Proxy Dll
devicesetupstatusprovider.dll	6.3.9600.17485	Device Setup Status Provider Dll
deviceuxres.dll	6.3.9600.17415	Windows Device User Experience Resource File
devmgr.dll	6.3.9600.17415	Device Manager MMC Snapin
devobj.dll	6.3.9600.17415	Device Information Set DLL
devrtl.dll	6.3.9600.17415	Device Management Run Time Library
dfscli.dll	6.3.9600.17415	Windows NT Distributed File System Client DLL
dfshim.dll	6.3.9600.16384	ClickOnce Application Deployment Support Library
dfsshlex.dll	6.3.9600.17415	Distributed File System shell extension
dhcpcmonitor.dll	6.3.9600.17415	DHCP Client Monitor Dll
dhcpcore.dll	6.3.9600.17415	DHCP Client Service
dhcpcore6.dll	6.3.9600.17415	DHCPv6 Client
dhcpcsvc.dll	6.3.9600.17415	DHCP Client Service
dhcpcsvc6.dll	6.3.9600.17415	DHCPv6 Client
dhcpqec.dll	6.3.9600.17415	Microsoft DHCP NAP Enforcement Client
dhcpsapi.dll	6.3.9600.17415	DHCP Server API Stub DLL
difxapi.dll	2.1.0.0	Driver Install Frameworks for API library module
dimsjob.dll	6.3.9600.17415	DIMS Job DLL
dimsroam.dll	6.3.9600.17415	Key Roaming DIMS Provider DLL
dinput.dll	6.3.9600.17415	Microsoft DirectInput
dinput8.dll	6.3.9600.17415	Microsoft DirectInput
directdb.dll	6.3.9600.17415	Microsoft Direct Database API
diskcopy.dll	6.3.9600.17415	Windows DiskCopy
dismapi.dll	6.3.9600.17031	DISM API Framework
dispex.dll	5.8.9600.17415	Microsoft ® DispEx
display.dll	6.3.9600.17415	Display Control Panel
dlnashext.dll	12.0.9600.17415	DLNA Namespace DLL
dmband.dll	6.3.9600.17415	Microsoft DirectMusic Band
dmcompos.dll	6.3.9600.17415	Microsoft DirectMusic Composer
dmdlgs.dll	6.3.9600.17415	Disk Management Snap-in Dialogs
dmdskmgr.dll	6.3.9600.17415	Disk Management Snap-in Support Library
dmdskres.dll	6.3.9600.16384	Disk Management Snap-in Resources
dmdskres2.dll	6.3.9600.16384	Disk Management Snap-in Resources
dmime.dll	6.3.9600.17415	Microsoft DirectMusic Interactive Engine
dmintf.dll	6.3.9600.17415	Disk Management DCOM Interface Stub
dmloader.dll	6.3.9600.17415	Microsoft DirectMusic Loader
dmocx.dll	6.3.9600.17415	TreeView OCX
dmscript.dll	6.3.9600.17415	Microsoft DirectMusic Scripting
dmstyle.dll	6.3.9600.17415	Microsoft DirectMusic Style Engline
dmsynth.dll	6.3.9600.17415	Microsoft DirectMusic Software Synthesizer
dmusic.dll	6.3.9600.17415	Microsoft DirectMusic Core Services
dmutil.dll	6.3.9600.17415	Logical Disk Manager Utility Library
dmvdsitf.dll	6.3.9600.17415	Disk Management Snap-in Support Library
dnsapi.dll	6.3.9600.17481	DNS Client API DLL
dnscmmc.dll	6.3.9600.16384	DNS Client MMC Snap-in DLL
docprop.dll	6.3.9600.17415	OLE DocFile Property Page
dot3api.dll	6.3.9600.17415	802.3 Autoconfiguration API
dot3cfg.dll	6.3.9600.17415	802.3 Netsh Helper
dot3dlg.dll	6.3.9600.17415	802.3 UI Helper
dot3gpclnt.dll	6.3.9600.17415	802.3 Group Policy Client

dot3gpui.dll	6.3.9600.17415	802.3 Network Policy Management Snap-in
dot3hc.dll	6.3.9600.17415	Dot3 Helper Class
dot3msm.dll	6.3.9600.17415	802.3 Media Specific Module
dot3ui.dll	6.3.9600.17415	802.3 Advanced UI
dpapi.dll	6.3.9600.17415	Data Protection API
dpapiprovider.dll	6.3.9600.17415	dpapiprovider DLL
dplayx.dll	6.3.9600.16384	DirectPlay Stub
dpmodemx.dll	6.3.9600.16384	DirectPlay Stub
dpnaddr.dll	6.3.9600.16384	DirectPlay Stub
dpnathlp.dll	6.3.9600.16384	DirectPlay Stub
dpnet.dll	6.3.9600.16384	DirectPlay Stub
dpnhpast.dll	6.3.9600.16384	DirectPlay Stub
dpnhupnp.dll	6.3.9600.16384	DirectPlay Stub
dpnlobby.dll	6.3.9600.16384	DirectPlay Stub
dpwsockx.dll	6.3.9600.16384	DirectPlay Stub
dpx.dll	6.3.9600.16384	Microsoft(R) Delta Package Expander
drmmgrtn.dll	11.0.9600.17415	DRM Migration DLL
drmv2clt.dll	11.0.9600.17415	DRMv2 Client DLL
drprov.dll	6.3.9600.17415	Microsoft Remote Desktop Session Host Server Network Provider
drt.dll	6.3.9600.17415	Distributed Routing Table
drtprov.dll	6.3.9600.17415	Distributed Routing Table Providers
drttransport.dll	6.3.9600.17415	Distributed Routing Table Transport Provider
drvstore.dll	6.3.9600.17415	Driver Store API
dsauth.dll	6.3.9600.17415	DS Authorization for Services
dsdmo.dll	6.3.9600.17415	DirectSound Effects
dskquota.dll	6.3.9600.17415	Windows Shell Disk Quota Support DLL
dskquoui.dll	6.3.9600.17415	Windows Shell Disk Quota UI DLL
dsound.dll	6.3.9600.17415	DirectSound
dsparse.dll	6.3.9600.17415	Active Directory Domain Services API
dsprop.dll	6.3.9600.17415	Windows Active Directory Property Pages
dsquery.dll	6.3.9600.17415	Directory Service Find
dsrole.dll	6.3.9600.17415	DS Setup Client DLL
dssec.dll	6.3.9600.17415	Directory Service Security UI
dssenh.dll	6.3.9600.17415	Microsoft Enhanced DSS and Diffie-Hellman Cryptographic Provider
dsui.dll	6.3.9600.17415	Device Setup UI Pages
dsuiext.dll	6.3.9600.17415	Directory Service Common UI
dswave.dll	6.3.9600.17415	Microsoft DirectMusic Wave
dtsh.dll	6.3.9600.17415	Detection and Sharing Status API
dui70.dll	6.3.9600.17415	Windows DirectUI Engine
duser.dll	6.3.9600.17415	Windows DirectUser Engine
dwmapi.dll	6.3.9600.17415	Microsoft Desktop Window Manager API
dwmcore.dll	6.3.9600.17674	Microsoft DWM Core Library
dwrite.dll	6.3.9600.17415	Microsoft DirectX Typography Services
dxdiagn.dll	6.3.9600.17415	Microsoft DirectX Diagnostic Tool
dxgi.dll	6.3.9600.17415	DirectX Graphics Infrastructure
dxmasf.dll	12.0.9600.17415	Microsoft Windows Media Component Removal File.
dxptasksync.dll	6.3.9600.17415	Microsoft Windows DXP Sync.
dxtmsft.dll	11.0.9600.17631	DirectX Media -- Image DirectX Transforms
dxtrans.dll	11.0.9600.17690	DirectX Media -- DirectX Transform Core
dxva2.dll	6.3.9600.17415	DirectX Video Acceleration 2.0 DLL
eapp3hst.dll	6.3.9600.17670	Microsoft ThirdPartyEapDispatcher
eappcfg.dll	6.3.9600.17670	Eap Peer Config
eappgnui.dll	6.3.9600.17670	EAP Generic UI
eapphost.dll	6.3.9600.17670	Microsoft EAPHost Peer service

eappprxy.dll	6.3.9600.17415	Microsoft EAPHost Peer Client DLL
eapprovp.dll	6.3.9600.17415	EAP extension DLL
eapqec.dll	6.3.9600.17415	Microsoft EAP NAP Enforcement Client
easwrt.dll	6.3.9600.17415	Exchange ActiveSync Windows Runtime DLL
efsadu.dll	6.3.9600.17415	File Encryption Utility
efscore.dll	6.3.9600.17415	EFS Core Library
efsutil.dll	6.3.9600.17415	EFS Utility Library
efswrt.dll	6.3.9600.17415	Storage Protection Windows Runtime DLL
ehstorapi.dll	6.3.9600.17415	Windows Enhanced Storage API
ehstorpwdmgr.dll	6.3.9600.17415	Microsoft Enhanced Storage Password Manager
els.dll	6.3.9600.17415	Event Viewer Snapin
elscore.dll	6.3.9600.17415	Els Core Platform DLL
elshyph.dll	6.3.9600.17415	ELS Hyphenation Service
elslad.dll	6.3.9600.17415	ELS Language Detection
elstrans.dll	6.3.9600.17415	ELS Transliteration Service
encapi.dll	6.3.9600.17415	Encoder API
encdec.dll	6.6.9600.17415	XDSCodec & Encypter/Decrypter Tagger Filters.
eqossnap.dll	6.3.9600.17415	EQoS Snapin extension
es.dll	2001.12.10530.17415	COM+
esent.dll	6.3.9600.17415	Extensible Storage Engine for Microsoft(R) Windows(R)
esentprf.dll	6.3.9600.17415	Extensible Storage Engine Performance Monitoring Library for Microsoft(R) Windows(R)
etweseproviderresources.dll	6.3.9600.16384	Microsoft ESE ETW
eventcls.dll	6.3.9600.17466	Microsoft® Volume Shadow Copy Service event class
evr.dll	6.3.9600.17415	Enhanced Video Renderer DLL
explorerframe.dll	6.3.9600.17415	ExplorerFrame
expsrv.dll	6.0.72.9589	Visual Basic for Applications Runtime - Expression Service
ext-ms-win-advapi32-auth-l1-1-0.dll	6.3.9600.16384	ApiSet Stub DLL
ext-ms-win-advapi32-encryptedfile-l1-1-0.dll	6.3.9600.16384	ApiSet Stub DLL
ext-ms-win-advapi32-eventingcontroller-l1-1-0.dll	6.3.9600.16384	ApiSet Stub DLL
ext-ms-win-advapi32-eventlog-l1-1-0.dll	6.3.9600.16384	ApiSet Stub DLL
ext-ms-win-advapi32-idletask-l1-1-0.dll	6.3.9600.16384	ApiSet Stub DLL
ext-ms-win-advapi32-lsa-l1-1-0.dll	6.3.9600.16384	ApiSet Stub DLL
ext-ms-win-advapi32-msi-l1-1-0.dll	6.3.9600.16384	ApiSet Stub DLL
ext-ms-win-advapi32-ntmarta-l1-1-0.dll	6.3.9600.16384	ApiSet Stub DLL
ext-ms-win-advapi32-psm-app-l1-1-0.dll	6.3.9600.16384	ApiSet Stub DLL
ext-ms-win-advapi32-registry-l1-1-0.dll	6.3.9600.16384	ApiSet Stub DLL
ext-ms-win-advapi32-safer-l1-1-0.dll	6.3.9600.16384	ApiSet Stub DLL
ext-ms-win-advapi32-shutdown-l1-1-0.dll	6.3.9600.16384	ApiSet Stub DLL
ext-ms-win-appmodel-deployment-l1-1-0.dll	6.3.9600.16384	ApiSet Stub DLL
ext-ms-win-appxdeploymentclient-appxdeploy-l1-1-0.dll	6.3.9600.16384	ApiSet Stub DLL
ext-ms-win-audiocore-pal-l1-1-0.dll	6.3.9600.16384	ApiSet Stub DLL
ext-ms-win-authz-claimpolicies-l1-1-0.dll	6.3.9600.16384	ApiSet Stub DLL
ext-ms-win-authz-context-l1-1-0.dll	6.3.9600.16384	ApiSet Stub DLL
ext-ms-win-authz-remote-l1-1-0.dll	6.3.9600.16384	ApiSet Stub DLL
ext-ms-win-biometrics-winbio-l1-1-0.dll	6.3.9600.16384	ApiSet Stub DLL
ext-ms-win-bluetooth-deviceassociation-l1-1-0.dll	6.3.9600.16384	ApiSet Stub DLL
ext-ms-win-branding-winbrand-l1-1-0.dll	6.3.9600.16384	ApiSet Stub DLL
ext-ms-win-cluster-clusapi-l1-1-0.dll	6.3.9600.16384	ApiSet Stub DLL
ext-ms-win-cluster-clusapi-l1-1-1.dll	6.3.9600.16384	ApiSet Stub DLL
ext-ms-win-cluster-resutils-l1-1-0.dll	6.3.9600.16384	ApiSet Stub DLL
ext-ms-win-cmd-util-l1-1-0.dll	6.3.9600.16384	ApiSet Stub DLL
ext-ms-win-cng-rng-l1-1-0.dll	6.3.9600.16384	ApiSet Stub DLL
ext-ms-win-com-clbcatq-l1-1-0.dll	6.3.9600.16384	ApiSet Stub DLL
ext-ms-win-com-ole32-l1-1-0.dll	6.3.9600.16384	ApiSet Stub DLL

ext-ms-win-com-ole32-l1-1-1.dll	6.3.9600.16384	ApiSet Stub DLL
ext-ms-win-com-psmregister-l1-1-0.dll	6.3.9600.16384	ApiSet Stub DLL
ext-ms-win-core-bi-service-l1-1-0.dll	6.3.9600.16384	ApiSet Stub DLL
ext-ms-win-core-psm-service-l1-1-0.dll	6.3.9600.16384	ApiSet Stub DLL
ext-ms-win-domainjoin-netjoin-l1-1-0.dll	6.3.9600.16384	ApiSet Stub DLL
ext-ms-win-firewallapi-webproxy-l1-1-0.dll	6.3.9600.16384	ApiSet Stub DLL
ext-ms-win-font-fontgroups-l1-1-0.dll	6.3.9600.16384	ApiSet Stub DLL
ext-ms-win-fs-clfs-l1-1-0.dll	6.3.9600.16384	ApiSet Stub DLL
ext-ms-win-fsutilext-ifsutil-l1-1-0.dll	6.3.9600.16384	ApiSet Stub DLL
ext-ms-win-fsutilext-ulib-l1-1-0.dll	6.3.9600.16384	ApiSet Stub DLL
ext-ms-win-fveapi-query-l1-1-0.dll	6.3.9600.16384	ApiSet Stub DLL
ext-ms-win-gdi-dc-create-l1-1-0.dll	6.3.9600.16384	ApiSet Stub DLL
ext-ms-win-gdi-dc-create-l1-1-1.dll	6.3.9600.16384	ApiSet Stub DLL
ext-ms-win-gdi-dc-l1-2-0.dll	6.3.9600.16384	ApiSet Stub DLL
ext-ms-win-gdi-draw-l1-1-0.dll	6.3.9600.16384	ApiSet Stub DLL
ext-ms-win-gdi-draw-l1-1-1.dll	6.3.9600.16384	ApiSet Stub DLL
ext-ms-win-gdi-font-l1-1-0.dll	6.3.9600.16384	ApiSet Stub DLL
ext-ms-win-gdi-font-l1-1-1.dll	6.3.9600.16384	ApiSet Stub DLL
ext-ms-win-gdi-metafile-l1-1-0.dll	6.3.9600.16384	ApiSet Stub DLL
ext-ms-win-gdi-metafile-l1-1-1.dll	6.3.9600.16384	ApiSet Stub DLL
ext-ms-win-gdi-path-l1-1-0.dll	6.3.9600.16384	ApiSet Stub DLL
ext-ms-win-gdi-private-l1-1-0.dll	6.3.9600.16384	ApiSet Stub DLL
ext-ms-win-gdi-render-l1-1-0.dll	6.3.9600.16384	ApiSet Stub DLL
ext-ms-win-gdi-wcs-l1-1-0.dll	6.3.9600.16384	ApiSet Stub DLL
ext-ms-win-globalization-collation-l1-1-0.dll	6.3.9600.16384	ApiSet Stub DLL
ext-ms-win-globalization-input-l1-1-0.dll	6.3.9600.16384	ApiSet Stub DLL
ext-ms-win-gpapi-grouppolicy-l1-1-0.dll	6.3.9600.16384	ApiSet Stub DLL
ext-ms-win-gpsvc-grouppolicy-l1-1-0.dll	6.3.9600.16384	ApiSet Stub DLL
ext-ms-win-gui-uxinit-l1-1-0.dll	6.3.9600.16384	ApiSet Stub DLL
ext-ms-win-imm-l1-1-0.dll	6.3.9600.16384	ApiSet Stub DLL
ext-ms-win-kernel32-appcompat-l1-1-0.dll	6.3.9600.16384	ApiSet Stub DLL
ext-ms-win-kernel32-datetime-l1-1-0.dll	6.3.9600.16384	ApiSet Stub DLL
ext-ms-win-kernel32-elevation-l1-1-0.dll	6.3.9600.16384	ApiSet Stub DLL
ext-ms-win-kernel32-errorhandling-l1-1-0.dll	6.3.9600.16384	ApiSet Stub DLL
ext-ms-win-kernel32-file-l1-1-0.dll	6.3.9600.16384	ApiSet Stub DLL
ext-ms-win-kernel32-localization-l1-1-0.dll	6.3.9600.16384	ApiSet Stub DLL
ext-ms-win-kernel32-package-current-l1-1-0.dll	6.3.9600.16384	ApiSet Stub DLL
ext-ms-win-kernel32-package-l1-1-0.dll	6.3.9600.16384	ApiSet Stub DLL
ext-ms-win-kernel32-package-l1-1-1.dll	6.3.9600.17031	ApiSet Stub DLL
ext-ms-win-kernel32-quirks-l1-1-0.dll	6.3.9600.16384	ApiSet Stub DLL
ext-ms-win-kernel32-registry-l1-1-0.dll	6.3.9600.16384	ApiSet Stub DLL
ext-ms-win-kernel32-sidebyside-l1-1-0.dll	6.3.9600.16384	ApiSet Stub DLL
ext-ms-win-kernel32-transacted-l1-1-0.dll	6.3.9600.16384	ApiSet Stub DLL
ext-ms-win-kernel32-windowserrorreporting-l1-1-0.dll	6.3.9600.16384	ApiSet Stub DLL
ext-ms-win-kernelbase-processthread-l1-1-0.dll	6.3.9600.16384	ApiSet Stub DLL
ext-ms-win-mm-msacm-l1-1-0.dll	6.3.9600.16384	ApiSet Stub DLL
ext-ms-win-mm-pehelper-l1-1-0.dll	6.3.9600.16384	ApiSet Stub DLL
ext-ms-win-mm-wmdrmsdk-l1-1-0.dll	6.3.9600.16384	ApiSet Stub DLL
ext-ms-win-mpr-multipleproviderrouter-l1-1-0.dll	6.3.9600.16384	ApiSet Stub DLL
ext-ms-win-mrmcorer-environment-l1-1-0.dll	6.3.9600.16384	ApiSet Stub DLL
ext-ms-win-mrmcorer-resmanager-l1-1-0.dll	6.3.9600.16384	ApiSet Stub DLL
ext-ms-win-msa-ui-l1-1-0.dll	6.3.9600.16384	ApiSet Stub DLL
ext-ms-win-msa-user-l1-1-0.dll	6.3.9600.16384	ApiSet Stub DLL
ext-ms-win-msiltcfg-msi-l1-1-0.dll	6.3.9600.16384	ApiSet Stub DLL

ext-ms-win-net-isoext-l1-1-0.dll	6.3.9600.16384	ApiSet Stub DLL
ext-ms-win-networking-wcmapi-l1-1-0.dll	6.3.9600.17031	ApiSet Stub DLL
ext-ms-win-networking-winipsec-l1-1-0.dll	6.3.9600.16384	ApiSet Stub DLL
ext-ms-win-networking-wlanapi-l1-1-0.dll	6.3.9600.16384	ApiSet Stub DLL
ext-ms-win-newdev-config-l1-1-0.dll	6.3.9600.16384	ApiSet Stub DLL
ext-ms-win-ntdsa-activedirectoryserver-l1-1-0.dll	6.3.9600.16384	ApiSet Stub DLL
ext-ms-win-ntdsapi-activedirectoryclient-l1-1-0.dll	6.3.9600.16384	ApiSet Stub DLL
ext-ms-win-ntos-kcminitcfg-l1-1-0.dll	6.3.9600.16384	ApiSet Stub DLL
ext-ms-win-ntos-ksecurity-l1-1-0.dll	6.3.9600.16384	ApiSet Stub DLL
ext-ms-win-ntos-ksecurity-l1-1-1.dll	6.3.9600.16384	ApiSet Stub DLL
ext-ms-win-ntos-ksigningpolicy-l1-1-0.dll	6.3.9600.16384	ApiSet Stub DLL
ext-ms-win-ntos-ksr-l1-1-0.dll	6.3.9600.16384	ApiSet Stub DLL
ext-ms-win-ntos-pico-l1-1-0.dll	6.3.9600.16384	ApiSet Stub DLL
ext-ms-win-ntos-tm-l1-1-0.dll	6.3.9600.16384	ApiSet Stub DLL
ext-ms-win-ntos-werkernel-l1-1-0.dll	6.3.9600.16384	ApiSet Stub DLL
ext-ms-win-ntuser-caret-l1-1-0.dll	6.3.9600.16384	ApiSet Stub DLL
ext-ms-win-ntuser-chartranslation-l1-1-0.dll	6.3.9600.16384	ApiSet Stub DLL
ext-ms-win-ntuser-dialogbox-l1-1-0.dll	6.3.9600.16384	ApiSet Stub DLL
ext-ms-win-ntuser-dialogbox-l1-1-1.dll	6.3.9600.16384	ApiSet Stub DLL
ext-ms-win-ntuser-draw-l1-1-0.dll	6.3.9600.16384	ApiSet Stub DLL
ext-ms-win-ntuser-draw-l1-1-1.dll	6.3.9600.16384	ApiSet Stub DLL
ext-ms-win-ntuser-gui-l1-1-0.dll	6.3.9600.16384	ApiSet Stub DLL
ext-ms-win-ntuser-gui-l1-1-1.dll	6.3.9600.16384	ApiSet Stub DLL
ext-ms-win-ntuser-keyboard-l1-1-0.dll	6.3.9600.16384	ApiSet Stub DLL
ext-ms-win-ntuser-keyboard-l1-1-1.dll	6.3.9600.16384	ApiSet Stub DLL
ext-ms-win-ntuser-menu-l1-1-0.dll	6.3.9600.16384	ApiSet Stub DLL
ext-ms-win-ntuser-menu-l1-1-1.dll	6.3.9600.16384	ApiSet Stub DLL
ext-ms-win-ntuser-message-l1-1-0.dll	6.3.9600.16384	ApiSet Stub DLL
ext-ms-win-ntuser-message-l1-1-1.dll	6.3.9600.16384	ApiSet Stub DLL
ext-ms-win-ntuser-misc-l1-1-0.dll	6.3.9600.16384	ApiSet Stub DLL
ext-ms-win-ntuser-misc-l1-2-0.dll	6.3.9600.16384	ApiSet Stub DLL
ext-ms-win-ntuser-mouse-l1-1-0.dll	6.3.9600.16384	ApiSet Stub DLL
ext-ms-win-ntuser-powermanagement-l1-1-0.dll	6.3.9600.16384	ApiSet Stub DLL
ext-ms-win-ntuser-private-l1-1-0.dll	6.3.9600.17031	ApiSet Stub DLL
ext-ms-win-ntuser-private-l1-1-1.dll	6.3.9600.17031	ApiSet Stub DLL
ext-ms-win-ntuser-rectangle-ext-l1-1-0.dll	6.3.9600.16384	ApiSet Stub DLL
ext-ms-win-ntuser-rotationmanager-l1-1-0.dll	6.3.9600.16384	ApiSet Stub DLL
ext-ms-win-ntuser-string-l1-1-0.dll	6.3.9600.16384	ApiSet Stub DLL
ext-ms-win-ntuser-synch-l1-1-0.dll	6.3.9600.16384	ApiSet Stub DLL
ext-ms-win-ntuser-touch-hittest-l1-1-0.dll	6.3.9600.16384	ApiSet Stub DLL
ext-ms-win-ntuser-windowclass-l1-1-0.dll	6.3.9600.16384	ApiSet Stub DLL
ext-ms-win-ntuser-windowclass-l1-1-1.dll	6.3.9600.16384	ApiSet Stub DLL
ext-ms-win-ntuser-window-l1-1-0.dll	6.3.9600.16384	ApiSet Stub DLL
ext-ms-win-ntuser-window-l1-1-1.dll	6.3.9600.16384	ApiSet Stub DLL
ext-ms-win-ntuser-windowstation-l1-1-0.dll	6.3.9600.16384	ApiSet Stub DLL
ext-ms-win-ntuser-windowstation-l1-1-1.dll	6.3.9600.16384	ApiSet Stub DLL
ext-ms-win-ole32-bindctx-l1-1-0.dll	6.3.9600.16384	ApiSet Stub DLL
ext-ms-win-ole32-ie-ext-l1-1-0.dll	6.3.9600.16384	ApiSet Stub DLL
ext-ms-win-ole32-oleautomation-l1-1-0.dll	6.3.9600.16384	ApiSet Stub DLL
ext-ms-win-oleacc-l1-1-0.dll	6.3.9600.16384	ApiSet Stub DLL
ext-ms-win-printer-winspool-l1-1-0.dll	6.3.9600.16384	ApiSet Stub DLL
ext-ms-win-printer-winspool-l1-1-1.dll	6.3.9600.16384	ApiSet Stub DLL
ext-ms-win-profile-profsvc-l1-1-0.dll	6.3.9600.16384	ApiSet Stub DLL
ext-ms-win-profile-userenv-l1-1-0.dll	6.3.9600.16384	ApiSet Stub DLL

ext-ms-win-ras-rasapi32-l1-1-0.dll	6.3.9600.16384	ApiSet Stub DLL
ext-ms-win-ras-rasdlg-l1-1-0.dll	6.3.9600.16384	ApiSet Stub DLL
ext-ms-win-ras-rasman-l1-1-0.dll	6.3.9600.16384	ApiSet Stub DLL
ext-ms-win-ras-tapi32-l1-1-0.dll	6.3.9600.16384	ApiSet Stub DLL
ext-ms-win-reinfo-query-l1-1-0.dll	6.3.9600.16384	ApiSet Stub DLL
ext-ms-win-rometadata-dispenser-l1-1-0.dll	6.3.9600.16384	ApiSet Stub DLL
ext-ms-win-rtcore-gdi-devcaps-l1-1-0.dll	6.3.9600.16384	ApiSet Stub DLL
ext-ms-win-rtcore-gdi-object-l1-1-0.dll	6.3.9600.16384	ApiSet Stub DLL
ext-ms-win-rtcore-gdi-rgn-l1-1-0.dll	6.3.9600.16384	ApiSet Stub DLL
ext-ms-win-rtcore-ntuser-dc-access-l1-1-0.dll	6.3.9600.16384	ApiSet Stub DLL
ext-ms-win-rtcore-ntuser-dpi-l1-1-0.dll	6.3.9600.16384	ApiSet Stub DLL
ext-ms-win-rtcore-ntuser-sysparams-l1-1-0.dll	6.3.9600.16384	ApiSet Stub DLL
ext-ms-win-samsrv-accountstore-l1-1-0.dll	6.3.9600.16384	ApiSet Stub DLL
ext-ms-win-scesrv-server-l1-1-0.dll	6.3.9600.16384	ApiSet Stub DLL
ext-ms-win-secur32-translatename-l1-1-0.dll	6.3.9600.16384	ApiSet Stub DLL
ext-ms-win-security-credui-l1-1-0.dll	6.3.9600.16384	ApiSet Stub DLL
ext-ms-win-security-cryptui-l1-1-0.dll	6.3.9600.16384	ApiSet Stub DLL
ext-ms-win-security-kerberos-l1-1-0.dll	6.3.9600.16384	ApiSet Stub DLL
ext-ms-win-security-vaultcli-l1-1-0.dll	6.3.9600.16384	ApiSet Stub DLL
ext-ms-win-session-userinit-l1-1-0.dll	6.3.9600.16384	ApiSet Stub DLL
ext-ms-win-session-usertoken-l1-1-0.dll	6.3.9600.16384	ApiSet Stub DLL
ext-ms-win-session-wininit-l1-1-0.dll	6.3.9600.16384	ApiSet Stub DLL
ext-ms-win-session-winlogon-l1-1-0.dll	6.3.9600.16384	ApiSet Stub DLL
ext-ms-win-session-winsta-l1-1-0.dll	6.3.9600.17031	ApiSet Stub DLL
ext-ms-win-session-wtsapi32-l1-1-0.dll	6.3.9600.16384	ApiSet Stub DLL
ext-ms-win-setupapi-cfgmgr32remote-l1-1-0.dll	6.3.9600.16384	ApiSet Stub DLL
ext-ms-win-setupapi-classinstallers-l1-1-0.dll	6.3.9600.16384	ApiSet Stub DLL
ext-ms-win-setupapi-inf-l1-1-0.dll	6.3.9600.16384	ApiSet Stub DLL
ext-ms-win-setupapi-logging-l1-1-0.dll	6.3.9600.16384	ApiSet Stub DLL
ext-ms-win-shell32-shellcom-l1-1-0.dll	6.3.9600.16384	ApiSet Stub DLL
ext-ms-win-shell32-shellfolders-l1-1-0.dll	6.3.9600.16384	ApiSet Stub DLL
ext-ms-win-shell-propsys-l1-1-0.dll	6.3.9600.16384	ApiSet Stub DLL
ext-ms-win-shell-settingsync-l1-1-0.dll	6.3.9600.16384	ApiSet Stub DLL
ext-ms-win-shell-shell32-l1-2-0.dll	6.3.9600.16384	ApiSet Stub DLL
ext-ms-win-shell-shlwapi-l1-1-0.dll	6.3.9600.16384	ApiSet Stub DLL
ext-ms-win-smbshare-browser-l1-1-0.dll	6.3.9600.16384	ApiSet Stub DLL
ext-ms-win-smbshare-sscore-l1-1-0.dll	6.3.9600.16384	ApiSet Stub DLL
ext-ms-win-spinf-inf-l1-1-0.dll	6.3.9600.16384	ApiSet Stub DLL
ext-ms-win-storage-iscsidsc-l1-1-0.dll	6.3.9600.16384	ApiSet Stub DLL
ext-ms-win-sxs-oleautomation-l1-1-0.dll	6.3.9600.16384	ApiSet Stub DLL
ext-ms-win-uiacore-l1-1-0.dll	6.3.9600.16384	ApiSet Stub DLL
ext-ms-win-umpoext-umpo-l1-1-0.dll	6.3.9600.16384	ApiSet Stub DLL
ext-ms-win-usp10-l1-1-0.dll	6.3.9600.16384	ApiSet Stub DLL
ext-ms-win-uxtheme-themes-l1-1-0.dll	6.3.9600.16384	ApiSet Stub DLL
ext-ms-win-webio-pal-l1-1-0.dll	6.3.9600.16384	ApiSet Stub DLL
ext-ms-win-wer-reporting-l1-1-0.dll	6.3.9600.16384	ApiSet Stub DLL
ext-ms-win-wevtapi-eventlog-l1-1-0.dll	6.3.9600.16384	ApiSet Stub DLL
ext-ms-win-winbici-l1-1-0.dll	6.3.9600.16384	ApiSet Stub DLL
ext-ms-win-winhttp-pal-l1-1-0.dll	6.3.9600.16384	ApiSet Stub DLL
ext-ms-win-wininet-pal-l1-1-0.dll	6.3.9600.16384	ApiSet Stub DLL
ext-ms-win-winlogon-mincreds-l1-1-0.dll	6.3.9600.16384	ApiSet Stub DLL
ext-ms-win-winrt-storage-l1-1-0.dll	6.3.9600.16384	ApiSet Stub DLL
ext-ms-win-wlan-grouppolicy-l1-1-0.dll	6.3.9600.16384	ApiSet Stub DLL
ext-ms-win-wlan-onexui-l1-1-0.dll	6.3.9600.16384	ApiSet Stub DLL

ext-ms-win-wlan-scard-l1-1-0.dll	6.3.9600.16384	ApiSet Stub DLL
ext-ms-win-wsclient-devlicense-l1-1-0.dll	6.3.9600.16384	ApiSet Stub DLL
ext-ms-win-wwan-wwapi-l1-1-0.dll	6.3.9600.16384	ApiSet Stub DLL
ext-ms-win-xaml-controls-l1-1-0.dll	6.3.9600.16384	ApiSet Stub DLL
ext-ms-win-xaml-pal-l1-1-0.dll	6.3.9600.16384	ApiSet Stub DLL
f3ahvoas.dll	6.3.9600.17031	JP Japanese Keyboard Layout for Fujitsu FMV oyayubi-shift keyboard
faultrep.dll	6.3.9600.17550	Windows User Mode Crash Reporting DLL
fdbth.dll	6.3.9600.17415	Function Discovery Bluetooth Provider Dll
fdbthproxy.dll	6.3.9600.17415	Bluetooth Provider Proxy Dll
fddevquery.dll	6.3.9600.17415	Microsoft Windows Device Query Helper
fde.dll	6.3.9600.17415	Folder Redirection Snapin Extension
fdeploy.dll	6.3.9600.17415	Folder Redirection Group Policy Extension
fdpnp.dll	6.3.9600.17415	Pnp Provider Dll
fdprint.dll	6.3.9600.17415	Function Discovery Print Provider Dll
fdproxy.dll	6.3.9600.17415	Function Discovery Proxy Dll
fdssdp.dll	6.3.9600.17415	Function Discovery SSDP Provider Dll
fdwcn.dll	6.3.9600.17415	Windows Connect Now - Config Function Discovery Provider DLL
fdwnet.dll	6.3.9600.17415	Function Discovery WNet Provider Dll
fdwsd.dll	6.3.9600.17415	Function Discovery WS Discovery Provider Dll
feclient.dll	6.3.9600.17415	Windows NT File Encryption Client Interfaces
filemgmt.dll	6.3.9600.17415	Services and Shared Folders
findnetprinters.dll	6.3.9600.17415	Find Network Printers COM Component
firewallapi.dll	6.3.9600.17415	Windows Firewall API
firewallcontrolpanel.dll	6.3.9600.17415	Windows Firewall Control Panel
fltlib.dll	6.3.9600.17415	Filter Library
fmifs.dll	6.3.9600.17415	FM IFS Utility DLL
fms.dll	6.3.9600.17415	Font Management Services
fontext.dll	6.3.9600.17415	Windows Font Folder
fontsub.dll	6.3.9600.17415	Font Subsetting DLL
fphc.dll	6.3.9600.17415	Filtering Platform Helper Class
framedyn.dll	6.3.9600.17415	WMI SDK Provider Framework
framedynos.dll	6.3.9600.17415	WMI SDK Provider Framework
frprov.dll	6.3.9600.17415	Folder Redirection WMI Provider
fsutilext.dll	6.3.9600.17415	FS Utility Extension DLL
fundisc.dll	6.3.9600.17415	Function Discovery Dll
fwcfg.dll	6.3.9600.17415	Windows Firewall Configuration Helper
fwpuclnt.dll	6.3.9600.17485	FWP/IPsec User-Mode API
fwremotesvr.dll	6.3.9600.17415	Windows Firewall Remote APIs Server
fxsapi.dll	6.3.9600.17415	Microsoft Fax API Support DLL
fxscom.dll	6.3.9600.17415	Microsoft Fax Server COM Client Interface
fxscomex.dll	6.3.9600.17415	Microsoft Fax Server Extended COM Client Interface
fxsext32.dll	6.3.9600.17415	Microsoft Fax Exchange Command Extension
fxsresm.dll	6.3.9600.16384	Microsoft Fax Resource DLL
fxsxp32.dll	6.3.9600.17415	Microsoft Fax Transport Provider
gameux.dll	6.3.9600.17415	Games Explorer
gameuxlegacygdfs.dll	1.0.0.1	Legacy GDF resource DLL
gcdef.dll	6.3.9600.17415	Game Controllers Default Sheets
gdi32.dll	6.3.9600.17415	GDI Client DLL
gdiplus.dll	6.3.9600.17415	Microsoft GDI+
geofencemonitorservice.dll	6.3.9600.17415	Windows Location Framework Service
getuname.dll	6.3.9600.17415	Unicode name Dll for UCE
glcndfilter.dll	6.3.9600.17415	glcndFilter DLL
glmf32.dll	6.3.9600.17415	OpenGL Metafiling DLL
globcollationhost.dll	6.3.9600.17415	GlobCollationHost

globinputhost.dll	6.3.9600.17415	Windows Globalization Extension API for Input
glu32.dll	6.3.9600.17415	OpenGL Utility Library DLL
gpapi.dll	6.3.9600.17415	Group Policy Client API
gpedit.dll	6.3.9600.17415	GPEdit
gpprefcl.dll	6.3.9600.17415	Group Policy Preference Client
gpprnext.dll	6.3.9600.17415	Group Policy Printer Extension
gpscript.dll	6.3.9600.17415	Script Client Side Extension
gptext.dll	6.3.9600.17415	GPTExt
hbaapi.dll	6.3.9600.17415	HBA API data interface dll for HBA_API_Rev_2-18_2002MAR1.doc
hcproviders.dll	6.3.9600.17415	Action Center Providers
helppaneproxy.dll	6.3.9600.17415	Microsoft® Help Proxy
hgcpl.dll	6.3.9600.17415	HomeGroup Control Panel
hhsetup.dll	6.3.9600.17415	Microsoft® HTML Help
hid.dll	6.3.9600.17415	Hid User Library
hidserv.dll	6.3.9600.17415	Human Interface Device Service
hlink.dll	6.3.9600.17416	Microsoft Office 2000 component
hnetcfg.dll	6.3.9600.17415	Home Networking Configuration Manager
hnetmon.dll	6.3.9600.17415	Home Networking Monitor DLL
httpapi.dll	6.3.9600.17415	HTTP Protocol Stack API
htui.dll	6.3.9600.17415	Common halftone Color Adjustment Dialogs
ias.dll	6.3.9600.17415	Network Policy Server
iasacct.dll	6.3.9600.17415	NPS Accounting Provider
iasads.dll	6.3.9600.17415	NPS Active Directory Data Store
iasdatastore.dll	6.3.9600.17415	NPS Datastore server
iashlpr.dll	6.3.9600.17415	NPS Surrogate Component
iasmigplugin.dll	6.3.9600.17415	NPS Migration DLL
iasnap.dll	6.3.9600.17415	NPS NAP Provider
iaspolcy.dll	6.3.9600.17415	NPS Pipeline
iasrad.dll	6.3.9600.17415	NPS RADIUS Protocol Component
iasrecst.dll	6.3.9600.17415	NPS XML Datastore Access
iassam.dll	6.3.9600.17415	NPS NT SAM Provider
iassdo.dll	6.3.9600.17415	NPS SDO Component
iassvcs.dll	6.3.9600.17415	NPS Services Component
iccvid.dll	1.10.0.12	Cinepak® Codec
icm32.dll	6.3.9600.17415	Microsoft Color Management Module (CMM)
icmp.dll	6.3.9600.16384	ICMP DLL
icmui.dll	6.3.9600.17415	Microsoft Color Matching System User Interface DLL
iconcodecservice.dll	6.3.9600.17415	Converts a PNG part of the icon to a legacy bmp icon
icsigd.dll	6.3.9600.17415	Internet Gateway Device properties
idctrls.dll	6.3.9600.17415	Identity Controls
idndl.dll	6.3.9600.17415	Downlevel DLL
idstore.dll	6.3.9600.17415	Identity Store
ieadvpack.dll	11.0.9600.17416	ADVPACK
ieapfltr.dll	11.0.9600.17728	Microsoft SmartScreen Filter
iedkcs32.dll	18.0.9600.17631	IEAK branding
ieetwproxystub.dll	11.0.9600.17416	IE ETW Collector Proxy Stub Resources
ieframe.dll	11.0.9600.17728	Internet Browser
iepeers.dll	11.0.9600.17690	Internet Explorer Peer Objects
iernonce.dll	11.0.9600.17416	Extended RunOnce processing with UI
iertutil.dll	11.0.9600.17728	Run time utility for Internet Explorer
iesetup.dll	11.0.9600.17416	IOD Version Map
iesysprep.dll	11.0.9600.17416	IE Sysprep Provider
ieui.dll	11.0.9600.17416	Internet Explorer UI Engine
ifmon.dll	6.3.9600.17415	IF Monitor DLL

ifsutil.dll	6.3.9600.17415	IFS Utility DLL
ifsutilx.dll	6.3.9600.17415	IFS Utility Extension DLL
ig4icd32.dll	9.17.10.4101	OpenGL(R) Driver for Intel(R) Graphics Accelerator
ig7icd32.dll	10.18.10.3958	OpenGL(R) Driver for Intel(R) Graphics Accelerator
igd10iumd32.dll	10.18.10.3958	User Mode Driver for Intel(R) Graphics Technology
igd10umd32.dll	9.17.10.4101	LDDM User Mode Driver for Intel(R) Graphics Technology
igdail32.dll		
igdbcl32.dll	10.18.10.3958	OpenCL User Mode Driver for Intel(R) Graphics Technology
igdde32.dll		
igdfcl32.dll	10.18.10.3958	OpenCL User Mode Driver for Intel(R) Graphics Technology
igdmd32.dll	10.18.10.3958	Metrics Discovery API for Intel(R) Graphics Accelerator
igdrcl32.dll	10.18.10.3958	OpenCL User Mode Driver for Intel(R) Graphics Technology
igdumd32.dll	9.17.10.4101	LDDM User Mode Driver for Intel(R) Graphics Technology
igdumdim32.dll	10.18.10.3958	User Mode Driver for Intel(R) Graphics Technology
igdusc32.dll	10.18.10.3958	Unified Shader Compiler for Intel(R) Graphics Accelerator
igfx11cmrt32.dll	3.0.0.1248	MDF(CM) Runtime DX11 Dynamic Link Library
igfxcmjit32.dll	3.0.0.1248	MDF(CM) JIT Dynamic Link Library
igfxcmrt32.dll	3.0.0.1248	MDF(CM) Runtime Dynamic Link Library
igfxdv32.dll	8.15.10.4101	igfxdev Module
igfxexps32.dll	6.15.10.3958	igfxext Module
iglhcp32.dll	9.0.20.9000	iglhcp32 Dynamic Link Library
iglhsip32.dll	9.0.20.9000	iglhsip32 Dynamic Link Library
imagehlp.dll	6.3.9600.17415	Windows NT Image Helper
imageres.dll	6.3.9600.16384	Windows Image Resource
imagesp1.dll	6.3.9600.16384	Windows SP1 Image Resource
imapi.dll	6.3.9600.17415	Image Mastering API
imapi2.dll	6.3.9600.17415	Image Mastering API v2
imapi2fs.dll	6.3.9600.17415	Image Mastering File System Imaging API v2
imgutil.dll	11.0.9600.17416	IE plugin image decoder support DLL
imm32.dll	6.3.9600.17415	Multi-User Windows IMM32 API Client DLL
inetcomm.dll	6.3.9600.17728	Microsoft Internet Messaging API Resources
inetmib1.dll	6.3.9600.17415	Microsoft MIB-II subagent
inetres.dll	6.3.9600.16384	Microsoft Internet Messaging API Resources
inked.dll	6.3.9600.17415	Microsoft Tablet PC InkEdit Control
input.dll	6.3.9600.17415	InputSetting DLL
inputswitch.dll	6.3.9600.17415	Microsoft Windows Input Switcher
inseng.dll	11.0.9600.17416	Install engine
intel_opencl_icd32.dll	1.2.11.0	OpenCL Client DLL
intelopencl32.dll	10.18.10.3958	Intel(R) OpenCL(TM) Common Runtime Driver
iologmsg.dll	6.3.9600.16384	IO Logging DLL
iphlpapi.dll	6.3.9600.17415	IP Helper API
iprop.dll	6.3.9600.17415	OLE PropertySet Implementation
iprtprio.dll	6.3.9600.17415	IP Routing Protocol Priority DLL
iprtrmgr.dll	6.3.9600.17415	IP Router Manager
ipsecsnp.dll	6.3.9600.17415	IP Security Policy Management Snap-in
ipsmsnap.dll	6.3.9600.17415	IP Security Monitor Snap-in
ir32_32.dll	6.3.9600.17415	IR32_32 WRAPPER DLL
ir32_32original.dll	3.24.15.3	Intel Indeo(R) Video R3.2 32-bit Driver
ir41_32original.dll	4.51.16.3	Intel Indeo® Video 4.5
ir41_qc.dll	6.3.9600.17415	IR41_QC WRAPPER DLL
ir41_qcoriginal.dll	4.30.62.2	Intel Indeo® Video Interactive Quick Compressor
ir41_qcx.dll	6.3.9600.17415	IR41_QCX WRAPPER DLL
ir41_qcxoriginal.dll	4.30.64.1	Intel Indeo® Video Interactive Quick Compressor
ir50_32.dll	6.3.9600.17415	IR50_32 WRAPPER DLL

ir50_32original.dll	5.2562.15.55	Intel Indeo® video 5.10
ir50_qc.dll	6.3.9600.17415	IR50_QC WRAPPER DLL
ir50_qcoriginal.dll	5.0.63.48	Intel Indeo® video 5.10 Quick Compressor
ir50_qcx.dll	6.3.9600.17415	IR50_QCX WRAPPER DLL
ir50_qcxoriginal.dll	5.0.64.48	Intel Indeo® video 5.10 Quick Compressor
irclass.dll	6.3.9600.17415	Infrared Class Coinstaller
iscsicpl.dll	5.2.3790.1830	iSCSI Initiator Control Panel Applet
iscsidsc.dll	6.3.9600.17415	iSCSI Discovery api
iscsied.dll	6.3.9600.17415	iSCSI Extension DLL
iscsium.dll	6.3.9600.17415	iSCSI Discovery api
iscsiwmi.dll	6.3.9600.17415	MS iSCSI Initiator WMI Provider
iscsiwmiv2.dll	6.3.9600.17415	WMI Provider for iSCSI
itircl.dll	6.3.9600.17415	Microsoft® InfoTech IR Local DLL
itss.dll	6.3.9600.17415	Microsoft® InfoTech Storage System Library
iyuv_32.dll	6.3.9600.17415	Intel Indeo(R) Video YUV Codec
javascriptcollectionagent.dll	11.0.9600.17416	JavaScript Performance Collection Agent
jscript.dll	5.8.9600.17728	Microsoft ® JScript
jscript9.dll	11.0.9600.17728	Microsoft ® JScript
jscript9diag.dll	11.0.9600.17416	Microsoft ® JScript Diagnostics
jsproxy.dll	11.0.9600.17416	JScript Proxy Auto-Configuration
kbd101.dll	6.3.9600.16384	JP Japanese Keyboard Layout for 101
kbd101a.dll	6.3.9600.16384	KO Hangeul Keyboard Layout for 101 (Type A)
kbd101b.dll	6.3.9600.16384	KO Hangeul Keyboard Layout for 101(Type B)
kbd101c.dll	6.3.9600.16384	KO Hangeul Keyboard Layout for 101(Type C)
kbd103.dll	6.3.9600.16384	KO Hangeul Keyboard Layout for 103
kbd106.dll	6.3.9600.16384	JP Japanese Keyboard Layout for 106
kbd106n.dll	6.3.9600.16384	JP Japanese Keyboard Layout for 106
kbda1.dll	6.3.9600.16384	Arabic_English_101 Keyboard Layout
kbda2.dll	6.3.9600.16384	Arabic_2 Keyboard Layout
kbda3.dll	6.3.9600.16384	Arabic_French_102 Keyboard Layout
kbdal.dll	6.3.9600.16384	Albania Keyboard Layout
kbdarme.dll	6.3.9600.16384	Eastern Armenian Keyboard Layout
kbdarmph.dll	6.3.9600.16384	Armenian Phonetic Keyboard Layout
kbdarmty.dll	6.3.9600.16384	Armenian Typewriter Keyboard Layout
kbdarmw.dll	6.3.9600.16384	Western Armenian Keyboard Layout
kbdax2.dll	6.3.9600.16384	JP Japanese Keyboard Layout for AX2
kbdaze.dll	6.3.9600.16384	Azerbaijan_Cyrillic Keyboard Layout
kbdazel.dll	6.3.9600.16384	Azeri-Latin Keyboard Layout
kbdazst.dll	6.3.9600.16384	Azerbaijani (Standard) Keyboard Layout
kbdbash.dll	6.3.9600.17238	Bashkir Keyboard Layout
kbdbe.dll	6.3.9600.16384	Belgian Keyboard Layout
kbdbene.dll	6.3.9600.16384	Belgian Dutch Keyboard Layout
kbdbgph.dll	6.3.9600.16384	Bulgarian Phonetic Keyboard Layout
kbdbgph1.dll	6.3.9600.16384	Bulgarian (Phonetic Traditional) Keyboard Layout
kbdbhc.dll	6.3.9600.16384	Bosnian (Cyrillic) Keyboard Layout
kbdblr.dll	6.3.9600.16384	Belarusian Keyboard Layout
kbdbr.dll	6.3.9600.16384	Brazilian Keyboard Layout
kbdbu.dll	6.3.9600.16384	Bulgarian (Typewriter) Keyboard Layout
kbdbug.dll	6.3.9600.16384	Buginese Keyboard Layout
kbdbulg.dll	6.3.9600.16384	Bulgarian Keyboard Layout
kbdca.dll	6.3.9600.16384	Canadian Multilingual Keyboard Layout
kbdcan.dll	6.3.9600.16384	Canadian Multilingual Standard Keyboard Layout
kbdcher.dll	6.3.9600.16384	Cherokee Nation Keyboard Layout
kbdcherp.dll	6.3.9600.16384	Cherokee Phonetic Keyboard Layout

kbdcr.dll	6.3.9600.16384	Croatian/Slovenian Keyboard Layout
kbdcz.dll	6.3.9600.16384	Czech Keyboard Layout
kbdcz1.dll	6.3.9600.16384	Czech_101 Keyboard Layout
kbdcz2.dll	6.3.9600.16384	Czech_Programmer's Keyboard Layout
kbdda.dll	6.3.9600.16384	Danish Keyboard Layout
kbddiv1.dll	6.3.9600.16384	Divehi Phonetic Keyboard Layout
kbddiv2.dll	6.3.9600.16384	Divehi Typewriter Keyboard Layout
kbddv.dll	6.3.9600.16384	Dvorak US English Keyboard Layout
kbdes.dll	6.3.9600.16384	Spanish Alernate Keyboard Layout
kbdest.dll	6.3.9600.16384	Estonia Keyboard Layout
kbdfa.dll	6.3.9600.16384	Persian Keyboard Layout
kbdfar.dll	6.3.9600.16384	Persian Standard Keyboard Layout
kbdfc.dll	6.3.9600.16384	Canadian French Keyboard Layout
kbdfi.dll	6.3.9600.16384	Finnish Keyboard Layout
kbdfi1.dll	6.3.9600.16384	Finnish-Swedish with Sami Keyboard Layout
kbdfo.dll	6.3.9600.16384	Færoese Keyboard Layout
kbdfr.dll	6.3.9600.16384	French Keyboard Layout
kbdfthrk.dll	6.3.9600.16384	Futhark Keyboard Layout
kbdgae.dll	6.3.9600.16384	Scottish Gaelic (United Kingdom) Keyboard Layout
kbdgeo.dll	6.3.9600.16384	Georgian Keyboard Layout
kbdgeoer.dll	6.3.9600.16384	Georgian (Ergonomic) Keyboard Layout
kbdgeome.dll	6.3.9600.16384	Georgian (MES) Keyboard Layout
kbdgeooa.dll	6.3.9600.16384	Georgian (Old Alphabets) Keyboard Layout
kbdgeoqw.dll	6.3.9600.16384	Georgian (QWERTY) Keyboard Layout
kbdgkl.dll	6.3.9600.16384	Greek_Latin Keyboard Layout
kbdgn.dll	6.3.9600.16384	Guarani Keyboard Layout
kbdgr.dll	6.3.9600.16384	German Keyboard Layout
kbdgr1.dll	6.3.9600.16384	German_IBM Keyboard Layout
kbdgrlnd.dll	6.3.9600.16384	Greenlandic Keyboard Layout
kbdgthc.dll	6.3.9600.16384	Gothic Keyboard Layout
kbdhau.dll	6.3.9600.16384	Hausa Keyboard Layout
kbdhaw.dll	6.3.9600.16384	Hawaiian Keyboard Layout
kbdhe.dll	6.3.9600.16384	Greek Keyboard Layout
kbdhe220.dll	6.3.9600.16384	Greek IBM 220 Keyboard Layout
kbdhe319.dll	6.3.9600.16384	Greek IBM 319 Keyboard Layout
kbdheb.dll	6.3.9600.16384	KBDHEB Keyboard Layout
kbdhebl3.dll	6.3.9600.16384	Hebrew Standard Keyboard Layout
kbdhela2.dll	6.3.9600.16384	Greek IBM 220 Latin Keyboard Layout
kbdhela3.dll	6.3.9600.16384	Greek IBM 319 Latin Keyboard Layout
kbdhept.dll	6.3.9600.16384	Greek_Polytonic Keyboard Layout
kbdhu.dll	6.3.9600.16384	Hungarian Keyboard Layout
kbdhu1.dll	6.3.9600.16384	Hungarian 101-key Keyboard Layout
kbdibm02.dll	6.3.9600.16384	JP Japanese Keyboard Layout for IBM 5576-002/003
kbdibo.dll	6.3.9600.16384	Igbo Keyboard Layout
kbdic.dll	6.3.9600.16384	Icelandic Keyboard Layout
kbdinasa.dll	6.3.9600.16384	Assamese (Inscript) Keyboard Layout
kbdinbe1.dll	6.3.9600.16384	Bengali - Inscript (Legacy) Keyboard Layout
kbdinbe2.dll	6.3.9600.16384	Bengali (Inscript) Keyboard Layout
kbdinben.dll	6.3.9600.16384	Bengali Keyboard Layout
kbdindev.dll	6.3.9600.16384	Devanagari Keyboard Layout
kbdinen.dll	6.3.9600.16384	English - India Keyboard Layout
kbdinguj.dll	6.3.9600.16384	Gujarati Keyboard Layout
kbdinhin.dll	6.3.9600.16384	Hindi Keyboard Layout
kbdinkan.dll	6.3.9600.16384	Kannada Keyboard Layout

kbdinmal.dll	6.3.9600.16384	Malayalam Keyboard Layout Keyboard Layout
kbdinmar.dll	6.3.9600.16384	Marathi Keyboard Layout
kbdinori.dll	6.3.9600.16384	Odia Keyboard Layout
kbdinpun.dll	6.3.9600.16384	Punjabi/Gurmukhi Keyboard Layout
kbdintam.dll	6.3.9600.16384	Tamil Keyboard Layout
kbdintel.dll	6.3.9600.16384	Telugu Keyboard Layout
kbdinuk2.dll	6.3.9600.16384	Inuktitut Naqittaut Keyboard Layout
kbdir.dll	6.3.9600.16384	Irish Keyboard Layout
kbdit.dll	6.3.9600.16384	Italian Keyboard Layout
kbdit142.dll	6.3.9600.16384	Italian 142 Keyboard Layout
kbdiulat.dll	6.3.9600.16384	Inuktitut Latin Keyboard Layout
kbdjav.dll	6.3.9600.16384	Javanese Keyboard Layout
kbdjpn.dll	6.3.9600.16384	JP Japanese Keyboard Layout Stub driver
kbdkaz.dll	6.3.9600.16384	Kazak_Cyrillic Keyboard Layout
kbdkhmr.dll	6.3.9600.16384	Cambodian Standard Keyboard Layout
kbdkni.dll	6.3.9600.16384	Khmer (NIDA) Keyboard Layout
kbdkor.dll	6.3.9600.16384	KO Hangeul Keyboard Layout Stub driver
kbdkurd.dll	6.3.9600.16384	Central Kurdish Keyboard Layout
kbdkyr.dll	6.3.9600.16384	Kyrgyz Keyboard Layout
kbdla.dll	6.3.9600.16384	Latin-American Spanish Keyboard Layout
kbdlao.dll	6.3.9600.16384	Lao Standard Keyboard Layout
kbdlisub.dll	6.3.9600.16384	Lisu Basic Keyboard Layout
kbdlisus.dll	6.3.9600.16384	Lisu Standard Keyboard Layout
kbdlk41a.dll	6.3.9600.16384	DEC LK411-AJ Keyboard Layout
kbdlt.dll	6.3.9600.16384	Lithuania Keyboard Layout
kbdlt1.dll	6.3.9600.16384	Lithuanian Keyboard Layout
kbdlt2.dll	6.3.9600.16384	Lithuanian Standard Keyboard Layout
kbdlv.dll	6.3.9600.16384	Latvia Keyboard Layout
kbdlv1.dll	6.3.9600.16384	Latvia-QWERTY Keyboard Layout
kbdlvst.dll	6.3.9600.16384	Latvian (Standard) Keyboard Layout
kbdmac.dll	6.3.9600.16384	Macedonian (FYROM) Keyboard Layout
kbdmacst.dll	6.3.9600.16384	Macedonian (FYROM) - Standard Keyboard Layout
kbdmaori.dll	6.3.9600.16384	Maori Keyboard Layout
kbdmlt47.dll	6.3.9600.16384	Maltese 47-key Keyboard Layout
kbdmlt48.dll	6.3.9600.16384	Maltese 48-key Keyboard Layout
kbdmon.dll	6.3.9600.16384	Mongolian Keyboard Layout
kbdmonmo.dll	6.3.9600.16384	Mongolian (Mongolian Script) Keyboard Layout
kbdmonst.dll	6.3.9600.16384	Traditional Mongolian (Standard) Keyboard Layout
kbdmyan.dll	6.3.9600.16384	Myanmar Keyboard Layout
kbdne.dll	6.3.9600.16384	Dutch Keyboard Layout
kbdnec.dll	6.3.9600.16384	JP Japanese Keyboard Layout for (NEC PC-9800)
kbdnec95.dll	6.3.9600.16384	JP Japanese Keyboard Layout for (NEC PC-9800 Windows 95)
kbdnecat.dll	6.3.9600.16384	JP Japanese Keyboard Layout for (NEC PC-9800 on PC98-NX)
kbdnecnt.dll	6.3.9600.16384	JP Japanese NEC PC-9800 Keyboard Layout
kbdnepr.dll	6.3.9600.16384	Nepali Keyboard Layout
kbdnko.dll	6.3.9600.16384	N'Ko Keyboard Layout
kbdno.dll	6.3.9600.16384	Norwegian Keyboard Layout
kbdno1.dll	6.3.9600.16384	Norwegian with Sami Keyboard Layout
kbdnso.dll	6.3.9600.16384	Sesotho sa Leboa Keyboard Layout
kbdntl.dll	6.3.9600.16384	New Tai Leu Keyboard Layout
kbdogham.dll	6.3.9600.16384	Ogham Keyboard Layout
kbdolch.dll	6.3.9600.16384	Ol Chiki Keyboard Layout
kbdoldit.dll	6.3.9600.16384	Old Italic Keyboard Layout
kbdosm.dll	6.3.9600.16384	Osmanya Keyboard Layout

kbdpash.dll	6.3.9600.16384	Pashto (Afghanistan) Keyboard Layout
kbdphags.dll	6.3.9600.16384	Phags-pa Keyboard Layout
kbdpl.dll	6.3.9600.16384	Polish Keyboard Layout
kbdpl1.dll	6.3.9600.16384	Polish Programmer's Keyboard Layout
kbdpo.dll	6.3.9600.16384	Portuguese Keyboard Layout
kbdro.dll	6.3.9600.16384	Romanian (Legacy) Keyboard Layout
kbdropr.dll	6.3.9600.16384	Romanian (Programmers) Keyboard Layout
kbdrost.dll	6.3.9600.16384	Romanian (Standard) Keyboard Layout
kbdru.dll	6.3.9600.17238	Russian Keyboard Layout
kbdru1.dll	6.3.9600.17238	Russia(Typewriter) Keyboard Layout
kbdrum.dll	6.3.9600.17238	Russian - Mnemonic Keyboard Layout
kbdsf.dll	6.3.9600.16384	Swiss French Keyboard Layout
kbdsg.dll	6.3.9600.16384	Swiss German Keyboard Layout
kbdsl.dll	6.3.9600.16384	Slovak Keyboard Layout
kbdsl1.dll	6.3.9600.16384	Slovak(QWERTY) Keyboard Layout
kbdsmsfi.dll	6.3.9600.16384	Sami Extended Finland-Sweden Keyboard Layout
kbdsmsno.dll	6.3.9600.16384	Sami Extended Norway Keyboard Layout
kbdsn1.dll	6.3.9600.16384	Sinhala Keyboard Layout
kbdsora.dll	6.3.9600.16384	Sora Keyboard Layout
kbdsorex.dll	6.3.9600.16384	Sorbian Extended Keyboard Layout
kbdsors1.dll	6.3.9600.16384	Sorbian Standard Keyboard Layout
kbdsorst.dll	6.3.9600.16384	Sorbian Standard (Legacy) Keyboard Layout
kbdsp.dll	6.3.9600.16384	Spanish Keyboard Layout
kbdsw.dll	6.3.9600.16384	Swedish Keyboard Layout
kbdsw09.dll	6.3.9600.16384	Sinhala - Wij 9 Keyboard Layout
kbdsyr1.dll	6.3.9600.16384	Syriac Standard Keyboard Layout
kbdsyr2.dll	6.3.9600.16384	Syriac Phoenetic Keyboard Layout
kbdtaile.dll	6.3.9600.16384	Tai Le Keyboard Layout
kbdtajik.dll	6.3.9600.16384	Tajik Keyboard Layout
kbdtat.dll	6.3.9600.17238	Tatar (Legacy) Keyboard Layout
kbdth0.dll	6.3.9600.16384	Thai Kedmanee Keyboard Layout
kbdth1.dll	6.3.9600.16384	Thai Pattachote Keyboard Layout
kbdth2.dll	6.3.9600.16384	Thai Kedmanee (non-ShiftLock) Keyboard Layout
kbdth3.dll	6.3.9600.16384	Thai Pattachote (non-ShiftLock) Keyboard Layout
kbdtifi.dll	6.3.9600.16384	Tifinagh (Basic) Keyboard Layout
kbdtifi2.dll	6.3.9600.16384	Tifinagh (Extended) Keyboard Layout
kbdtiprc.dll	6.3.9600.16384	Tibetan (PRC) Keyboard Layout
kbdtiprd.dll	6.3.9600.16384	Tibetan (PRC) - Updated Keyboard Layout
kbdtt102.dll	6.3.9600.17238	Tatar Keyboard Layout
kbdtuf.dll	6.3.9600.16384	Turkish F Keyboard Layout
kbdtuq.dll	6.3.9600.16384	Turkish Q Keyboard Layout
kbdturme.dll	6.3.9600.16384	Turkmen Keyboard Layout
kbdtzm.dll	6.3.9600.16384	Central Atlas Tamazight Keyboard Layout
kbdughr.dll	6.3.9600.16384	Uyghur (Legacy) Keyboard Layout
kbdughr1.dll	6.3.9600.16384	Uyghur Keyboard Layout
kbduk.dll	6.3.9600.16384	United Kingdom Keyboard Layout
kbdukx.dll	6.3.9600.16384	United Kingdom Extended Keyboard Layout
kbdur.dll	6.3.9600.16384	Ukrainian Keyboard Layout
kbdur1.dll	6.3.9600.16384	Ukrainian (Enhanced) Keyboard Layout
kbdurdu.dll	6.3.9600.16384	Urdu Keyboard Layout
kbdus.dll	6.3.9600.16384	United States Keyboard Layout
kbdusa.dll	6.3.9600.16384	US IBM Arabic 238_L Keyboard Layout
kbdusl.dll	6.3.9600.16384	Dvorak Left-Hand US English Keyboard Layout
kbdusr.dll	6.3.9600.16384	Dvorak Right-Hand US English Keyboard Layout

kbdusx.dll	6.3.9600.16384	US Multinational Keyboard Layout
kbduzb.dll	6.3.9600.16384	Uzbek_Cyrillic Keyboard Layout
kbdvntc.dll	6.3.9600.16384	Vietnamese Keyboard Layout
kbdwol.dll	6.3.9600.16384	Wolof Keyboard Layout
kbdyak.dll	6.3.9600.17238	Sakha - Russia Keyboard Layout
kbdyba.dll	6.3.9600.16384	Yoruba Keyboard Layout
kbdycc.dll	6.3.9600.16384	Serbian (Cyrillic) Keyboard Layout
kbdycl.dll	6.3.9600.16384	Serbian (Latin) Keyboard Layout
kerberos.dll	6.3.9600.17423	Kerberos Security Package
kernel.appcore.dll	6.3.9600.17415	AppModel API Host
kernel32.dll	6.3.9600.17415	Windows NT BASE API Client DLL
kernelbase.dll	6.3.9600.17415	Windows NT BASE API Client DLL
keyboardfiltercore.dll	6.3.9600.17415	Keyboard Filter Hooks
keyiso.dll	6.3.9600.17415	CNG Key Isolation Service
keymgr.dll	6.3.9600.17415	Stored User Names and Passwords
korwbrkr.dll	6.3.9600.17415	Korean Word Breaker
ksuser.dll	6.3.9600.17415	User CSA Library
ktmw32.dll	6.3.9600.17415	Windows KTM Win32 Client DLL
l2gpstore.dll	6.3.9600.17415	Policy Storage dll
l2nacp.dll	6.3.9600.17415	Windows Onex Credential Provider
l2sechc.dll	6.3.9600.17415	Layer 2 Security Diagnostics Helper Classes
laprxy.dll	12.0.9600.17415	Windows Media Logagent Proxy
licmgr10.dll	11.0.9600.17416	Microsoft® License Manager DLL
linkinfo.dll	6.3.9600.17415	Windows Volume Tracking
loadperf.dll	6.3.9600.17415	Load & Unload Performance Counters
localsec.dll	6.3.9600.17415	Local Users and Groups MMC Snapin
locationapi.dll	6.3.9600.17415	Microsoft Windows Location API
loghours.dll	6.3.9600.17415	Schedule Dialog
logoncli.dll	6.3.9600.17415	Net Logon Client DLL
lpk.dll	6.3.9600.17415	Language Pack
lsmproxy.dll	6.3.9600.17415	LSM interfaces proxy Dll
luainstall.dll	6.3.9600.17415	Lua manifest install
lz32.dll	6.3.9600.16384	LZ Expand/Compress API DLL
magnification.dll	6.3.9600.17415	Microsoft Magnification API
mapi32.dll	1.0.2536.0	Extended MAPI 1.0 for Windows NT
mapistub.dll	1.0.2536.0	Extended MAPI 1.0 for Windows NT
mbaeapi.dll	6.3.9600.17415	Mobile Broadband Account Experience API
mbaeapipublic.dll	6.3.9600.17415	Mobile Broadband Account API
mbsmsapi.dll	6.3.9600.17415	Microsoft Windows Mobile Broadband SMS API
mbussdapi.dll	6.3.9600.17415	Microsoft Windows Mobile Broadband USSD API
mcewmdrmndbootstrap.dll	1.3.2310.10	Windows® Media Center WMDRM-ND Receiver Bridge Bootstrap DLL
mciavi32.dll	6.3.9600.17415	Video For Windows MCI driver
mcicda.dll	6.3.9600.17415	MCI driver for cdaudio devices
mciqtz32.dll	6.6.9600.17415	DirectShow MCI Driver
mciseq.dll	6.3.9600.17415	MCI driver for MIDI sequencer
mciwave.dll	6.3.9600.17415	MCI driver for waveform audio
mdminst.dll	6.3.9600.17415	Modem Class Installer
mdmregistration.dll	6.3.9600.17415	MDM Registration DLL
mf.dll	12.0.9600.17415	Media Foundation DLL
mf3216.dll	6.3.9600.17415	32-bit to 16-bit Metafile Conversion DLL
mfaacenc.dll	6.3.9600.17415	Media Foundation AAC Encoder
mfasfsrcsnk.dll	12.0.9600.17415	Media Foundation ASF Source and Sink DLL
mfc100.dll	10.0.40219.325	MFCDLL Shared Library - Retail Version
mfc100chs.dll	10.0.40219.325	MFC Language Specific Resources

mfc100cht.dll	10.0.40219.325	MFC Language Specific Resources
mfc100deu.dll	10.0.40219.325	MFC Language Specific Resources
mfc100enu.dll	10.0.40219.325	MFC Language Specific Resources
mfc100esn.dll	10.0.40219.325	MFC Language Specific Resources
mfc100fra.dll	10.0.40219.325	MFC Language Specific Resources
mfc100ita.dll	10.0.40219.325	MFC Language Specific Resources
mfc100jpn.dll	10.0.40219.325	MFC Language Specific Resources
mfc100kor.dll	10.0.40219.325	MFC Language Specific Resources
mfc100rus.dll	10.0.40219.325	MFC Language Specific Resources
mfc100u.dll	10.0.40219.325	MFCDLL Shared Library - Retail Version
mfc40.dll	4.1.0.6140	MFCDLL Shared Library - Retail Version
mfc40u.dll	4.1.0.6140	MFCDLL Shared Library - Retail Version
mfc42.dll	6.6.8063.0	MFCDLL Shared Library - Retail Version
mfc42u.dll	6.6.8063.0	MFCDLL Shared Library - Retail Version
mfcaptureengine.dll	12.0.9600.17415	Media Foundation CaptureEngine DLL
mfcm100.dll	10.0.40219.325	MFC Managed Library - Retail Version
mfcm100u.dll	10.0.40219.325	MFC Managed Library - Retail Version
mfcore.dll	12.0.9600.17415	Media Foundation Core DLL
mfcsubs.dll	2001.12.10530.17415	COM+
mfds.dll	12.0.9600.17415	Media Foundation Direct Show wrapper DLL
mfdvdec.dll	6.3.9600.17415	Media Foundation DV Decoder
mferror.dll	12.0.9600.16384	Media Foundation Error DLL
mfh264enc.dll	6.3.9600.17415	Media Foundation H264 Encoder
mfmediaengine.dll	6.3.9600.17489	Media Foundation Media Engine DLL
mfmjpegdec.dll	6.3.9600.17415	Media Foundation MJPEG Decoder
mfmp4srcsnk.dll	12.0.9600.17483	Media Foundation MPEG4 Source and Sink DLL
mfmpeg2srcsnk.dll	12.0.9600.17415	Media Foundation MPEG2 Source and Sink DLL
mfnetcore.dll	12.0.9600.17415	Media Foundation Net Core DLL
mfnetsrc.dll	12.0.9600.17415	Media Foundation Net Source DLL
mfplat.dll	12.0.9600.17489	Media Foundation Platform DLL
mfplay.dll	12.0.9600.17415	Media Foundation Playback API DLL
mfps.dll	12.0.9600.17415	Media Foundation Proxy DLL
mfreadwrite.dll	12.0.9600.17415	Media Foundation ReadWrite DLL
mfsrcsnk.dll	12.0.9600.17415	Media Foundation Source and Sink DLL
mfsvr.dll	6.3.9600.17415	Media Foundation Simple Video Renderer DLL
mftranscode.dll	12.0.9600.17415	Media Foundation Transcode DLL
mfvdsp.dll	6.3.9600.17415	Windows Media Foundation Video DSP Components
mfwmaaec.dll	6.3.9600.17415	Windows Media Audio AEC for Media Foundation
mgmtapi.dll	6.3.9600.17415	Microsoft SNMP Manager API (uses WinSNMP)
mi.dll	6.3.9600.17415	Management Infrastructure
mibincodec.dll	6.3.9600.17415	Management Infrastructure binary codec component
microsoft.management.infrastructure.native.unmanaged.dll	6.3.9600.17415	Microsoft.Management.Infrastructure.Native.Unmanaged.dll
microsoftaccounttokenprovider.dll	6.3.9600.17415	Microsoft® Account Token Provider
midimap.dll	6.3.9600.17415	Microsoft MIDI Mapper
migisol.dll	6.3.9600.17031	Migration System Isolation Layer
miguiresource.dll	6.3.9600.17415	MIG wini32 resources
mimefilt.dll	2008.0.9600.17415	MIME Filter
mimofcodec.dll	6.3.9600.17415	Management Infrastructure mof codec component
mirrordrvcompat.dll	6.3.9600.17415	Mirror Driver Compatibility Helper
mispace.dll	6.3.9600.17415	Storage Management Provider for Spaces
miutils.dll	6.3.9600.17415	Management Infrastructure
mlang.dll	6.3.9600.17415	Multi Language Support DLL
mmcbase.dll	6.3.9600.17415	MMC Base DLL
mmci.dll	6.3.9600.17415	Media class installer

mmcico.dll	6.3.9600.17415	Media class co-installer
mmcndmgr.dll	6.3.9600.17415	MMC Node Manager DLL
mmcshext.dll	6.3.9600.17415	MMC Shell Extension DLL
mmdevapi.dll	6.3.9600.17415	MMDevice API
mmres.dll	6.3.9600.16384	General Audio Resources
modemui.dll	6.3.9600.17415	Windows Modem Properties
moricons.dll	6.3.9600.16384	Windows NT Setup Icon Resources Library
mp3dmod.dll	6.3.9600.17415	Microsoft MP3 Decoder DMO
mp43decd.dll	6.3.9600.17415	Windows Media MPEG-4 Video Decoder
mp4sdecd.dll	6.3.9600.17415	Windows Media MPEG-4 S Video Decoder
mpg4decd.dll	6.3.9600.17415	Windows Media MPEG-4 Video Decoder
mpr.dll	6.3.9600.17415	Multiple Provider Router DLL
mprapi.dll	6.3.9600.17415	Windows NT MP Router Administration DLL
mprddm.dll	6.3.9600.17415	Demand Dial Manager Supervisor
mprdim.dll	6.3.9600.17415	Dynamic Interface Manager
mprext.dll	6.3.9600.17415	Multiple Provider Router Extension DLL
mprmsg.dll	6.3.9600.17415	Multi-Protocol Router Service Messages DLL
mrmcorer.dll	6.3.9600.17676	Microsoft Windows MRM
mrmindexer.dll	6.3.9600.17415	Microsoft Windows MRM
mrt_map.dll	1.0.51112.34112	Microsoft SLR Error Reporting Helper
mrt100.dll	1.0.30319.34112	System Language Runtime
msaatext.dll	2.0.10413.0	Active Accessibility text support
msac3enc.dll	6.3.9600.17415	Microsoft AC-3 Encoder
msacm32.dll	6.3.9600.17415	Microsoft ACM Audio Filter
msadce.dll	6.3.9600.17415	OLE DB Cursor Engine
msadcer.dll	6.3.9600.16384	OLE DB Cursor Engine Resources
msadco.dll	6.3.9600.17415	Remote Data Services Data Control
msadcor.dll	6.3.9600.16384	Remote Data Services Data Control Resources
msadds.dll	6.3.9600.17415	OLE DB Data Shape Provider
msaddsr.dll	6.3.9600.16384	OLE DB Data Shape Provider Resources
msader15.dll	6.3.9600.16384	ActiveX Data Objects Resources
msado15.dll	6.3.9600.17415	ActiveX Data Objects
msadomd.dll	6.3.9600.17415	ActiveX Data Objects (Multi-Dimensional)
msador15.dll	6.3.9600.17415	Microsoft ActiveX Data Objects Recordset
msadox.dll	6.3.9600.17415	ActiveX Data Objects Extensions
msadrh15.dll	6.3.9600.17415	ActiveX Data Objects Rowset Helper
msafd.dll	6.3.9600.16384	Microsoft Windows Sockets 2.0 Service Provider
msasn1.dll	6.3.9600.17415	ASN.1 Runtime APIs
msauddecmft.dll	6.3.9600.17415	Media Foundation Audio Decoders
msaudite.dll	6.3.9600.17415	Security Audit Events DLL
mscandui.dll	6.3.9600.17415	MSCANDUI Server DLL
mscat32.dll	6.3.9600.17415	MSCAT32 Forwarder DLL
msclmd.dll	6.3.9600.17415	Microsoft Class Mini-driver
mscms.dll	6.3.9600.17415	Microsoft Color Matching System DLL
mscoree.dll	6.3.9600.16384	Microsoft .NET Runtime Execution Engine
mscorier.dll	6.3.9600.16384	Microsoft .NET Runtime IE resources
mscories.dll	2.0.50727.7905	Microsoft .NET IE SECURITY REGISTRATION
mscpx32r.dll	6.3.9600.16384	ODBC Code Page Translator Resources
mscpxl32.dll	6.3.9600.17415	ODBC Code Page Translator
msctf.dll	6.3.9600.17706	MSCTF Server DLL
msctfmonitor.dll	6.3.9600.17415	MsCtfMonitor DLL
msctfp.dll	6.3.9600.17415	MSCTFP Server DLL
msctfui.dll	6.3.9600.17415	MSCTFUI Server DLL
msctfuimanager.dll	6.3.9600.17415	Microsoft UIManager DLL

msdadc.dll	6.3.9600.17415	OLE DB Data Conversion Stub
msdadiag.dll	6.3.9600.17415	Built-In Diagnostics
msdaenum.dll	6.3.9600.17415	OLE DB Root Enumerator Stub
msdaer.dll	6.3.9600.17415	OLE DB Error Collection Stub
msdaora.dll	6.3.9600.17415	OLE DB Provider for Oracle
msdaorar.dll	6.3.9600.16384	OLE DB Provider for Oracle Resources
msdaosp.dll	6.3.9600.17415	OLE DB Simple Provider
msdaprsr.dll	6.3.9600.16384	OLE DB Persistence Services Resources
msdaprst.dll	6.3.9600.17415	OLE DB Persistence Services
msdaps.dll	6.3.9600.17415	OLE DB Interface Proxies/Stubs
msdarem.dll	6.3.9600.17415	OLE DB Remote Provider
msdaremr.dll	6.3.9600.16384	OLE DB Remote Provider Resources
msdart.dll	6.3.9600.17415	OLE DB Runtime Routines
msdasc.dll	6.3.9600.17415	OLE DB Service Components Stub
msdasql.dll	6.3.9600.17415	OLE DB Provider for ODBC Drivers
msdasqlr.dll	6.3.9600.16384	OLE DB Provider for ODBC Drivers Resources
msdatl3.dll	6.3.9600.17415	OLE DB Implementation Support Routines
msdatt.dll	6.3.9600.17415	OLE DB Temporary Table Services
msdaurl.dll	6.3.9600.17415	OLE DB RootBinder Stub
msdelta.dll	6.3.9600.17415	Microsoft Patch Engine
msdfmap.dll	6.3.9600.17415	Data Factory Handler
msdmo.dll	6.6.9600.17415	DMO Runtime
msdrm.dll	6.3.9600.17415	Windows Rights Management client
msdtcprx.dll	2001.12.10530.17415	Microsoft Distributed Transaction Coordinator OLE Transactions Interface Proxy DLL
msdtcuiu.dll	2001.12.10530.17415	Microsoft Distributed Transaction Coordinator Administrative DLL
msdtcvsp1res.dll	2001.12.10530.16384	Microsoft Distributed Transaction Coordinator Resources for Vista SP1
msexch40.dll	4.0.9756.0	Microsoft Jet Exchange Isam
msexcl40.dll	4.0.9756.0	Microsoft Jet Excel Isam
msfeeds.dll	11.0.9600.17728	Microsoft Feeds Manager
msfeedsbs.dll	11.0.9600.17416	Microsoft Feeds Background Sync
msftedit.dll	6.3.9600.17671	Rich Text Edit Control, v7.5
mshtml.dll	11.0.9600.17728	Microsoft (R) HTML Viewer
mshtmldac.dll	11.0.9600.17689	DAC for Trident DOM
mshtmled.dll	11.0.9600.17690	Microsoft® HTML Editing Component
mshtmler.dll	11.0.9600.16384	Microsoft® HTML Editing Component's Resource DLL
msi.dll	5.0.9600.17415	Windows Installer
msidcrl40.dll	6.3.9600.17415	Microsoft® Account Dynamic Link Library
msident.dll	6.3.9600.17415	Microsoft Identity Manager
msidle.dll	6.3.9600.17415	User Idle Monitor
msidntld.dll	6.3.9600.16384	Microsoft Identity Manager
msieftp.dll	6.3.9600.17415	Microsoft Internet Explorer FTP Folder Shell Extension
msihnd.dll	5.0.9600.17415	Windows® installer
msiltcfg.dll	5.0.9600.17415	Windows Installer Configuration API Stub
msimg32.dll	6.3.9600.17415	GDIEXT Client DLL
msimsg.dll	5.0.9600.16384	Windows® Installer International Messages
msimtf.dll	6.3.9600.17415	Active IMM Server DLL
msisip.dll	5.0.9600.17415	MSI Signature SIP Provider
msiwer.dll	5.0.9600.17415	MSI Windows Error Reporting
msjet40.dll	4.0.9765.0	Microsoft Jet Engine Library
msjetoledb40.dll	4.0.9756.0	
msjint40.dll	4.0.9765.0	Microsoft Jet Database Engine International DLL
msjro.dll	6.3.9600.17415	Jet and Replication Objects
msjter40.dll	4.0.9756.0	Microsoft Jet Database Engine Error DLL
msjtes40.dll	4.0.9756.0	Microsoft Jet Expression Service

mskeyprotcli.dll	6.3.9600.17415	Windows Client Key Protection Provider
mskeyprotect.dll	6.3.9600.17415	Microsoft Key Protection Provider
msls31.dll	3.10.349.0	Microsoft Line Services library file
msltus40.dll	4.0.9756.0	Microsoft Jet Lotus 1-2-3 Isam
msmpeg2adec.dll	12.0.9477.0	Microsoft DTV-DVD Audio Decoder
msmpeg2enc.dll	12.0.9600.17415	Microsoft MPEG-2 Encoder
msmpeg2vdec.dll	12.0.9600.17374	Microsoft DTV-DVD Video Decoder
msnetobj.dll	11.0.9600.17415	DRM ActiveX Network Object
msobjs.dll	6.3.9600.16384	System object audit names
msoeacct.dll	6.3.9600.17415	Microsoft Internet Account Manager
msoert2.dll	6.3.9600.17415	Microsoft Windows Mail RT Lib
msorc32r.dll	6.3.9600.16384	ODBC Driver for Oracle Resources
msorcl32.dll	6.3.9600.17415	ODBC Driver for Oracle
mspatcha.dll	6.3.9600.17415	Microsoft File Patch Application API
mspatchc.dll	6.3.9600.17415	Microsoft Patch Creation Engine
mspbde40.dll	4.0.9756.0	Microsoft Jet Paradox Isam
msports.dll	6.3.9600.17415	Ports Class Installer
msrating.dll	11.0.9600.17416	Internet Ratings and Local User Management DLL
msrd2x40.dll	4.0.9756.0	Microsoft (R) Red ISAM
msrd3x40.dll	4.0.9756.0	Microsoft (R) Red ISAM
msrdc.dll	6.3.9600.17415	Remote Differential Compression COM server
msrdpwebaccess.dll	6.3.9600.17415	Microsoft Remote Desktop Services Web Access Control
msrepl40.dll	4.0.9756.0	Microsoft Replication Library
msrle32.dll	6.3.9600.17415	Microsoft RLE Compressor
msscntrs.dll	7.0.9600.17415	PKM Perfmon Counter DLL
msscp.dll	11.0.9600.17415	Windows Media Secure Content Provider
mssha.dll	6.3.9600.17415	Windows Security Health Agent
msshavmsg.dll	6.3.9600.16384	Windows Security Health Agent Validator Message
msshooks.dll	7.0.9600.17415	Microsoft Search Hooks
mssign32.dll	6.3.9600.17415	Microsoft Trust Signing APIs
mssip32.dll	6.3.9600.17415	MSSIP32 Forwarder DLL
mssitlb.dll	7.0.9600.17415	mssitlb
msspellcheckingfacility.dll	6.3.9600.17415	Microsoft Spell Checking Facility
mssph.dll	7.0.9600.17415	Microsoft Search Protocol Handler
mssphtb.dll	7.0.9600.17415	Outlook MSSearch Connector
mssprxy.dll	7.0.9600.17415	Microsoft Search Proxy
mssrch.dll	7.0.9600.17415	Microsoft Embedded Search
mssvp.dll	7.0.9600.17415	MSSearch Vista Platform
mstask.dll	6.3.9600.17415	Task Scheduler interface DLL
mstext40.dll	4.0.9756.0	Microsoft Jet Text Isam
mstscax.dll	6.3.9600.17415	Remote Desktop Services ActiveX Client
msutb.dll	6.3.9600.17415	MSUTB Server DLL
msv1_0.dll	6.3.9600.17415	Microsoft Authentication Package v1.0
msvbvm60.dll	6.0.98.15	Visual Basic Virtual Machine
msvcirt.dll	7.0.9600.17415	Windows NT IOStreams DLL
msvcp100.dll	10.0.40219.325	Microsoft® C Runtime Library
msvcp120_clr0400.dll	12.0.20806.33440	Microsoft® C Runtime Library
msvcp60.dll	7.0.9600.17415	Windows NT C++ Runtime Library DLL
msvcr100.dll	10.0.40219.325	Microsoft® C Runtime Library
msvcr100_clr0400.dll	12.0.20806.33440	Microsoft® .NET Framework
msvcr120_clr0400.dll	12.0.51670.34230	Microsoft® C Runtime Library
msvcrt.dll	7.0.9600.17415	Windows NT CRT DLL
msvcrt20.dll	2.12.0.0	Microsoft® C Runtime Library
msvcrt40.dll	6.3.9600.16384	VC 4.x CRT DLL (Forwarded to msvcrt.dll)

msvfw32.dll	6.3.9600.17415	Microsoft Video for Windows DLL
msvidc32.dll	6.3.9600.17415	Microsoft Video 1 Compressor
msvidctl.dll	6.5.9600.17415	ActiveX control for streaming video
msvideodsp.dll	6.3.9600.17415	Video Stabilization MFT
msvproc.dll	12.0.9600.17415	Media Foundation Video Processor
mswb7.dll	6.3.9600.17415	MSWB7 DLL
mswb70011.dll	6.3.9600.17415	MSWB7EA DLL
mswb7001e.dll	6.3.9600.17415	MSWB7EA DLL
mswb70404.dll	6.3.9600.17415	MSWB7EA DLL
mswb70804.dll	6.3.9600.17415	MSWB7EA DLL
mswdat10.dll	4.0.9756.0	Microsoft Jet Sort Tables
mswmdm.dll	12.0.9600.17415	Windows Media Device Manager Core
mswsock.dll	6.3.9600.17415	Microsoft Windows Sockets 2.0 Service Provider
mswstr10.dll	4.0.9765.0	Microsoft Jet Sort Library
msxactps.dll	6.3.9600.17415	OLE DB Transaction Proxies/Stubs
msxbde40.dll	4.0.9756.0	Microsoft Jet xBASE Isam
msxml3.dll	8.110.9600.17415	MSXML 3.0
msxml3r.dll	8.110.9600.16384	XML Resources
msxml6.dll	6.30.9600.17415	MSXML 6.0
msxml6r.dll	6.30.9600.16384	XML Resources
msyuv.dll	6.3.9600.17415	Microsoft UYVY Video Decompressor
mtxclu.dll	2001.12.10530.17415	Microsoft Distributed Transaction Coordinator Failover Clustering Support DLL
mtxdm.dll	2001.12.10530.17415	COM+
mtxex.dll	2001.12.10530.17415	COM+
mtxlegih.dll	2001.12.10530.17415	COM+
mtxoci.dll	2001.12.10530.17415	Microsoft Distributed Transaction Coordinator Database Support DLL for Oracle
muifontsetup.dll	6.3.9600.17415	MUI Callback for font registry settings
mycomput.dll	6.3.9600.17415	Computer Management
mydocs.dll	6.3.9600.17415	My Documents Folder UI
napcrypt.dll	6.3.9600.16384	NAP Cryptographic API helper
napdsnap.dll	6.3.9600.17415	NAP GPEdit Extension
naphlpr.dll	6.3.9600.16384	NAP client config API helper
napinsp.dll	6.3.9600.17415	E-mail Naming Shim Provider
napipsec.dll	6.3.9600.17415	NAP IPSec Enforcement Client
napmontr.dll	6.3.9600.17415	NAP Netsh Helper
naturallanguage6.dll	6.3.9600.17415	Natural Language Development Platform 6
ncaapi.dll	6.3.9600.17415	Microsoft Network Connectivity Assistant API
ncdprop.dll	6.3.9600.17415	Advanced network device properties
nci.dll	6.3.9600.17415	CoInstaller: NET
ncobjapi.dll	6.3.9600.17415	Microsoft® Windows® Operating System
ncrypt.dll	6.3.9600.17415	Windows NCrypt Router
ncryptprov.dll	6.3.9600.17415	Microsoft KSP
ncryptsslp.dll	6.3.9600.17415	Microsoft SChannel Provider
nddeapi.dll	6.3.9600.17415	Network DDE Share Management APIs
ndfapi.dll	6.3.9600.17415	Network Diagnostic Framework Client API
ndfetw.dll	6.3.9600.17415	Network Diagnostic Engine Event Interface
ndfhcdiscovery.dll	6.3.9600.17415	Network Diagnostic Framework HC Discovery API
ndiscapcfg.dll	6.3.9600.17415	NdisCap Notify Object
ndishc.dll	6.3.9600.17415	NDIS Helper Classes
ndproxystub.dll	6.3.9600.17415	Network Diagnostic Engine Proxy/Stub
negoexts.dll	6.3.9600.17415	NegoExtender Security Package
netapi32.dll	6.3.9600.17415	Net Win32 API DLL
netbios.dll	6.3.9600.17415	NetBIOS Interface Library
netcenter.dll	6.3.9600.17415	Network Center control panel

netcfgx.dll	6.3.9600.17415	Network Configuration Objects
netcorehc.dll	6.3.9600.17415	Networking Core Diagnostics Helper Classes
netdiagfx.dll	6.3.9600.17415	Network Diagnostic Framework
netevent.dll	6.3.9600.16384	Net Event Handler
netfxperf.dll	6.3.9600.16384	Extensible Performance Counter Shim
neth.dll	6.3.9600.16384	Net Help Messages DLL
netid.dll	6.3.9600.17415	System Control Panel Applet; Network ID Page
netiohlp.dll	6.3.9600.17415	Netio Helper DLL
netjoin.dll	6.3.9600.17415	Domain Join DLL
netlogon.dll	6.3.9600.17415	Net Logon Services DLL
netmsg.dll	6.3.9600.16384	Net Messages DLL
netplwiz.dll	6.3.9600.17415	Map Network Drives/Network Places Wizard
netprofm.dll	6.3.9600.17415	Network List Manager
netprovisionsp.dll	6.3.9600.17415	Provisioning Service Provider DLL
netshell.dll	6.3.9600.17415	Network Connections Shell
netutils.dll	6.3.9600.17415	Net Win32 API Helpers DLL
networkexplorer.dll	6.3.9600.17415	Network Explorer
networkitemfactory.dll	6.3.9600.17415	NetworkItem Factory
newdev.dll	6.0.5054.0	Add Hardware Device Library
ninput.dll	6.3.9600.17415	Microsoft Pen and Touch Input Component
nl7data0011.dll	6.3.9600.17415	Microsoft Japanese Natural Language Data and Code
nl7data001e.dll	6.3.9600.17415	Microsoft Thai Natural Language Data and Code
nl7data0404.dll	6.3.9600.17415	Microsoft Chinese Traditional Natural Language Data and Code
nl7data0804.dll	6.3.9600.17415	Microsoft Chinese Simplified Natural Language Data and Code
nlaapi.dll	6.3.9600.17415	Network Location Awareness 2
nlhtml.dll	2008.0.9600.17415	HTML filter
nlmgp.dll	6.3.9600.17415	Network List Manager Snapin
nlmproxy.dll	6.3.9600.17415	Network List Manager Public Proxy
nlmsprep.dll	6.3.9600.17415	Network List Manager Sysprep Module
nlsbres.dll	6.3.9600.16384	NLSBuild resource DLL
nlsdata0000.dll	6.3.9600.17415	Microsoft Neutral Natural Language Server Data and Code
nlsdata0002.dll	6.3.9600.17415	Microsoft Neutral Natural Language Server Data and Code
nlsdata0003.dll	6.3.9600.17415	Microsoft Neutral Natural Language Server Data and Code
nlsdata0007.dll	6.3.9600.17415	Microsoft German Natural Language Server Data and Code
nlsdata0009.dll	6.3.9600.17415	Microsoft English Natural Language Server Data and Code
nlsdata000a.dll	6.3.9600.17415	Microsoft Spanish Natural Language Server Data and Code
nlsdata000c.dll	6.3.9600.17415	Microsoft French Natural Language Server Data and Code
nlsdata000d.dll	6.3.9600.17415	Microsoft Neutral Natural Language Server Data and Code
nlsdata000f.dll	6.3.9600.17415	Microsoft Neutral Natural Language Server Data and Code
nlsdata0010.dll	6.3.9600.17415	Microsoft Neutral Natural Language Server Data and Code
nlsdata0018.dll	6.3.9600.17415	Microsoft Neutral Natural Language Server Data and Code
nlsdata001a.dll	6.3.9600.17415	Microsoft Neutral Natural Language Server Data and Code
nlsdata001b.dll	6.3.9600.17415	Microsoft Neutral Natural Language Server Data and Code
nlsdata001d.dll	6.3.9600.17415	Microsoft Neutral Natural Language Server Data and Code
nlsdata0020.dll	6.3.9600.17415	Microsoft Neutral Natural Language Server Data and Code
nlsdata0021.dll	6.3.9600.17415	Microsoft Neutral Natural Language Server Data and Code
nlsdata0022.dll	6.3.9600.17415	Microsoft Neutral Natural Language Server Data and Code
nlsdata0024.dll	6.3.9600.17415	Microsoft Neutral Natural Language Server Data and Code
nlsdata0026.dll	6.3.9600.17415	Microsoft Neutral Natural Language Server Data and Code
nlsdata0027.dll	6.3.9600.17415	Microsoft Neutral Natural Language Server Data and Code
nlsdata002a.dll	6.3.9600.17415	Microsoft Neutral Natural Language Server Data and Code
nlsdata0039.dll	6.3.9600.17415	Microsoft Neutral Natural Language Server Data and Code
nlsdata003e.dll	6.3.9600.17415	Microsoft Neutral Natural Language Server Data and Code
nlsdata0045.dll	6.3.9600.17415	Microsoft Neutral Natural Language Server Data and Code

nlsdata0046.dll	6.3.9600.17415	Microsoft Neutral Natural Language Server Data and Code
nlsdata0047.dll	6.3.9600.17415	Microsoft Neutral Natural Language Server Data and Code
nlsdata0049.dll	6.3.9600.17415	Microsoft Neutral Natural Language Server Data and Code
nlsdata004a.dll	6.3.9600.17415	Microsoft Neutral Natural Language Server Data and Code
nlsdata004b.dll	6.3.9600.17415	Microsoft Neutral Natural Language Server Data and Code
nlsdata004c.dll	6.3.9600.17415	Microsoft Neutral Natural Language Server Data and Code
nlsdata004e.dll	6.3.9600.17415	Microsoft Neutral Natural Language Server Data and Code
nlsdata0414.dll	6.3.9600.17415	Microsoft Neutral Natural Language Server Data and Code
nlsdata0416.dll	6.3.9600.17415	Microsoft Neutral Natural Language Server Data and Code
nlsdata0816.dll	6.3.9600.17415	Microsoft Neutral Natural Language Server Data and Code
nlsdata081a.dll	6.3.9600.17415	Microsoft Neutral Natural Language Server Data and Code
nlsdata0c1a.dll	6.3.9600.17415	Microsoft Neutral Natural Language Server Data and Code
nlsdl.dll	6.3.9600.17415	Nls Downlevel DLL
nlslexicons0002.dll	6.3.9600.16384	Microsoft Neutral Natural Language Server Data and Code
nlslexicons0003.dll	6.3.9600.16384	Microsoft Neutral Natural Language Server Data and Code
nlslexicons0007.dll	6.3.9600.16384	Microsoft German Natural Language Server Data and Code
nlslexicons0009.dll	6.3.9600.17415	Microsoft English Natural Language Server Data and Code
nlslexicons000a.dll	6.3.9600.16384	Microsoft Spanish Natural Language Server Data and Code
nlslexicons000c.dll	6.3.9600.16384	Microsoft French Natural Language Server Data and Code
nlslexicons000d.dll	6.3.9600.16384	Microsoft Neutral Natural Language Server Data and Code
nlslexicons000f.dll	6.3.9600.16384	Microsoft Neutral Natural Language Server Data and Code
nlslexicons0010.dll	6.3.9600.16384	Microsoft Neutral Natural Language Server Data and Code
nlslexicons0018.dll	6.3.9600.16384	Microsoft Neutral Natural Language Server Data and Code
nlslexicons001a.dll	6.3.9600.16384	Microsoft Neutral Natural Language Server Data and Code
nlslexicons001b.dll	6.3.9600.16384	Microsoft Neutral Natural Language Server Data and Code
nlslexicons001d.dll	6.3.9600.16384	Microsoft Neutral Natural Language Server Data and Code
nlslexicons0020.dll	6.3.9600.16384	Microsoft Neutral Natural Language Server Data and Code
nlslexicons0021.dll	6.3.9600.16384	Microsoft Neutral Natural Language Server Data and Code
nlslexicons0022.dll	6.3.9600.16384	Microsoft Neutral Natural Language Server Data and Code
nlslexicons0024.dll	6.3.9600.16384	Microsoft Neutral Natural Language Server Data and Code
nlslexicons0026.dll	6.3.9600.16384	Microsoft Neutral Natural Language Server Data and Code
nlslexicons0027.dll	6.3.9600.16384	Microsoft Neutral Natural Language Server Data and Code
nlslexicons002a.dll	6.3.9600.16384	Microsoft Neutral Natural Language Server Data and Code
nlslexicons0039.dll	6.3.9600.16384	Microsoft Neutral Natural Language Server Data and Code
nlslexicons003e.dll	6.3.9600.16384	Microsoft Neutral Natural Language Server Data and Code
nlslexicons0045.dll	6.3.9600.16384	Microsoft Neutral Natural Language Server Data and Code
nlslexicons0046.dll	6.3.9600.16384	Microsoft Neutral Natural Language Server Data and Code
nlslexicons0047.dll	6.3.9600.16384	Microsoft Neutral Natural Language Server Data and Code
nlslexicons0049.dll	6.3.9600.16384	Microsoft Neutral Natural Language Server Data and Code
nlslexicons004a.dll	6.3.9600.16384	Microsoft Neutral Natural Language Server Data and Code
nlslexicons004b.dll	6.3.9600.16384	Microsoft Neutral Natural Language Server Data and Code
nlslexicons004c.dll	6.3.9600.16384	Microsoft Neutral Natural Language Server Data and Code
nlslexicons004e.dll	6.3.9600.16384	Microsoft Neutral Natural Language Server Data and Code
nlslexicons0414.dll	6.3.9600.16384	Microsoft Neutral Natural Language Server Data and Code
nlslexicons0416.dll	6.3.9600.16384	Microsoft Neutral Natural Language Server Data and Code
nlslexicons0816.dll	6.3.9600.16384	Microsoft Neutral Natural Language Server Data and Code
nlslexicons081a.dll	6.3.9600.16384	Microsoft Neutral Natural Language Server Data and Code
nlslexicons0c1a.dll	6.3.9600.16384	Microsoft Neutral Natural Language Server Data and Code
normaliz.dll	6.3.9600.17415	Unicode Normalization DLL
npmproxy.dll	6.3.9600.17415	Network List Manager Proxy
nshhttp.dll	6.3.9600.17415	HTTP netsh DLL
nshipsec.dll	6.3.9600.17415	Net Shell IP Security helper DLL
nshwfp.dll	6.3.9600.17485	Windows Filtering Platform Netsh Helper
nsi.dll	6.3.9600.17415	NSI User-mode interface DLL

ntasn1.dll	6.3.9600.17415	Microsoft ASN.1 API
ntdll.dll	6.3.9600.17736	NT Layer DLL
ntdsapi.dll	6.3.9600.17415	Active Directory Domain Services API
ntlanman.dll	6.3.9600.17415	Microsoft® Lan Manager
ntlanui2.dll	6.3.9600.17415	Network object shell UI
ntmarta.dll	6.3.9600.17415	Windows NT MARTA provider
ntprint.dll	6.3.9600.17415	Spooler Setup DLL
ntshrui.dll	6.3.9600.17415	Shell extensions for sharing
ntvdm64.dll	6.3.9600.17475	16-bit Emulation on NT64
objsel.dll	6.3.9600.17415	Object Picker Dialog
occache.dll	11.0.9600.17416	Object Control Viewer
ocsetapi.dll	6.3.9600.17415	Windows Optional Component Setup API
odbc32.dll	6.3.9600.17415	ODBC Driver Manager
odbcbcp.dll	6.3.9600.17415	BCP for ODBC
odbcconf.dll	6.3.9600.17415	ODBC Driver Configuration Program
odbccp32.dll	6.3.9600.17415	ODBC Installer
odbccr32.dll	6.3.9600.17415	ODBC Cursor Library
odbccu32.dll	6.3.9600.17415	ODBC Cursor Library
odbcint.dll	6.3.9600.16384	ODBC Resources
odbcji32.dll	6.3.9600.17415	Microsoft ODBC Desktop Driver Pack 3.5
odbcjt32.dll	6.3.9600.17415	Microsoft ODBC Desktop Driver Pack 3.5
odbctrac.dll	6.3.9600.17415	ODBC Driver Manager Trace
oddbse32.dll	6.3.9600.17415	ODBC (3.0) driver for DBase
odexl32.dll	6.3.9600.17415	ODBC (3.0) driver for Excel
odfox32.dll	6.3.9600.17415	ODBC (3.0) driver for FoxPro
odpdx32.dll	6.3.9600.17415	ODBC (3.0) driver for Paradox
odtext32.dll	6.3.9600.17415	ODBC (3.0) driver for text files
oemlicense.dll		
offfilt.dll	2008.0.9600.17415	OFFICE Filter
offreg.dll	6.3.9600.17415	Offline registry DLL
ogldrv.dll	6.3.9600.17415	MSOGL
ole2.dll	3.10.0.103	Windows Win16 Application Launcher
ole2disp.dll	3.10.0.103	Windows Win16 Application Launcher
ole2nls.dll	3.10.0.103	Windows Win16 Application Launcher
ole32.dll	6.3.9600.17415	Microsoft OLE for Windows
oleacc.dll	7.2.9600.17415	Active Accessibility Core Component
oleacchooks.dll	7.2.9600.17415	Active Accessibility Event Hooks Library
oleaccrc.dll	7.2.9600.16384	Active Accessibility Resource DLL
oleaut32.dll	6.3.9600.17560	
olecli32.dll	6.3.9600.17415	Object Linking and Embedding Client Library
oledb32.dll	6.3.9600.17415	OLE DB Core Services
oledb32r.dll	6.3.9600.16384	OLE DB Core Services Resources
oledlg.dll	6.3.9600.17415	OLE User Interface Support
oleprn.dll	6.3.9600.17415	Oleprn DLL
olepro32.dll	6.3.9600.17415	
olesvr32.dll	6.3.9600.17415	Object Linking and Embedding Server Library
olethk32.dll	6.3.9600.17415	Microsoft OLE for Windows
ondemandconnroutehelper.dll	6.3.9600.17415	On Demand Connctiond Route Helper
onex.dll	6.3.9600.17415	IEEE 802.1X supplicant library
onexui.dll	6.3.9600.17415	IEEE 802.1X supplicant UI library
oobefldr.dll	6.3.9600.17415	Getting Started
opcservices.dll	6.3.9600.17415	Native Code OPC Services Library
opencl.dll	1.2.11.0	OpenCL Client DLL
opengl32.dll	6.3.9600.17415	OpenGL Client DLL

osbaseln.dll	6.3.9600.17415	Service Reporting API
osksupport.dll	6.3.9600.17415	Microsoft On-Screen Keyboard Support Utilities
osuninst.dll	6.3.9600.17415	Uninstall Interface
p2p.dll	6.3.9600.17415	Peer-to-Peer Grouping
p2pgraph.dll	6.3.9600.17415	Peer-to-Peer Graphing
p2pnetsh.dll	6.3.9600.17415	Peer-to-Peer NetSh Helper
packager.dll	6.3.9600.17415	Object Packager2
packagestateroaming.dll	6.3.9600.17415	Package State Roaming
panmap.dll	6.3.9600.17415	PANOSE(tm) Font Mapper
pautoenr.dll	6.3.9600.17415	Auto Enrollment DLL
pcacli.dll	6.3.9600.17415	Program Compatibility Assistant Client Module
pcaui.dll	6.3.9600.17415	Program Compatibility Assistant User Interface Module
pcpksp.dll	6.3.9600.17415	Microsoft Platform Key Storage Provider for Platform Crypto Provider
pcptpm12.dll	6.3.9600.17415	Microsoft Platform Crypto Provider for Trusted Platform Module 1.2
pcwum.dll	6.3.9600.16384	Performance Counters for Windows Native DLL
pdh.dll	6.3.9600.17415	Windows Performance Data Helper DLL
pdhui.dll	6.3.9600.17415	PDH UI
peerdist.dll	6.3.9600.17415	BranchCache Client Library
peerdistsh.dll	6.3.9600.17415	BranchCache Netshell Helper
perfctrs.dll	6.3.9600.17415	Performance Counters
perfdisk.dll	6.3.9600.17415	Windows Disk Performance Objects DLL
perfnet.dll	6.3.9600.17415	Windows Network Service Performance Objects DLL
perfos.dll	6.3.9600.17415	Windows System Performance Objects DLL
perfproc.dll	6.3.9600.17415	Windows System Process Performance Objects DLL
perfts.dll	6.3.9600.17415	Windows Remote Desktop Services Performance Objects
photometadatahandler.dll	6.3.9600.17746	Photo Metadata Handler
photowiz.dll	6.3.9600.17669	Photo Printing Wizard
pid.dll	6.3.9600.17415	Microsoft PID
pidgenx.dll	6.3.9600.16384	Pid Generation
pifmgr.dll	6.3.9600.16384	Windows NT PIF Manager Icon Resources Library
pku2u.dll	6.3.9600.17728	Pku2u Security Package
pla.dll	6.3.9600.17415	Performance Logs & Alerts
playlistfolder.dll	6.3.9600.17415	Playlist Folder
playsndsrv.dll	6.3.9600.17415	PlaySound Service
playtodevice.dll	12.0.9600.17415	PLAYTODEVICE DLL
playtomanager.dll	6.3.9600.17415	Microsoft Windows PlayTo Manager
playtostatusprovider.dll	6.3.9600.17415	PlayTo Status Provider Dll
pngfilt.dll	11.0.9600.17416	IE PNG plugin image decoder
pnrpnsp.dll	6.3.9600.17415	PNRP Name Space Provider
polstore.dll	6.3.9600.17415	Policy Storage dll
portabledeviceapi.dll	6.3.9600.17415	Windows Portable Device API Components
portabledeviceclassextension.dll	6.3.9600.17415	Windows Portable Device Class Extension Component
portabledeviceconnectapi.dll	6.3.9600.17415	Portable Device Connection API Components
portabledevicestatus.dll	6.3.9600.17415	Microsoft Windows Portable Device Status Provider
portabledevicesyncprovider.dll	6.3.9600.17415	Microsoft Windows Portable Device Provider.
portabledevicetypes.dll	6.3.9600.17415	Windows Portable Device (Parameter) Types Component
portabledevicewiacompat.dll	6.3.9600.17415	PortableDevice WIA Compatibility Driver
portabledevicewmdrm.dll	6.3.9600.17415	Windows Portable Device WMDRM Component
pots.dll	6.3.9600.17415	Power Troubleshooter
powercpl.dll	6.3.9600.17415	Power Options Control Panel
powrprof.dll	6.3.9600.17415	Power Profile Helper DLL
presentationcffrasterizernative_v0300.dll	3.0.6920.7903	WinFX OpenType/CFF Rasterizer
presentationhostproxy.dll	6.3.9600.16384	Windows Presentation Foundation Host Proxy
presentationnative_v0300.dll	3.0.6920.7903	PresentationNative_v0300.dll

prflbmsg.dll	6.3.9600.16384	Perflib Event Messages
printconfig.dll	0.3.9600.17705	PrintConfig User Interface
printdialogs.dll	6.3.9600.17415	Microsoft® Windows® Operating System
printui.dll	6.3.9600.17415	Printer Settings User Interface
prncache.dll	6.3.9600.17415	Print UI Cache
prnfldr.dll	6.3.9600.17415	prnfldr dll
prnntfy.dll	6.3.9600.17415	prnntfy DLL
prntvpt.dll	6.3.9600.17415	Print Ticket Services Module
profapi.dll	6.3.9600.17415	User Profile Basic API
profext.dll	6.3.9600.17415	profext
propsys.dll	7.0.9600.17415	Microsoft Property System
provcore.dll	6.3.9600.17415	Microsoft Wireless Provisioning Core
provsvc.dll	6.3.9600.17415	Windows HomeGroup
provthrd.dll	6.3.9600.17415	WMI Provider Thread & Log Library
proximitycommon.dll	6.3.9600.17415	Proximity Common Implementation
proximitycommonpal.dll	6.3.9600.17415	Proximity Common PAL
proximityrtapipal.dll	6.3.9600.17415	Proximity WinRT API PAL
prvdmofcomp.dll	6.3.9600.17415	WMI
psapi.dll	6.3.9600.17415	Process Status Helper
pshed.dll	6.3.9600.16384	Platform Specific Hardware Error Driver
psisdecd.dll	6.6.9600.17415	Microsoft SI/PSI parser for MPEG2 based networks.
psmodulediscoveryprovider.dll	6.3.9600.17415	WMI
pstorec.dll	6.3.9600.17415	Deprecated Protected Storage COM interfaces
puiapi.dll	6.3.9600.17415	puiapi DLL
puiobj.dll	6.3.9600.17415	PrintUI Objects DLL
pwrshplugin.dll	6.3.9600.17415	pwrshplugin.dll
qagent.dll	6.3.9600.17415	Quarantine Agent Proxy
qasf.dll	12.0.9600.17415	DirectShow ASF Support
qcap.dll	6.6.9600.16384	DirectShow Runtime.
qcliprov.dll	6.3.9600.17415	Quarantine Client WMI Provider
qdv.dll	6.6.9600.17415	DirectShow Runtime.
qdvd.dll	6.6.9600.17415	DirectShow DVD PlayBack Runtime.
qedit.dll	6.6.9600.17415	DirectShow Editing.
qedwipes.dll	6.6.9600.16384	DirectShow Editing SMPTE Wipes
qmgrprxy.dll	7.7.9600.17415	Background Intelligent Transfer Service Proxy
qshvhost.dll	6.3.9600.17481	Quarantine SHV Host
qsvrmgmt.dll	6.3.9600.17481	Quarantine Server Management
quartz.dll	6.6.9600.17415	DirectShow Runtime.
query.dll	6.3.9600.17415	Content Index Utility DLL
qutil.dll	6.3.9600.17415	Quarantine Utilities
qwave.dll	6.3.9600.17415	Windows NT
racengn.dll	6.3.9600.17415	Reliability analysis metrics calculation engine
racpldlg.dll	6.3.9600.17415	Remote Assistance Contact List
radardt.dll	6.3.9600.17415	Microsoft Windows Resource Exhaustion Detector
radarrs.dll	6.3.9600.17415	Microsoft Windows Resource Exhaustion Resolver
radcui.dll	6.3.9600.17415	RemoteApp and Desktop Connection UI Component
rasadhlp.dll	6.3.9600.17415	Remote Access AutoDial Helper
rasapi32.dll	6.3.9600.17485	Remote Access API
rascfg.dll	6.3.9600.17626	RAS Configuration Objects
raschap.dll	6.3.9600.17415	Remote Access PPP CHAP
raschapext.dll	6.3.9600.17415	Windows Extension library for raschap
rasctrs.dll	6.3.9600.17415	Windows NT Remote Access Perfmon Counter dll
rasdiag.dll	6.3.9600.17484	RAS Diagnostics Helper Classes
rasdlg.dll	6.3.9600.17415	Remote Access Common Dialog API

rasgcw.dll	6.3.9600.17415	RAS Wizard Pages
rasman.dll	6.3.9600.17415	Remote Access Connection Manager
rasmontr.dll	6.3.9600.17415	RAS Monitor DLL
rasmxs.dll	6.3.9600.17484	Remote Access Device DLL for modems, PADs and switches
rasplap.dll	6.3.9600.17415	RAS PLAP Credential Provider
rasppp.dll	6.3.9600.17415	Remote Access PPP
rasser.dll	6.3.9600.17484	Remote Access Media DLL for COM ports
rastapi.dll	6.3.9600.17415	Remote Access TAPI Compliance Layer
rastls.dll	6.3.9600.17415	Remote Access PPP EAP-TLS
rastlsext.dll	6.3.9600.17415	Windows Extension library for rastls
rdpcore.dll	6.3.9600.17415	RDP Core DLL
rdpencom.dll	6.3.9600.17415	RDPSRAPI COM Objects
rdpendp.dll	6.3.9600.17415	RDP Audio Endpoint
rdpsaps.dll	6.3.9600.17415	RDP Session Agent Proxy Stub
rdvidcrl.dll	6.3.9600.17415	Remote Desktop Services Client for Microsoft Online Services
rdvvmtransport.dll	6.3.9600.17415	RdvVmTransport EndPoints
reagent.dll	6.3.9600.17415	Microsoft Windows Recovery Agent DLL
regapi.dll	6.3.9600.17415	Registry Configuration APIs
regctrl.dll	6.3.9600.17415	RegCtrl
reinfo.dll	6.3.9600.17415	Microsoft Windows Recovery Info DLL
remotepg.dll	6.3.9600.17415	Remote Sessions CPL Extension
removedevicecontexthandler.dll	6.3.9600.17415	Devices & Printers Remove Device Context Menu Handler
removedeviceelevated.dll	6.3.9600.17415	RemoveDeviceElevated Proxy Dll
resampledmo.dll	6.3.9600.17415	Windows Media Resampler
resutils.dll	6.3.9600.17415	Microsoft Cluster Resource Utility DLL
rgb9rast.dll	6.3.9600.17415	Microsoft® Windows® Operating System
riched20.dll	5.31.23.1231	Rich Text Edit Control, v3.1
riched32.dll	6.3.9600.17415	Wrapper Dll for Richedit 1.0
rnr20.dll	6.3.9600.17415	Windows Socket2 NameSpace DLL
rometadata.dll	4.0.20806.33440	Microsoft MetaData Library
rpchttp.dll	6.3.9600.17415	RPC HTTP DLL
rpcns4.dll	6.3.9600.17415	Remote Procedure Call Name Service Client
rpcnsh.dll	6.3.9600.17415	RPC Netshell Helper
rpcrt4.dll	6.3.9600.17415	Remote Procedure Call Runtime
rpcrtremote.dll	6.3.9600.17415	Remote RPC Extension
rsaenh.dll	6.3.9600.17415	Microsoft Enhanced Cryptographic Provider
rshx32.dll	6.3.9600.17415	Security Shell Extension
rstrtmgr.dll	6.3.9600.17415	Restart Manager
rtffilt.dll	2008.0.9600.17415	RTF Filter
rtm.dll	6.3.9600.17415	Routing Table Manager
rtutils.dll	6.3.9600.17415	Routing Utilities
rtworkq.dll	12.0.9600.17415	Realtime WorkQueue DLL
samcli.dll	6.3.9600.17415	Security Accounts Manager Client DLL
samlib.dll	6.3.9600.17415	SAM Library DLL
sas.dll	6.3.9600.17415	WinLogon Software SAS Library
sbe.dll	6.6.9600.17415	DirectShow Stream Buffer Filter.
sbeio.dll	12.0.9600.17415	Stream Buffer IO DLL
sberes.dll	6.6.9600.16384	DirectShow Stream Buffer Filter Resouces.
scansetting.dll	6.3.9600.17415	Microsoft® Windows(TM) ScanSettings Profile and Scanning implementation
scarddlg.dll	6.3.9600.17415	SCardDlg - Smart Card Common Dialog
scecli.dll	6.3.9600.17415	Windows Security Configuration Editor Client Engine
scesrv.dll	6.3.9600.17552	Windows Security Configuration Editor Engine
schannel.dll	6.3.9600.17728	TLS / SSL Security Provider
schedcli.dll	6.3.9600.17415	Scheduler Service Client DLL

scksp.dll	6.3.9600.17415	Microsoft Smart Card Key Storage Provider
scripto.dll	6.6.9600.17415	Microsoft ScriptO
scrobj.dll	5.8.9600.17415	Windows ® Script Component Runtime
scrptadm.dll	6.3.9600.17415	Script Adm Extension
scrrun.dll	5.8.9600.17415	Microsoft ® Script Runtime
sdiageng.dll	6.3.9600.17415	Scripted Diagnostics Execution Engine
sdiagprv.dll	6.3.9600.17415	Windows Scripted Diagnostic Provider API
sdohlp.dll	6.3.9600.17415	NPS SDO Helper Component
searchfolder.dll	6.3.9600.17415	SearchFolder
sechost.dll	6.3.9600.17734	Host for SCM/SDDL/LSA Lookup APIs
secproc.dll	6.3.9600.17415	Windows Rights Management Desktop Security Processor
secproc_isv.dll	6.3.9600.17415	Windows Rights Management Desktop Security Processor
secproc_ssp.dll	6.3.9600.17415	Windows Rights Management Services Server Security Processor
secproc_ssp_isv.dll	6.3.9600.17415	Windows Rights Management Services Server Security Processor (Pre-production)
secur32.dll	6.3.9600.17415	Security Support Provider Interface
security.dll	6.3.9600.16384	Security Support Provider Interface
sendmail.dll	6.3.9600.17415	Send Mail
sensapi.dll	6.3.9600.17415	SENS Connectivity API DLL
sensorsapi.dll	6.3.9600.17415	Sensor API
sensorscpl.dll	6.3.9600.17415	Open Location and Other Sensors
serialui.dll	6.3.9600.17415	Serial Port Property Pages
serwvdrv.dll	6.3.9600.17415	Unimodem Serial Wave driver
sessenv.dll	6.3.9600.17415	Remote Desktop Configuration service
settingmonitor.dll	6.3.9600.17415	Setting Synchronization Change Monitor
settingsync.dll	6.3.9600.17415	Setting Synchronization
settingsynccore.dll	6.3.9600.17415	Setting Synchronization Core
settingsyncpolicy.dll	6.3.9600.17415	SettingSync Policy
setupapi.dll	6.3.9600.17415	Windows Setup API
setupcln.dll	6.3.9600.17415	Setup Files Cleanup
sfc.dll	6.3.9600.16384	Windows File Protection
sfc_os.dll	6.3.9600.17415	Windows File Protection
shacct.dll	6.3.9600.17415	Shell Accounts Classes
shcore.dll	6.3.9600.17666	SHCORE
shdocvw.dll	6.3.9600.17415	Shell Doc Object and Control Library
shell32.dll	6.3.9600.17680	Windows Shell Common Dll
shellstyle.dll	6.3.9600.16384	Windows Shell Style Resource Dll
shfolder.dll	6.3.9600.17415	Shell Folder Service
shgina.dll	6.3.9600.17415	Windows Shell User Logon
shimeng.dll	6.3.9600.17415	Shim Engine DLL
shimgvw.dll	6.3.9600.17415	Photo Gallery Viewer
shlwapi.dll	6.3.9600.17415	Shell Light-weight Utility Library
shpafact.dll	6.3.9600.17415	Windows Shell LUA/PA Elevation Factory Dll
shsetup.dll	6.3.9600.17415	Shell setup helper
shsvcs.dll	6.3.9600.17415	Windows Shell Services Dll
shunimpl.dll	6.3.9600.17415	Windows Shell Obsolete APIs
shwebsvc.dll	6.3.9600.17415	Windows Shell Web Services
signdrv.dll	6.3.9600.17415	WMI provider for Signed Drivers
simauth.dll	6.3.9600.17415	EAP SIM run-time dll
simcfg.dll	6.3.9600.17415	EAP SIM config dll
sisbkup.dll	6.3.9600.17415	Single-Instance Store Backup Support Functions
skydriveshell.dll	6.3.9600.17416	Microsoft OneDrive Shell Extension
slc.dll	6.3.9600.17031	Software Licensing Client Dll
slcext.dll	6.3.9600.16384	Software Licensing Client Extension Dll
slpts.dll	6.3.9600.17415	Sleep Study Troubleshooter

slwga.dll	6.3.9600.16384	Software Licensing WGA API
smartcardcredentialprovider.dll	6.3.9600.17415	Windows Smartcard Credential Provider
smbhelperclass.dll	1.0.0.1	SMB (File Sharing) Helper Class for Network Diagnostic Framework
smphost.dll	6.3.9600.17415	Storage Management Provider (SMP) host service
sndvolsso.dll	6.3.9600.17415	SCA Volume
snmpapi.dll	6.3.9600.17415	SNMP Utility Library
softkbd.dll	6.3.9600.17415	Soft Keyboard Server and Tip
softpub.dll	6.3.9600.17415	Softpub Forwarder DLL
sortserver2003compat.dll	6.3.9600.17415	Sort Version Server 2003
sortwindows61.dll	6.3.9600.17415	SortWindows61 Dll
sortwindows6compat.dll	6.3.9600.17415	Sort Version Windows 6.0
spbcd.dll	6.3.9600.17415	BCD Sysprep Plugin
spfileq.dll	6.3.9600.17415	Windows SPFILEQ
spinf.dll	6.3.9600.17415	Windows SPINF
spnet.dll	6.3.9600.17415	Net Sysprep Plugin
spopk.dll	6.3.9600.17415	OPK Sysprep Plugin
spp.dll	6.3.9600.17415	Microsoft® Windows Shared Protection Point Library
sppc.dll	6.3.9600.17031	Software Licensing Client Dll
sppcext.dll	6.3.9600.16384	Software Protection Platform Client Extension Dll
sppinst.dll	6.3.9600.16384	SPP CMI Installer Plug-in DLL
sppwmi.dll	6.3.9600.16384	Software Protection Platform WMI provider
spwinsat.dll	6.3.9600.17415	WinSAT Sysprep Plugin
spwizeng.dll	6.3.9600.17415	Setup Wizard Framework
spwizimg.dll	6.3.9600.16384	Setup Wizard Framework Resources
spwizres.dll	6.3.9600.16384	Setup Wizard Framework Resources
spwmp.dll	6.3.9600.17415	Windows Media Player System Preparation DLL
sqlcecompact40.dll	4.0.8275.1	Database Repair Tool (32-bit)
sqlceoledb40.dll	4.0.9600.1	OLEDB Provider (32-bit)
sqlceqp40.dll	4.0.9600.1	Query Processor (32-bit)
sqlcese40.dll	4.0.9600.1	Storage Engine (32-bit)
sqloledb.dll	6.3.9600.17415	OLE DB Provider for SQL Server
sqlsrv32.dll	6.3.9600.17415	SQL Server ODBC Driver
sqlunirl.dll	2000.80.2039.0	String Function .DLL for SQL Enterprise Components
sqlwid.dll	2000.80.2039.0	Unicode Function .DLL for SQL Enterprise Components
sqlwoa.dll	2000.80.2040.0	Unicode/ANSI Function .DLL for SQL Enterprise Components
sqlxmlx.dll	6.3.9600.17415	XML extensions for SQL Server
sqmapi.dll	6.3.9600.17415	SQM Client
srchadmin.dll	7.0.9600.17415	Indexing Options
srclient.dll	6.3.9600.17415	Microsoft® Windows System Restore Client Library
srh.dll	6.3.9600.17666	Screen Reader Helper DLL
srm.dll	6.3.9600.17415	Microsoft® File Server Resource Manager Common Library
srm_ps.dll	6.3.9600.17415	Microsoft® FSRM internal proxy/stub
srmclient.dll	6.3.9600.17415	Microsoft® File Server Resource Management Client Extensions
srmlib.dll	6.3.9600.16384	Microsoft (R) File Server Resource Management Interop Assembly
srmscan.dll	6.3.9600.17415	Microsoft® File Server Storage Reports Scan Engine
srmshell.dll	6.3.9600.17415	Microsoft® File Server Resource Management Shell Extension
srmstormod.dll	6.3.9600.17415	Microsoft® File Server Resource Management Office Parser
srmtrace.dll	6.3.9600.17415	Microsoft® File Server Resource Management Tracing Library
srpuxnativesnapin.dll	6.3.9600.17415	Application Control Policies Group Policy Editor Extension
srumapi.dll	6.3.9600.17415	System Resource Usage Monitor API
srumsvc.dll	6.3.9600.17415	System Resource Usage Monitor Service
srvcli.dll	6.3.9600.17415	Server Service Client DLL
sscore.dll	6.3.9600.17415	Server Service Core DLL
ssdpapi.dll	6.3.9600.17415	SSDP Client API DLL

sspicli.dll	6.3.9600.17415	Security Support Provider Interface
ssshim.dll	6.3.9600.17415	Windows Componentization Platform Servicing API
startupscan.dll	6.3.9600.17415	Startup scan task DLL
stclient.dll	2001.12.10530.17415	COM+ Configuration Catalog Client
sti.dll	6.3.9600.17415	Still Image Devices client DLL
stobject.dll	6.3.9600.17415	Systray shell service object
storage.dll	3.10.0.103	Windows Win16 Application Launcher
storagecontexthandler.dll	6.3.9600.17668	Device Center Storage Context Menu Handler
storagewmi.dll	6.3.9600.17415	WMI Provider for Storage Management
storagewmi_passthru.dll	6.3.9600.17415	WMI PassThru Provider for Storage Management
storprop.dll	6.3.9600.17415	Property Pages for Storage Devices
storsvc.dll	6.3.9600.17415	Storage Services
structuredquery.dll	7.0.9600.17415	Structured Query
sud.dll	6.3.9600.17415	SUD Control Panel
sxproxy.dll	6.3.9600.17415	Microsoft® Windows System Protection Proxy Library
sxs.dll	6.3.9600.17415	Fusion 2.5
sxshared.dll	6.3.9600.17415	Microsoft® Windows SX Shared Library
sxsstore.dll	6.3.9600.17415	Sxs Store DLL
synccenter.dll	6.3.9600.17415	Microsoft Sync Center
synceng.dll	6.3.9600.17415	Windows Briefcase Engine
synchostps.dll	6.3.9600.17415	Proxystub for sync host
syncinfrastructure.dll	6.3.9600.17415	Microsoft Windows Sync Infrastructure.
syncinfrastructureps.dll	6.3.9600.17415	Microsoft Windows sync infrastructure proxy stub.
syncreg.dll	2007.94.9600.17415	Microsoft Synchronization Framework Registration
syncui.dll	6.3.9600.17415	Windows Briefcase
syssetup.dll	6.3.9600.17415	Windows NT System Setup
systemcpl.dll	6.3.9600.17415	My System CPL
systemeventsbrokerclient.dll	6.3.9600.17415	system Events Broker Client Library
t2embed.dll	6.3.9600.17415	Microsoft T2Embed Font Embedding
tapi3.dll	6.3.9600.17415	Microsoft TAPI3
tapi32.dll	6.3.9600.17415	Microsoft® Windows(TM) Telephony API Client DLL
tapimigplugin.dll	6.3.9600.17415	Microsoft® Windows(TM) TAPI Migration Plugin Dll
tapiperf.dll	6.3.9600.17415	Microsoft® Windows(TM) Telephony Performance Monitor
tapisrv.dll	6.3.9600.17415	Microsoft® Windows(TM) Telephony Server
tapisysprep.dll	6.3.9600.17415	Microsoft® Windows(TM) Telephony Sysprep Work
tapiui.dll	6.3.9600.16384	Microsoft® Windows(TM) Telephony API UI DLL
taskcomp.dll	6.3.9600.17415	Task Scheduler Backward Compatibility Plug-in
taskschd.dll	6.3.9600.17415	Task Scheduler COM API
taskschdps.dll	6.3.9600.17415	Task Scheduler Interfaces Proxy
tbs.dll	6.3.9600.17415	TBS
tcpipcfg.dll	6.3.9600.17415	Network Configuration Objects
tcpmib.dll	6.3.9600.17415	Standard TCP/IP Port Monitor Helper DLL
tcpmonui.dll	6.3.9600.17415	Standard TCP/IP Port Monitor UI DLL
tdh.dll	6.3.9600.17734	Event Trace Helper Library
termmgr.dll	6.3.9600.17415	Microsoft TAPI3 Terminal Manager
themecpl.dll	6.3.9600.17415	Personalization CPL
themeui.dll	6.3.9600.17415	Windows Theme API
threadpoolwinrt.dll	6.3.9600.17415	Windows WinRT Threadpool
thumbcache.dll	6.3.9600.17415	Microsoft Thumbnail Cache
timebrokerclient.dll	6.3.9600.17415	Time Broker Client Library
timedatemuicallback.dll	6.3.9600.17415	Time Date Control UI Language Change plugin
tlscsp.dll	6.3.9600.17415	Microsoft® Remote Desktop Services Cryptographic Utility
tpmcompc.dll	6.3.9600.17415	Computer Chooser Dialog
tquery.dll	7.0.9600.17415	Microsoft Tripoli Query

traffic.dll	6.3.9600.17415	Microsoft Traffic Control 1.0 DLL
tsbyuv.dll	6.3.9600.17415	Toshiba Video Codec
tschannel.dll	6.3.9600.17415	Task Scheduler Proxy
tsgqec.dll	6.3.9600.17415	RD Gateway QEC
tsmf.dll	6.3.9600.17415	RDP MF Plugin
tspkg.dll	6.3.9600.17415	Web Service Security Package
tsworkspace.dll	6.3.9600.17415	RemoteApp and Desktop Connection Component
ttlsauth.dll	6.3.9600.17415	EAP TTLS run-time dll
ttlscfg.dll	6.3.9600.17415	EAP TTLS configuration dll
ttlsext.dll	6.3.9600.17415	Windows Extension library for EAP TTLS
tvratings.dll	6.6.9600.17415	Module for managing TV ratings
twext.dll	6.3.9600.17415	Previous Versions property page
twinapi.appcore.dll	6.3.9600.17415	twinapi.appcore
twinapi.dll	6.3.9600.17415	twinapi
twinui.appcore.dll	6.3.9600.17415	TWINUI.APPCORE
twinui.dll	6.3.9600.17415	TWINUI
txflog.dll	2001.12.10530.17415	COM+
txfw32.dll	6.3.9600.17415	TxF Win32 DLL
typelib.dll	3.10.0.103	Windows Win16 Application Launcher
tzres.dll	6.3.9600.16384	Time Zones resource DLL
ucmhc.dll	6.3.9600.17415	UCM Helper Class
udhisapi.dll	6.3.9600.17415	UPnP Device Host ISAPI Extension
uexfat.dll	6.3.9600.17415	eXfat Utility DLL
ufat.dll	6.3.9600.17415	FAT Utility DLL
uianimation.dll	6.3.9600.17415	Windows Animation Manager
uiautomationcore.dll	7.2.9600.17415	Microsoft UI Automation Core
uiautomationcoreres.dll	7.2.9600.16384	Microsoft UI Automation Core Resource
uicom.dll	6.3.9600.17415	Add/Remove Modems
uireng.dll	6.3.9600.17415	UI Recording Engine Library
uiribbon.dll	6.3.9600.17415	Windows Ribbon Framework
uiribbonres.dll	6.3.9600.17415	Windows Ribbon Framework Resources
ulib.dll	6.3.9600.17415	File Utilities Support DLL
umdmxfrm.dll	6.3.9600.17415	Unimodem Tranform Module
unimdmat.dll	6.3.9600.17415	Unimodem Service Provider AT Mini Driver
uniplat.dll	6.3.9600.17415	Unimodem AT Mini Driver Platform Driver for Windows NT
untfs.dll	6.3.9600.17481	NTFS Utility DLL
upnp.dll	6.3.9600.17415	UPnP Control Point API
upnphost.dll	6.3.9600.17415	UPnP Device Host
urefs.dll	6.3.9600.16384	NTFS Utility DLL
ureg.dll	6.3.9600.17415	Registry Utility DLL
url.dll	11.0.9600.17416	Internet Shortcut Shell Extension DLL
urlmon.dll	11.0.9600.17728	OLE32 Extensions for Win32
usbceip.dll	6.3.9600.17415	USBCEIP Task
usbperf.dll	6.3.9600.17415	USB Performance Objects DLL
usbui.dll	6.3.9600.17415	USB UI Dll
user32.dll	6.3.9600.17415	Multi-User Windows USER API Client DLL
useraccountcontrolsettings.dll	6.3.9600.17415	UserAccountControlSettings
usercpl.dll	6.3.9600.17415	User control panel
userenv.dll	6.3.9600.17415	Userenv
userinitext.dll	6.3.9600.17415	UserInit Utility Extension DLL
userlanguageprofilecallback.dll	6.3.9600.17415	MUI Callback for User Language profile changed
userlanguagescpl.dll	6.3.9600.17415	My Languages Configuration Control Panel
usp10.dll	6.3.9600.17415	Uniscribe Unicode script processor
ustprov.dll	6.3.9600.17415	User State WMI Provider

utildll.dll	6.3.9600.17415	WinStation utility support DLL
uudf.dll	6.3.9600.17415	UDF Utility DLL
uxinit.dll	6.3.9600.17415	Windows User Experience Session Initialization Dll
uxlib.dll	6.3.9600.17415	Setup Wizard Framework
uxlibres.dll	6.3.9600.16384	UXLib Resources
uxtheme.dll	6.3.9600.17415	Microsoft UxTheme Library
van.dll	6.3.9600.17415	View Available Networks
vault.dll	6.3.9600.17415	Windows vault Control Panel
vaultcli.dll	6.3.9600.17415	Credential Vault Client Library
vbajet32.dll	6.0.1.9431	Visual Basic for Applications Development Environment - Expression Service Loader
vbscript.dll	5.8.9600.17728	Microsoft ® VBScript
vcomp100.dll	10.0.40219.325	Microsoft® C/C++ OpenMP Runtime
vdmdbg.dll	6.3.9600.17415	VDMDBG.DLL
vds_ps.dll	6.3.9600.17415	Microsoft® Virtual Disk Service proxy/stub
verifier.dll	6.3.9600.17415	Standard application verifier provider dll
version.dll	6.3.9600.17415	Version Checking and File Installation Libraries
vfwwdm32.dll	6.3.9600.17415	VfW MM Driver for WDM Video Capture Devices
vidreszr.dll	6.3.9600.17415	Windows Media Resizer
virtdisk.dll	6.3.9600.17415	Virtual Disk API DLL
vpnikeapi.dll	6.3.9600.17415	VPN IKE API's
vscmgrps.dll	6.3.9600.17415	Microsoft Virtual Smart Card Manager Proxy/Stub
vss_ps.dll	6.3.9600.17415	Microsoft® Volume Shadow Copy Service proxy/stub
vssapi.dll	6.3.9600.17466	Microsoft® Volume Shadow Copy Requestor/Writer Services API DLL
vsstrace.dll	6.3.9600.17466	Microsoft® Volume Shadow Copy Service Tracing Library
w32topl.dll	6.3.9600.17415	Windows NT Topology Maintenance Tool
wab32.dll	6.3.9600.17415	Microsoft (R) Contacts DLL
wab32res.dll	6.3.9600.16384	Microsoft (R) Contacts DLL
wabsyncprovider.dll	6.3.9600.17415	Microsoft Windows Contacts Sync Provider
wavemsp.dll	6.3.9600.17415	Microsoft Wave MSP
wbemcomn.dll	6.3.9600.17415	WMI
wcmapi.dll	6.3.9600.17415	Windows Connection Manager Client API
wcnapi.dll	6.3.9600.17415	Windows Connect Now - API Helper DLL
wcnwiz.dll	6.3.9600.17415	Windows Connect Now Wizards
wcspluginservice.dll	6.3.9600.17415	WcsPlugInService DLL
wdc.dll	6.3.9600.17415	Performance Monitor
wdi.dll	6.3.9600.17415	Windows Diagnostic Infrastructure
wdigest.dll	6.3.9600.17415	Microsoft Digest Access
wdscore.dll	6.3.9600.17415	Panther Engine Module
webcamui.dll	6.3.9600.17415	Microsoft® Windows® Operating System
webcheck.dll	11.0.9600.17689	Web Site Monitor
webclnt.dll	6.3.9600.17415	Web DAV Service DLL
webio.dll	6.3.9600.17415	Web Transfer Protocols API
webservices.dll	6.3.9600.17415	Windows Web Services Runtime
websocket.dll	6.3.9600.17415	Web Socket API
wecapi.dll	6.3.9600.17415	Event Collector Configuration API
wer.dll	6.3.9600.17550	Windows Error Reporting DLL
werdiagcontroller.dll	6.3.9600.17415	WER Diagnostic Controller
werui.dll	6.3.9600.17415	Windows Error Reporting UI DLL
wevtapi.dll	6.3.9600.17415	Eventing Consumption and Configuration API
wevtfwd.dll	6.3.9600.17415	WS-Management Event Forwarding Plug-in
wfapigp.dll	6.3.9600.17415	Windows Firewall GPO Helper dll
wfdprov.dll	6.3.9600.17415	Private WPS provisioning API DLL for Wi-Fi Direct
wfhc.dll	6.3.9600.17415	Windows Firewall Helper Class
whhelper.dll	6.3.9600.17415	Net shell helper DLL for winHttp

wiaaut.dll	6.3.9600.17415	WIA Automation Layer
wiadefui.dll	6.3.9600.17415	WIA Scanner Default UI
wiadss.dll	6.3.9600.17415	WIA TWAIN compatibility layer
wiascanprofiles.dll	6.3.9600.17415	Microsoft Windows ScanProfiles
wiashext.dll	6.3.9600.17415	Imaging Devices Shell Folder UI
wiatrace.dll	6.3.9600.17415	WIA Tracing
wimgapi.dll	6.3.9600.17415	Windows Imaging Library
winbio.dll	6.3.9600.17415	Windows Biometrics Client API
winbrand.dll	6.3.9600.17415	Windows Branding Resources
wincorlib.dll	6.3.9600.17415	Microsoft Windows ® WinRT core library
wincredprovider.dll	6.3.9600.17415	wincredprovider DLL
windows.applicationmodel.background.systemeventsbroker.dll	6.3.9600.17415	Windows Background System Events Broker API Server
windows.applicationmodel.background.timebroker.dll	6.3.9600.17415	Windows Background Time Broker API Server
windows.applicationmodel.dll	6.3.9600.17415	Windows ApplicationModel API Server
windows.applicationmodel.store.dll	6.3.9600.17415	Windows Store Runtime DLL
windows.applicationmodel.store.testingframework.dll	6.3.9600.17669	Windows Store Testing Framework Runtime DLL
windows.data.pdf.dll	6.3.9600.17415	PDF WinRT APIs
windows.devices.background.dll	6.3.9600.17415	Windows.Devices.Background
windows.devices.background.ps.dll	6.3.9600.17415	Windows.Devices.Background Interface Proxy
windows.devices.bluetooth.dll	6.3.9600.17415	Windows.Devices.Bluetooth DLL
windows.devices.custom.dll	6.3.9600.17415	Windows.Devices.Custom
windows.devices.custom.ps.dll	6.3.9600.17415	Windows.Devices.Custom Interface Proxy
windows.devices.enumeration.dll	6.3.9600.17415	Windows.Devices.Enumeration
windows.devices.enumeration.ps.dll	6.3.9600.17415	Windows.Devices.Enumeration Interface Proxy
windows.devices.geolocation.dll	6.3.9600.17415	Geolocation Runtime DLL
windows.devices.humaninterfacedevice.dll	6.3.9600.17415	Windows.Devices.HumanInterfaceDevice DLL
windows.devices.pointofservice.dll	6.3.9600.17415	Windows Runtime PointOfService DLL
windows.devices.portable.dll	6.3.9600.17415	Windows Runtime Portable Devices DLL
windows.devices.printers.extensions.dll	6.3.9600.17415	Windows.Devices.Printers.Extensions
windows.devices.scanners.dll	6.3.9600.17415	Windows Runtime Devices Scanners DLL
windows.devices.sensors.dll	6.3.9600.17415	Windows Runtime Sensors DLL
windows.devices.smartcards.dll	6.3.9600.17415	Windows Runtime Smart Card API DLL
windows.devices.usb.dll	6.3.9600.17415	Windows Runtime Usb DLL
windows.devices.wifidirect.dll	6.3.9600.17415	Windows.Devices.WiFiDirect DLL
windows.globalization.dll	6.3.9600.17415	Windows Globalization
windows.globalization.fontgroups.dll	6.3.9600.17415	Fonts Mapping API
windows.graphics.dll	6.3.9600.17415	WinRT Windows Graphics DLL
windows.graphics.printing.dll	6.3.9600.17415	Microsoft Windows Printing Support
windows.management.workplace.workplacesettings.dll	6.3.9600.17415	Windows Runtime WorkplaceSettings DLL
windows.media.devices.dll	6.3.9600.17415	Windows Runtime media device server DLL
windows.media.dll	6.3.9600.17415	Windows Media Runtime DLL
windows.media.mediacontrol.dll	6.3.9600.17415	Windows Runtime MediaControl server DLL
windows.media.speechsynthesis.dll	6.3.9600.17415	Windows Speech Runtime DLL
windows.media.streaming.dll	12.0.9600.17415	DLNA DLL
windows.media.streaming.ps.dll	12.0.9600.17415	DLNA Proxy-Stub DLL
windows.networking.backgroundtransfer.dll	6.3.9600.17415	Windows.Networking.BackgroundTransfer DLL
windows.networking.connectivity.dll	6.3.9600.17415	Windows Networking Connectivity Runtime DLL
windows.networking.dll	6.3.9600.17415	Windows.Networking DLL
windows.networking.hostname.dll	6.3.9600.17415	Windows.Networking.HostName DLL
windows.networking.networkoperators.hotspotauthentication.dll	6.3.9600.17415	Microsoft Windows Hotspot Authentication API
windows.networking.proximity.dll	6.3.9600.17415	Windows Runtime Proximity API DLL
windows.networking.sockets.pushenabledapplication.dll	6.3.9600.17415	Windows.Networking.Sockets.PushEnabledApplication DLL
windows.security.authentication.onlineid.dll	6.3.9600.17415	Windows Runtime OnlineId Authentication DLL
windows.security.credentials.ui.credentialpicker.dll	6.3.9600.17415	WinRT Credential Picker Server

windows.security.credentials.ui.userconsentverifier.dll	6.3.9600.17415	Windows User Consent Verifier API
windows.shell.search.urihandler.dll	6.3.9600.17415	Windows Search URI Handler
windows.storage.applicationdata.dll	6.3.9600.17415	Windows Application Data API Server
windows.storage.compression.dll	6.3.9600.17415	WinRT Compression
windows.system.display.dll	6.3.9600.17415	Windows System Display Runtime DLL
windows.system.profile.hardwareid.dll	6.3.9600.17415	Windows System Profile HardwareId DLL
windows.system.profile.systemmanufacturers.dll	6.3.9600.17415	Windows.System.Profile.SystemManufacturers
windows.system.remotedesktop.dll	6.3.9600.17415	Windows System RemoteDesktop Runtime DLL
windows.ui.dll	6.3.9600.17415	Windows Runtime UI Foundation DLL
windows.ui.immersive.dll	6.3.9600.17415	WINDOWS.UI.IMMERSIVE
windows.ui.input.inking.dll	6.3.9600.17719	WinRT Windows Inking DLL
windows.ui.search.dll	6.3.9600.17415	Windows.UI.Search
windows.ui.xaml.dll	6.3.9600.17477	Windows.UI.Xaml dll
windows.web.dll	6.3.9600.17415	Web Client DLL
windows.web.http.dll	6.3.9600.17415	Windows.Web.Http DLL
windowscodecs.dll	6.3.9600.17669	Microsoft Windows Codecs Library
windowscodecsext.dll	6.3.9600.17415	Microsoft Windows Codecs Extended Library
windowslivelogin.dll	6.3.9600.17415	Microsoft® Account Login Helper
winfax.dll	6.3.9600.17415	Microsoft Fax API Support DLL
winhttp.dll	6.3.9600.17415	Windows HTTP Services
wininet.dll	11.0.9600.17728	Internet Extensions for Win32
wininitext.dll	6.3.9600.17415	WinInit Utility Extension DLL
winipsec.dll	6.3.9600.17415	Windows IPsec SPD Client DLL
winlangdb.dll	6.3.9600.17415	Windows Bcp47 Language Database
winmde.dll	12.0.9600.17415	WinMDE DLL
winmm.dll	6.3.9600.17415	MCI API DLL
winmmbase.dll	6.3.9600.17415	Base Multimedia Extension API DLL
winmsoirmprotector.dll	6.3.9600.17415	Windows Office file format IRM Protector
winnsi.dll	6.3.9600.17415	Network Store Information RPC interface
winopcirmprotector.dll	6.3.9600.17415	Windows Office file format IRM Protector
winrnr.dll	6.3.9600.17415	LDAP RnR Provider DLL
winrscmd.dll	6.3.9600.17415	remtsvc
winrsmgr.dll	6.3.9600.16384	WSMan Shell API
winrssrv.dll	6.3.9600.17415	winrssrv
winrttracing.dll	6.3.9600.17415	Windows Diagnostics Tracing
winsatapi.dll	6.3.9600.17415	Windows System Assessment Tool API
winscard.dll	6.3.9600.17475	Microsoft Smart Card API
winshfhc.dll	6.3.9762.0	File Risk Estimation
winsku.dll	6.3.9600.17415	Windows SKU Library
winsockhc.dll	6.3.9600.17415	Winsock Network Diagnostic Helper Class
winsrpc.dll	6.3.9600.17415	WINS RPC LIBRARY
winsta.dll	6.3.9600.17415	Winstation Library
winsync.dll	2007.94.9600.17415	Synchronization Framework
winsyncmetastore.dll	2007.94.9600.17415	Windows Synchronization Metadata Store
winsyncproviders.dll	2007.94.9600.17415	Windows Synchronization Provider Framework
wintrust.dll	6.3.9600.17415	Microsoft Trust Verification APIs
wintypes.dll	6.3.9600.17415	Windows Base Types DLL
winusb.dll	6.3.9600.17415	Windows USB Driver User Library
wisp.dll	6.3.9600.17415	Microsoft Pen and Touch Input Component
wkscli.dll	6.3.9600.17415	Workstation Service Client DLL
wkspbrokerax.dll	6.3.9600.17415	Microsoft Workspace Broker ActiveX Control
wksprtps.dll	6.3.9600.17415	WorkspaceRuntime ProxyStub DLL
wlanapi.dll	6.3.9600.17415	Windows WLAN AutoConfig Client Side API DLL
wlancfg.dll	6.3.9600.17415	Wlan Netsh Helper DLL

wlanconn.dll	6.3.9600.17415	Dot11 Connection Flows
wlandlg.dll	6.3.9600.17415	Wireless Lan Dialog Wizards
wlangpui.dll	6.3.9600.17415	Wireless Network Policy Management Snap-in
wlanhlp.dll	6.3.9600.17415	Windows Wireless LAN 802.11 Client Side Helper API
wlaninst.dll	6.3.9600.17415	Windows NET Device Class Co-Installer for Wireless LAN
wlanmm.dll	6.3.9600.17415	Dot11 Media and AdHoc Managers
wlanmsm.dll	6.3.9600.17415	Windows Wireless LAN 802.11 MSM DLL
wlanpref.dll	6.3.9600.17415	Wireless Preferred Networks
wlansec.dll	6.3.9600.17415	Windows Wireless LAN 802.11 MSM Security Module DLL
wlanui.dll	6.3.9600.17415	Wireless Profile UI
wlanutil.dll	6.3.9600.16384	Windows Wireless LAN 802.11 Utility DLL
wldap32.dll	6.3.9600.17415	Win32 LDAP API DLL
wlgpclnt.dll	6.3.9600.17415	802.11 Group Policy Client
wlidcli.dll	6.3.9600.17415	Microsoft® Account Dynamic Link Library
wlidcredprov.dll	6.3.9600.17415	Microsoft® Account Credential Provider
wlidfdp.dll	6.3.9600.17415	Microsoft® Account Function Discovery Provider
wlidnsp.dll	6.3.9600.17415	Microsoft® Account Namespace Provider
wlidprov.dll	6.3.9600.17415	Microsoft® Account Provider
wlidres.dll	6.3.9600.16384	Microsoft® Windows Live ID Resource
wls0wndh.dll	6.3.9600.17415	Session0 Viewer Window Hook DLL
wmadmod.dll	6.3.9600.17415	Windows Media Audio Decoder
wmadmoe.dll	6.3.9600.17415	Windows Media Audio 10 Encoder/Transcoder
wmasf.dll	12.0.9600.17415	Windows Media ASF DLL
wmcodecdspps.dll	6.3.9600.17415	Windows Media CodecDSP Proxy Stub Dll
wmdmlog.dll	12.0.9600.17415	Windows Media Device Manager Logger
wmdmps.dll	12.0.9600.17415	Windows Media Device Manager Proxy Stub
wmdrmdev.dll	12.0.9600.17415	Windows Media DRM for Network Devices Registration DLL
wmdrmnet.dll	12.0.9600.17415	Windows Media DRM for Network Devices DLL
wmdrmsdk.dll	11.0.9600.17415	Windows Media DRM SDK DLL
wmerror.dll	12.0.9600.16384	Windows Media Error Definitions (English)
wmi.dll	6.3.9600.17415	WMI DC and DP functionality
wmiclnt.dll	6.3.9600.17415	WMI Client API
wmidcom.dll	6.3.9600.17415	WMI
wmidx.dll	12.0.9600.17415	Windows Media Indexer DLL
wmiprop.dll	6.3.9600.17415	WDM Provider Dynamic Property Page CoInstaller
wmitomi.dll	6.3.9600.17415	CIM Provider Adapter
wmnetmgr.dll	12.0.9600.17415	Windows Media Network Plugin Manager DLL
wmp.dll	12.0.9600.17415	Windows Media Player
wmpdui.dll	12.0.9600.17415	Windows Media Player UI Engine
wmpdxm.dll	12.0.9600.17415	Windows Media Player Extension
wmpeffects.dll	12.0.9600.17415	Windows Media Player Effects
wmphoto.dll	6.3.9600.17668	Windows Media Photo Codec
wmploc.dll	12.0.9600.16384	Windows Media Player Resources
wmpps.dll	12.0.9600.17415	Windows Media Player Proxy Stub Dll
wmpshell.dll	12.0.9600.17415	Windows Media Player Launcher
wmsgapi.dll	6.3.9600.17415	WinLogon IPC Client
wmspdmod.dll	6.3.9600.17415	Windows Media Audio Voice Decoder
wmspdmoe.dll	6.3.9600.17415	Windows Media Audio Voice Encoder
wmvcore.dll	12.0.9600.17415	Windows Media Playback/Authoring DLL
wmvdecod.dll	6.3.9600.17415	Windows Media Video Decoder
wmvdspa.dll	6.3.9600.17415	Windows Media Video DSP Components - Advanced
wmvencod.dll	6.3.9600.17415	Windows Media Video 9 Encoder
wmvsdecd.dll	6.3.9600.17415	Windows Media Screen Decoder
wmvsencd.dll	6.3.9600.17415	Windows Media Screen Encoder

wmvxencd.dll	6.3.9600.17415	Windows Media Video Encoder
workfoldersres.dll	6.2.9200.16384	Work Folders Resources
wow32.dll	6.3.9600.17475	Wow32
wpc.dll	6.3.9600.17415	WPC Settings Library
wpcsvc.dll	6.3.9600.17415	WPC Filtering Service
wpdshext.dll	6.3.9600.17702	Portable Devices Shell Extension
wpdshserviceobj.dll	6.3.9600.17415	Windows Portable Device Shell Service Object
wpdsp.dll	6.3.9600.17415	WMDM Service Provider for Windows Portable Devices
wpnapps.dll	6.3.9600.17415	Windows Push Notification Apps
ws2_32.dll	6.3.9600.17415	Windows Socket 2.0 32-Bit DLL
ws2help.dll	6.3.9600.17415	Windows Socket 2.0 Helper for Windows NT
wscapi.dll	6.3.9600.17415	Windows Security Center API
wscinterop.dll	6.3.9600.17415	Windows Health Center WSC Interop
wscisvif.dll	6.3.9600.17415	Windows Security Center ISV API
wsclient.dll	6.3.9600.17415	Windows Store Licensing Client
wscproxystub.dll	6.3.9600.17415	Windows Security Center ISV Proxy Stub
wsdapi.dll	6.3.9600.17481	Web Services for Devices API DLL
wsdchngr.dll	6.3.9600.17415	WSD Challenge Component
wsecedit.dll	6.3.9600.17415	Security Configuration UI Module
wshbth.dll	6.3.9600.17415	Windows Sockets Helper DLL
wshcon.dll	5.8.9600.17415	Microsoft ® Windows Script Controller
wshelper.dll	6.3.9600.17415	Winsock Net shell helper DLL for winsock
wshext.dll	5.8.9600.17415	Microsoft ® Shell Extension for Windows Script Host
wship6.dll	6.3.9600.17415	Winsock2 Helper DLL (TL/IPv6)
wshirda.dll	6.3.9600.17415	Windows Sockets Helper DLL
wshqos.dll	6.3.9600.17415	QoS Winsock2 Helper DLL
wshrm.dll	6.3.9600.17415	Windows Sockets Helper DLL for PGM
wshtcpip.dll	6.3.9600.17415	Winsock2 Helper DLL (TL/IPv4)
wsmagent.dll	6.3.9600.17415	WinRM Agent
wsmanmigrationplugin.dll	6.3.9600.17415	WinRM Migration Plugin
wsmauto.dll	6.3.9600.17415	WSMAN Automation
wsmplpxy.dll	6.3.9600.17415	wsmplpxy
wsmres.dll	6.3.9600.16384	WSMan Resource DLL
wsmsvc.dll	6.3.9600.17415	WSMan Service
wsmwmipl.dll	6.3.9600.17415	WSMAN WMI Provider
wsnmp32.dll	6.3.9600.17415	Microsoft WinSNMP v2.0 Manager API
wsock32.dll	6.3.9600.17415	Windows Socket 32-Bit DLL
wsshared.dll	6.3.9600.17669	WSShared DLL
wssync.dll	6.3.9600.17415	Windows Store Licensing Sync Client
wtsapi32.dll	6.3.9600.17415	Windows Remote Desktop Session Host Server SDK APIs
wuapi.dll	7.9.9600.17729	Windows Update Client API
wudriver.dll	7.9.9600.17729	Windows Update WUDriver Stub
wups.dll	7.9.9600.17729	Windows Update client proxy stub
wuwebv.dll	7.9.9600.17729	Windows Update Vista Web Control
wvc.dll	6.3.9600.17415	Windows Visual Components
wwaapi.dll	6.3.9600.17415	Microsoft Web Application Host API library
wwanapi.dll	6.3.9600.17415	Mbnapi
wwapi.dll	8.1.9600.17415	WWAN API
x3daudio1_0.dll	9.11.519.0	X3DAudio
x3daudio1_1.dll	9.15.779.0	X3DAudio
x3daudio1_2.dll	9.21.1148.0	X3DAudio
x3daudio1_3.dll	9.22.1284.0	X3DAudio
x3daudio1_4.dll	9.23.1350.0	X3DAudio
x3daudio1_5.dll	9.25.1476.0	X3DAudio

x3daudio1_6.dll	9.26.1590.0	3D Audio Library
x3daudio1_7.dll	9.28.1886.0	3D Audio Library
xactengine2_0.dll	9.11.519.0	XACT Engine API
xactengine2_1.dll	9.12.589.0	XACT Engine API
xactengine2_10.dll	9.21.1148.0	XACT Engine API
xactengine2_2.dll	9.13.644.0	XACT Engine API
xactengine2_3.dll	9.14.701.0	XACT Engine API
xactengine2_4.dll	9.15.779.0	XACT Engine API
xactengine2_5.dll	9.16.857.0	XACT Engine API
xactengine2_6.dll	9.17.892.0	XACT Engine API
xactengine2_7.dll	9.18.944.0	XACT Engine API
xactengine2_8.dll	9.19.1007.0	XACT Engine API
xactengine2_9.dll	9.20.1057.0	XACT Engine API
xactengine3_0.dll	9.22.1284.0	XACT Engine API
xactengine3_1.dll	9.23.1350.0	XACT Engine API
xactengine3_2.dll	9.24.1400.0	XACT Engine API
xactengine3_3.dll	9.25.1476.0	XACT Engine API
xactengine3_4.dll	9.26.1590.0	XACT Engine API
xactengine3_5.dll	9.27.1734.0	XACT Engine API
xactengine3_6.dll	9.28.1886.0	XACT Engine API
xactengine3_7.dll	9.29.1962.0	XACT Engine API
xapofx1_0.dll	9.23.1350.0	XAPOFX
xapofx1_1.dll	9.24.1400.0	XAPOFX
xapofx1_2.dll	9.25.1476.0	XAPOFX
xapofx1_3.dll	9.26.1590.0	Audio Effect Library
xapofx1_4.dll	9.28.1886.0	Audio Effect Library
xapofx1_5.dll	9.29.1962.0	Audio Effect Library
xaudio2_0.dll	9.22.1284.0	XAudio2 Game Audio API
xaudio2_1.dll	9.23.1350.0	XAudio2 Game Audio API
xaudio2_2.dll	9.24.1400.0	XAudio2 Game Audio API
xaudio2_3.dll	9.25.1476.0	XAudio2 Game Audio API
xaudio2_4.dll	9.26.1590.0	XAudio2 Game Audio API
xaudio2_5.dll	9.27.1734.0	XAudio2 Game Audio API
xaudio2_6.dll	9.28.1886.0	XAudio2 Game Audio API
xaudio2_7.dll	9.29.1962.0	XAudio2 Game Audio API
xaudio2_8.dll	6.3.9600.17415	XAudio2 Game Audio API
xinput1_1.dll	9.12.589.0	Microsoft Common Controller API
xinput1_2.dll	9.14.701.0	Microsoft Common Controller API
xinput1_3.dll	9.18.944.0	Microsoft Common Controller API
xinput1_4.dll	6.3.9600.17415	Microsoft Common Controller API
xinput9_1_0.dll	6.3.9600.17415	XNA Common Controller
xmlfilter.dll	2008.0.9600.17415	XML Filter
xmllite.dll	6.3.9600.17415	Microsoft XmlLite Library
xmlprovi.dll	6.3.9600.17415	Network Provisioning Service Client API
xmlrw.dll	2011.110.2809.27	Microsoft XML Slim Library
xmlrwbin.dll	2011.110.2809.27	Microsoft XML Slim Library
xolehlp.dll	2001.12.10530.17415	Microsoft Distributed Transaction Coordinator Helper APIs DLL
xpsfilt.dll	6.3.9600.17415	XML Paper Specification Document IFilter
xpsgdiconverter.dll	6.3.9600.17415	XPS to GDI Converter
xpsprint.dll	6.3.9600.17415	XPS Printing DLL
xpsrasterservice.dll	6.3.9600.17415	XPS Rasterization Service Component
xpsservices.dll	6.3.9600.17415	Xps Object Model in memory creation and deserialization
xpsshhdr.dll	6.3.9600.17415	OPC Shell Metadata Handler
xpssvcs.dll	6.3.9600.17415	Native Code Xps Services Library

xwizards.dll	6.3.9600.17415	Extensible Wizards Manager Module
xwreg.dll	6.3.9600.17415	Extensible Wizard Registration Manager Module
xwtpdui.dll	6.3.9600.17415	Extensible Wizard Type Plugin for DUI
xwtpw32.dll	6.3.9600.17415	Extensible Wizard Type Plugin for Win32
zipfldr.dll	6.3.9600.17415	Compressed (zipped) Folders

Certificates

[Certificate Authorities / COMODO RSA Certification Authority]

Certificate Properties:

Version	V3
Signature Algorithm	SHA384 RSA (1.2.840.113549.1.1.12)
Serial Number	22 DE 84 FC A2 70 D7 AB 8E F3 49 EB 56 EE 66 27
Validity	5/30/2000 - 5/30/2020

Issuer Properties:

Common Name	AddTrust External CA Root
Organization	AddTrust AB
Organizational Unit	AddTrust External TTP Network
Country	Sweden

Subject Properties:

Common Name	COMODO RSA Certification Authority
Organization	COMODO CA Limited
Country	United Kingdom
Locality Name	Salford
State/Province	Greater Manchester

Public Key Properties:

Public Key Algorithm	RSA (1.2.840.113549.1.1.1)

[Certificate Authorities / Entrust Certification Authority - L1C]

Certificate Properties:

Version	V3
Signature Algorithm	SHA1 RSA (1.2.840.113549.1.1.5)
Serial Number	39 8C 0E 4C
Validity	11/11/2011 - 11/11/2021

Issuer Properties:

Common Name	Entrust.net Certification Authority (2048)
Organization	Entrust.net
Organizational Unit	www.entrust.net/CPS_2048 incorp. by ref. (limits liab.)
Organizational Unit	(c) 1999 Entrust.net Limited

Subject Properties:

Common Name	Entrust Certification Authority - L1C
Organization	Entrust, Inc.
Organizational Unit	www.entrust.net/rpa is incorporated by reference
Organizational Unit	(c) 2009 Entrust, Inc.

Country	United States

Public Key Properties:

Public Key Algorithm	RSA (1.2.840.113549.1.1.1)

[Certificate Authorities / Microsoft Update Secure Server CA 2.1]

Certificate Properties:

Version	V3
Signature Algorithm	SHA256 RSA (1.2.840.113549.1.1.11)
Serial Number	0A 00 00 00 00 00 DF A5 50 0A C8 A2 91 B8 0A 00 00 00 00 33
Validity	6/21/2012 - 6/21/2027

Issuer Properties:

Common Name	Microsoft Root Certificate Authority 2011
Organization	Microsoft Corporation
Country	United States
Locality Name	Redmond
State/Province	Washington

Subject Properties:

Common Name	Microsoft Update Secure Server CA 2.1
Organization	Microsoft Corporation
Country	United States
Locality Name	Redmond
State/Province	Washington

Public Key Properties:

Public Key Algorithm	RSA (1.2.840.113549.1.1.1)

[Certificate Authorities / Microsoft Windows Hardware Compatibility]

Certificate Properties:

Version	V3
Signature Algorithm	MD5 RSA (1.2.840.113549.1.1.4)
Serial Number	A0 69 FE 8F 9A 3F D1 11 8B 19
Validity	10/1/1997 - 12/31/2002

Issuer Properties:

Common Name	Microsoft Root Authority
Organizational Unit	Copyright (c) 1997 Microsoft Corp.
Organizational Unit	Microsoft Corporation

Subject Properties:

Common Name	Microsoft Windows Hardware Compatibility
Organizational Unit	Copyright (c) 1997 Microsoft Corp.
Organizational Unit	Microsoft Windows Hardware Compatibility Intermediate CA
Organizational Unit	Microsoft Corporation

Public Key Properties:

Public Key Algorithm	RSA (1.2.840.113549.1.1.1)

[Certificate Authorities / Root Agency]

Certificate Properties:

Version	V3
Signature Algorithm	MD5 RSA (1.2.840.113549.1.1.4)
Serial Number	F4 35 5C AA D4 B8 CF 11 8A 64 00 AA 00 6C 37 06
Validity	5/28/1996 - 12/31/2039

Issuer Properties:

Common Name	Root Agency

Subject Properties:

Common Name	Root Agency

Public Key Properties:

Public Key Algorithm	RSA (1.2.840.113549.1.1.1)

[Certificate Authorities / UTN-USERFirst-Hardware]

Certificate Properties:

Version	V3
Signature Algorithm	SHA1 RSA (1.2.840.113549.1.1.5)
Serial Number	25 97 49 35 74 A2 D1 43 13 D7 C7 AA F1 AC 4B 48
Validity	6/7/2005 - 5/30/2020

Issuer Properties:

Common Name	AddTrust External CA Root
Organization	AddTrust AB
Organizational Unit	AddTrust External TTP Network
Country	Sweden

Subject Properties:

Common Name	UTN-USERFirst-Hardware
Organization	The USERTRUST Network
Organizational Unit	http://www.usertrust.com
Country	United States
Locality Name	Salt Lake City
State/Province	UT

Public Key Properties:

Public Key Algorithm	RSA (1.2.840.113549.1.1.1)

[Certificate Authorities / VeriSign Class 3 International Server CA - G3]

Certificate Properties:

Version	V3
Signature Algorithm	SHA1 RSA (1.2.840.113549.1.1.5)
Serial Number	67 7E D6 95 2D 4D 2D F3 13 08 02 CE 20 E8 1B 64
Validity	2/7/2010 - 2/7/2020

Issuer Properties:

Common Name	VeriSign Class 3 Public Primary Certification Authority - G5
Organization	VeriSign, Inc.
Organizational Unit	VeriSign Trust Network
Organizational Unit	(c) 2006 VeriSign, Inc. - For authorized use only

Country	United States

Subject Properties:

Common Name	VeriSign Class 3 International Server CA - G3
Organization	VeriSign, Inc.
Organizational Unit	VeriSign Trust Network
Organizational Unit	Terms of use at https://www.verisign.com/rpa (c)10
Country	United States

Public Key Properties:

Public Key Algorithm	RSA (1.2.840.113549.1.1.1)

[Certificate Authorities / VeriSign Class 3 Secure Server CA - G3]

Certificate Properties:

Version	V3
Signature Algorithm	SHA1 RSA (1.2.840.113549.1.1.5)
Serial Number	91 D4 52 E9 F4 BC CE B8 09 20 03 A7 A5 7A CC 6E
Validity	2/7/2010 - 2/7/2020

Issuer Properties:

Common Name	VeriSign Class 3 Public Primary Certification Authority - G5
Organization	VeriSign, Inc.
Organizational Unit	VeriSign Trust Network
Organizational Unit	(c) 2006 VeriSign, Inc. - For authorized use only
Country	United States

Subject Properties:

Common Name	VeriSign Class 3 Secure Server CA - G3
Organization	VeriSign, Inc.
Organizational Unit	VeriSign Trust Network
Organizational Unit	Terms of use at https://www.verisign.com/rpa (c)10
Country	United States

Public Key Properties:

Public Key Algorithm	RSA (1.2.840.113549.1.1.1)

[Certificate Authorities / www.verisign.com/CPS Incorp.by Ref. LIABILITY LTD.(c)97 VeriSign]

Certificate Properties:

Version	V3
Signature Algorithm	SHA1 RSA (1.2.840.113549.1.1.5)
Serial Number	8F 07 93 3F 23 98 60 92 0F 2F D0 B4 BA EB FC 46
Validity	4/16/1997 - 10/24/2016

Issuer Properties:

Organization	VeriSign, Inc.
Organizational Unit	Class 3 Public Primary Certification Authority
Country	United States

Subject Properties:

Organization	VeriSign Trust Network
Organizational Unit	VeriSign, Inc.

Organizational Unit	VeriSign International Server CA - Class 3

Public Key Properties:

Public Key Algorithm	RSA (1.2.840.113549.1.1.1)

[Root Certificates / Baltimore CyberTrust Root]

Certificate Properties:

Version	V3
Signature Algorithm	SHA1 RSA (1.2.840.113549.1.1.5)
Serial Number	B9 00 00 02
Validity	5/12/2000 - 5/12/2025

Issuer Properties:

Common Name	Baltimore CyberTrust Root
Organization	Baltimore
Organizational Unit	CyberTrust
Country	Ireland

Subject Properties:

Common Name	Baltimore CyberTrust Root
Organization	Baltimore
Organizational Unit	CyberTrust
Country	Ireland

Public Key Properties:

Public Key Algorithm	RSA (1.2.840.113549.1.1.1)

[Root Certificates / DigiCert]

Certificate Properties:

Version	V3
Signature Algorithm	SHA1 RSA (1.2.840.113549.1.1.5)
Serial Number	39 30 F0 1B FC 60 E5 8F FE 46 D8 17 E5 E0 E7 0C
Validity	11/9/2006 - 11/9/2031

Issuer Properties:

Common Name	DigiCert Assured ID Root CA
Organization	DigiCert Inc
Organizational Unit	www.digicert.com
Country	United States

Subject Properties:

Common Name	DigiCert Assured ID Root CA
Organization	DigiCert Inc
Organizational Unit	www.digicert.com
Country	United States

Public Key Properties:

Public Key Algorithm	RSA (1.2.840.113549.1.1.1)

[Root Certificates / DigiCert]

Certificate Properties:

Version	V3
Signature Algorithm	SHA1 RSA (1.2.840.113549.1.1.5)
Serial Number	4A C7 91 59 C9 6A 75 A1 B1 46 42 90 56 E0 3B 08
Validity	11/9/2006 - 11/9/2031

Issuer Properties:

Common Name	DigiCert Global Root CA
Organization	DigiCert Inc
Organizational Unit	www.digicert.com
Country	United States

Subject Properties:

Common Name	DigiCert Global Root CA
Organization	DigiCert Inc
Organizational Unit	www.digicert.com
Country	United States

Public Key Properties:

Public Key Algorithm	RSA (1.2.840.113549.1.1.1)

[Root Certificates / DigiCert]

Certificate Properties:

Version	V3
Signature Algorithm	SHA1 RSA (1.2.840.113549.1.1.5)
Serial Number	77 25 46 AE F2 79 0B 8F 9B 40 0B 6A 26 5C AC 02
Validity	11/9/2006 - 11/9/2031

Issuer Properties:

Common Name	DigiCert High Assurance EV Root CA
Organization	DigiCert Inc
Organizational Unit	www.digicert.com
Country	United States

Subject Properties:

Common Name	DigiCert High Assurance EV Root CA
Organization	DigiCert Inc
Organizational Unit	www.digicert.com
Country	United States

Public Key Properties:

Public Key Algorithm	RSA (1.2.840.113549.1.1.1)

[Root Certificates / Entrust (2048)]

Certificate Properties:

Version	V3
Signature Algorithm	SHA1 RSA (1.2.840.113549.1.1.5)
Serial Number	F8 DE 63 38
Validity	12/24/1999 - 7/24/2029

Issuer Properties:

Common Name	Entrust.net Certification Authority (2048)

Organization	Entrust.net
Organizational Unit	www.entrust.net/CPS_2048 incorp. by ref. (limits liab.)
Organizational Unit	(c) 1999 Entrust.net Limited

Subject Properties:

Common Name	Entrust.net Certification Authority (2048)
Organization	Entrust.net
Organizational Unit	www.entrust.net/CPS_2048 incorp. by ref. (limits liab.)
Organizational Unit	(c) 1999 Entrust.net Limited

Public Key Properties:

Public Key Algorithm	RSA (1.2.840.113549.1.1.1)

[Root Certificates / Entrust]

Certificate Properties:

Version	V3
Signature Algorithm	SHA1 RSA (1.2.840.113549.1.1.5)
Serial Number	54 50 6B 45
Validity	11/27/2006 - 11/27/2026

Issuer Properties:

Common Name	Entrust Root Certification Authority
Organization	Entrust, Inc.
Organizational Unit	www.entrust.net/CPS is incorporated by reference
Organizational Unit	(c) 2006 Entrust, Inc.
Country	United States

Subject Properties:

Common Name	Entrust Root Certification Authority
Organization	Entrust, Inc.
Organizational Unit	www.entrust.net/CPS is incorporated by reference
Organizational Unit	(c) 2006 Entrust, Inc.
Country	United States

Public Key Properties:

Public Key Algorithm	RSA (1.2.840.113549.1.1.1)

[Root Certificates / GeoTrust Global CA]

Certificate Properties:

Version	V3
Signature Algorithm	SHA1 RSA (1.2.840.113549.1.1.5)
Serial Number	56 34 02
Validity	5/20/2002 - 5/20/2022

Issuer Properties:

Common Name	GeoTrust Global CA
Organization	GeoTrust Inc.
Country	United States

Subject Properties:

Common Name	GeoTrust Global CA

Organization	GeoTrust Inc.
Country	United States

Public Key Properties:

Public Key Algorithm	RSA (1.2.840.113549.1.1.1)

[Root Certificates / GeoTrust]

Certificate Properties:

Version	V3
Signature Algorithm	SHA1 RSA (1.2.840.113549.1.1.5)
Serial Number	CF F4 DE 35
Validity	8/22/1998 - 8/22/2018

Issuer Properties:

Organization	Equifax
Organizational Unit	Equifax Secure Certificate Authority
Country	United States

Subject Properties:

Organization	Equifax
Organizational Unit	Equifax Secure Certificate Authority
Country	United States

Public Key Properties:

Public Key Algorithm	RSA (1.2.840.113549.1.1.1)

[Root Certificates / GlobalSign]

Certificate Properties:

Version	V3
Signature Algorithm	SHA1 RSA (1.2.840.113549.1.1.5)
Serial Number	94 C3 5A 4B 15 01 00 00 00 00 04
Validity	9/1/1998 - 1/28/2028

Issuer Properties:

Common Name	GlobalSign Root CA
Organization	GlobalSign nv-sa
Organizational Unit	Root CA
Country	Belgium

Subject Properties:

Common Name	GlobalSign Root CA
Organization	GlobalSign nv-sa
Organizational Unit	Root CA
Country	Belgium

Public Key Properties:

Public Key Algorithm	RSA (1.2.840.113549.1.1.1)

[Root Certificates / GlobalSign]

Certificate Properties:

Version	V3
Signature Algorithm	SHA256 RSA (1.2.840.113549.1.1.11)
Serial Number	A2 08 53 58 21 01 00 00 00 00 04
Validity	3/18/2009 - 3/18/2029

Issuer Properties:

Common Name	GlobalSign
Organization	GlobalSign
Organizational Unit	GlobalSign Root CA - R3

Subject Properties:

Common Name	GlobalSign
Organization	GlobalSign
Organizational Unit	GlobalSign Root CA - R3

Public Key Properties:

Public Key Algorithm	RSA (1.2.840.113549.1.1.1)

[Root Certificates / Go Daddy Class 2 Certification Authority]

Certificate Properties:

Version	V3
Signature Algorithm	SHA1 RSA (1.2.840.113549.1.1.5)
Serial Number	00
Validity	6/29/2004 - 6/29/2034

Issuer Properties:

Organization	The Go Daddy Group, Inc.
Organizational Unit	Go Daddy Class 2 Certification Authority
Country	United States

Subject Properties:

Organization	The Go Daddy Group, Inc.
Organizational Unit	Go Daddy Class 2 Certification Authority
Country	United States

Public Key Properties:

Public Key Algorithm	RSA (1.2.840.113549.1.1.1)

[Root Certificates / Go Daddy Root Certificate Authority – G2]

Certificate Properties:

Version	V3
Signature Algorithm	SHA256 RSA (1.2.840.113549.1.1.11)
Serial Number	00
Validity	8/31/2009 - 12/31/2037

Issuer Properties:

Common Name	Go Daddy Root Certificate Authority - G2
Organization	GoDaddy.com, Inc.
Country	United States
Locality Name	Scottsdale
State/Province	Arizona

Subject Properties:

Common Name	Go Daddy Root Certificate Authority - G2
Organization	GoDaddy.com, Inc.
Country	United States
Locality Name	Scottsdale
State/Province	Arizona

Public Key Properties:

Public Key Algorithm	RSA (1.2.840.113549.1.1.1)

[Root Certificates / GTE CyberTrust Global Root]

Certificate Properties:

Version	V1
Signature Algorithm	MD5 RSA (1.2.840.113549.1.1.4)
Serial Number	A5 01
Validity	8/12/1998 - 8/13/2018

Issuer Properties:

Common Name	GTE CyberTrust Global Root
Organization	GTE Corporation
Organizational Unit	GTE CyberTrust Solutions, Inc.
Country	United States

Subject Properties:

Common Name	GTE CyberTrust Global Root
Organization	GTE Corporation
Organizational Unit	GTE CyberTrust Solutions, Inc.
Country	United States

Public Key Properties:

Public Key Algorithm	RSA (1.2.840.113549.1.1.1)

[Root Certificates / Microsoft Authenticode(tm) Root]

Certificate Properties:

Version	V3
Signature Algorithm	MD5 RSA (1.2.840.113549.1.1.4)
Serial Number	01
Validity	1/1/1995 - 12/31/1999

Issuer Properties:

Common Name	Microsoft Authenticode(tm) Root Authority
Organization	MSFT
Country	United States

Subject Properties:

Common Name	Microsoft Authenticode(tm) Root Authority
Organization	MSFT
Country	United States

Public Key Properties:

Public Key Algorithm	RSA (1.2.840.113549.1.1.1)

[Root Certificates / Microsoft Root Authority]

Certificate Properties:

Version	V3
Signature Algorithm	MD5 RSA (1.2.840.113549.1.1.4)
Serial Number	40 DF EC 63 F6 3E D1 11 88 3C 3C 8B 00 C1 00
Validity	1/10/1997 - 12/31/2020

Issuer Properties:

Common Name	Microsoft Root Authority
Organizational Unit	Copyright (c) 1997 Microsoft Corp.
Organizational Unit	Microsoft Corporation

Subject Properties:

Common Name	Microsoft Root Authority
Organizational Unit	Copyright (c) 1997 Microsoft Corp.
Organizational Unit	Microsoft Corporation

Public Key Properties:

Public Key Algorithm	RSA (1.2.840.113549.1.1.1)

[Root Certificates / Microsoft Root Certificate Authority 2010]

Certificate Properties:

Version	V3
Signature Algorithm	SHA256 RSA (1.2.840.113549.1.1.11)
Serial Number	AA 39 43 6B 58 9B 9A 44 AC 44 BA BF 25 3A CC 28
Validity	6/23/2010 - 6/23/2035

Issuer Properties:

Common Name	Microsoft Root Certificate Authority 2010
Organization	Microsoft Corporation
Country	United States
Locality Name	Redmond
State/Province	Washington

Subject Properties:

Common Name	Microsoft Root Certificate Authority 2010
Organization	Microsoft Corporation
Country	United States
Locality Name	Redmond
State/Province	Washington

Public Key Properties:

Public Key Algorithm	RSA (1.2.840.113549.1.1.1)

[Root Certificates / Microsoft Root Certificate Authority 2011]

Certificate Properties:

Version	V3
Signature Algorithm	SHA256 RSA (1.2.840.113549.1.1.11)
Serial Number	44 E1 42 6C D6 69 B5 43 96 B2 9F FC B5 C8 8B 3F

Validity	3/22/2011 - 3/22/2036

Issuer Properties:

Common Name	Microsoft Root Certificate Authority 2011
Organization	Microsoft Corporation
Country	United States
Locality Name	Redmond
State/Province	Washington

Subject Properties:

Common Name	Microsoft Root Certificate Authority 2011
Organization	Microsoft Corporation
Country	United States
Locality Name	Redmond
State/Province	Washington

Public Key Properties:

Public Key Algorithm	RSA (1.2.840.113549.1.1.1)

[Root Certificates / Microsoft Root Certificate Authority]

Certificate Properties:

Version	V3
Signature Algorithm	SHA1 RSA (1.2.840.113549.1.1.5)
Serial Number	65 2E 13 07 F4 58 73 4C AD A5 A0 4A A1 16 AD 79
Validity	5/9/2001 - 5/9/2021

Issuer Properties:

Common Name	Microsoft Root Certificate Authority

Subject Properties:

Common Name	Microsoft Root Certificate Authority

Public Key Properties:

Public Key Algorithm	RSA (1.2.840.113549.1.1.1)

[Root Certificates / Microsoft Timestamp Root]

Certificate Properties:

Version	V1
Signature Algorithm	MD5 RSA (1.2.840.113549.1.1.4)
Serial Number	01
Validity	5/13/1997 - 12/30/1999

Issuer Properties:

Organization	Microsoft Trust Network
Organizational Unit	Microsoft Corporation
Organizational Unit	Microsoft Time Stamping Service Root

Subject Properties:

Organization	Microsoft Trust Network
Organizational Unit	Microsoft Corporation
Organizational Unit	Microsoft Time Stamping Service Root

Public Key Properties:

Public Key Algorithm	RSA (1.2.840.113549.1.1.1)

[Root Certificates / Starfield Class 2 Certification Authority]

Certificate Properties:

Version	V3
Signature Algorithm	SHA1 RSA (1.2.840.113549.1.1.5)
Serial Number	00
Validity	6/29/2004 - 6/29/2034

Issuer Properties:

Organization	Starfield Technologies, Inc.
Organizational Unit	Starfield Class 2 Certification Authority
Country	United States

Subject Properties:

Organization	Starfield Technologies, Inc.
Organizational Unit	Starfield Class 2 Certification Authority
Country	United States

Public Key Properties:

Public Key Algorithm	RSA (1.2.840.113549.1.1.1)

[Root Certificates / Starfield Root Certificate Authority – G2]

Certificate Properties:

Version	V3
Signature Algorithm	SHA256 RSA (1.2.840.113549.1.1.11)
Serial Number	00
Validity	8/31/2009 - 12/31/2037

Issuer Properties:

Common Name	Starfield Root Certificate Authority - G2
Organization	Starfield Technologies, Inc.
Country	United States
Locality Name	Scottsdale
State/Province	Arizona

Subject Properties:

Common Name	Starfield Root Certificate Authority - G2
Organization	Starfield Technologies, Inc.
Country	United States
Locality Name	Scottsdale
State/Province	Arizona

Public Key Properties:

Public Key Algorithm	RSA (1.2.840.113549.1.1.1)

[Root Certificates / Thawte Timestamping CA]

Certificate Properties:

Version	V3

Signature Algorithm	MD5 RSA (1.2.840.113549.1.1.4)
Serial Number	00
Validity	12/31/1996 - 12/31/2020

Issuer Properties:

Common Name	Thawte Timestamping CA
Organization	Thawte
Organizational Unit	Thawte Certification
Country	South Africa
Locality Name	Durbanville
State/Province	Western Cape

Subject Properties:

Common Name	Thawte Timestamping CA
Organization	Thawte
Organizational Unit	Thawte Certification
Country	South Africa
Locality Name	Durbanville
State/Province	Western Cape

Public Key Properties:

Public Key Algorithm	RSA (1.2.840.113549.1.1.1)

[Root Certificates / thawte]

Certificate Properties:

Version	V3
Signature Algorithm	MD5 RSA (1.2.840.113549.1.1.4)
Serial Number	01
Validity	7/31/1996 - 12/31/2020

Issuer Properties:

Common Name	Thawte Premium Server CA
Organization	Thawte Consulting cc
Organizational Unit	Certification Services Division
Country	South Africa
Locality Name	Cape Town
State/Province	Western Cape
E-mail Address	premium-server@thawte.com

Subject Properties:

Common Name	Thawte Premium Server CA
Organization	Thawte Consulting cc
Organizational Unit	Certification Services Division
Country	South Africa
Locality Name	Cape Town
State/Province	Western Cape
E-mail Address	premium-server@thawte.com

Public Key Properties:

Public Key Algorithm	RSA (1.2.840.113549.1.1.1)

[Root Certificates / thawte]

Certificate Properties:

Version	V3
Signature Algorithm	SHA1 RSA (1.2.840.113549.1.1.5)
Serial Number	6D 2B DB 37 CE 2F F4 49 EC ED D5 20 57 D5 4E 34
Validity	11/16/2006 - 7/16/2036

Issuer Properties:

Common Name	thawte Primary Root CA
Organization	thawte, Inc.
Organizational Unit	Certification Services Division
Organizational Unit	(c) 2006 thawte, Inc. - For authorized use only
Country	United States

Subject Properties:

Common Name	thawte Primary Root CA
Organization	thawte, Inc.
Organizational Unit	Certification Services Division
Organizational Unit	(c) 2006 thawte, Inc. - For authorized use only
Country	United States

Public Key Properties:

Public Key Algorithm	RSA (1.2.840.113549.1.1.1)

[Root Certificates / Trustwave]

Certificate Properties:

Version	V3
Signature Algorithm	SHA1 RSA (1.2.840.113549.1.1.5)
Serial Number	D0 59 18 27 EB F0 7F 42 AD A5 16 08 5C 8E F0 0C
Validity	11/7/2006 - 12/31/2029

Issuer Properties:

Common Name	SecureTrust CA
Organization	SecureTrust Corporation
Country	United States

Subject Properties:

Common Name	SecureTrust CA
Organization	SecureTrust Corporation
Country	United States

Public Key Properties:

Public Key Algorithm	RSA (1.2.840.113549.1.1.1)

[Root Certificates / USERTrust]

Certificate Properties:

Version	V3
Signature Algorithm	SHA1 RSA (1.2.840.113549.1.1.5)
Serial Number	1B 5F B3 E0 2D 36 D3 11 B4 24 00 50 8B 0C BE 44
Validity	7/9/1999 - 7/9/2019

Issuer Properties:

Common Name	UTN-USERFirst-Object
Organization	The USERTRUST Network
Organizational Unit	http://www.usertrust.com
Country	United States
Locality Name	Salt Lake City
State/Province	UT

Subject Properties:

Common Name	UTN-USERFirst-Object
Organization	The USERTRUST Network
Organizational Unit	http://www.usertrust.com
Country	United States
Locality Name	Salt Lake City
State/Province	UT

Public Key Properties:

Public Key Algorithm	RSA (1.2.840.113549.1.1.1)

[Root Certificates / USERTrust]

Certificate Properties:

Version	V3
Signature Algorithm	SHA1 RSA (1.2.840.113549.1.1.5)
Serial Number	01
Validity	5/30/2000 - 5/30/2020

Issuer Properties:

Common Name	AddTrust External CA Root
Organization	AddTrust AB
Organizational Unit	AddTrust External TTP Network
Country	Sweden

Subject Properties:

Common Name	AddTrust External CA Root
Organization	AddTrust AB
Organizational Unit	AddTrust External TTP Network
Country	Sweden

Public Key Properties:

Public Key Algorithm	RSA (1.2.840.113549.1.1.1)

[Root Certificates / VeriSign Class 3 Public Primary CA]

Certificate Properties:

Version	V1
Signature Algorithm	MD2 RSA (1.2.840.113549.1.1.2)
Serial Number	BF BA CC 03 7B CA 38 B6 34 29 D9 10 1D E4 BA 70
Validity	1/28/1996 - 8/1/2028

Issuer Properties:

Organization	VeriSign, Inc.
Organizational Unit	Class 3 Public Primary Certification Authority
Country	United States

Subject Properties:

Organization	VeriSign, Inc.
Organizational Unit	Class 3 Public Primary Certification Authority
Country	United States

Public Key Properties:

Public Key Algorithm	RSA (1.2.840.113549.1.1.1)

[Root Certificates / VeriSign Time Stamping CA]

Certificate Properties:

Version	V1
Signature Algorithm	MD5 RSA (1.2.840.113549.1.1.4)
Serial Number	A3 DC 5D 15 5F 73 5D A5 1C 59 82 8C 38 D2 19 4A
Validity	5/11/1997 - 1/7/2004

Issuer Properties:

Organization	VeriSign Trust Network
Organizational Unit	VeriSign, Inc.
Organizational Unit	VeriSign Time Stamping Service Root
Organizational Unit	NO LIABILITY ACCEPTED, (c)97 VeriSign, Inc.

Subject Properties:

Organization	VeriSign Trust Network
Organizational Unit	VeriSign, Inc.
Organizational Unit	VeriSign Time Stamping Service Root
Organizational Unit	NO LIABILITY ACCEPTED, (c)97 VeriSign, Inc.

Public Key Properties:

Public Key Algorithm	RSA (1.2.840.113549.1.1.1)

[Root Certificates / VeriSign]

Certificate Properties:

Version	V1
Signature Algorithm	SHA1 RSA (1.2.840.113549.1.1.5)
Serial Number	C6 34 89 A7 FB 67 79 10 B7 1E A8 CF 07 FE D9 7D
Validity	5/17/1998 - 8/1/2028

Issuer Properties:

Organization	VeriSign, Inc.
Organizational Unit	Class 3 Public Primary Certification Authority - G2
Organizational Unit	(c) 1998 VeriSign, Inc. - For authorized use only
Country	United States

Subject Properties:

Organization	VeriSign, Inc.
Organizational Unit	Class 3 Public Primary Certification Authority - G2
Organizational Unit	(c) 1998 VeriSign, Inc. - For authorized use only
Country	United States

Public Key Properties:

Public Key Algorithm	RSA (1.2.840.113549.1.1.1)

[Root Certificates / VeriSign]

Certificate Properties:

Version	V3
Signature Algorithm	SHA1 RSA (1.2.840.113549.1.1.5)
Serial Number	4A 3B 6B CC CD 58 21 4A BB E8 7D 26 9E D1 DA 18
Validity	11/7/2006 - 7/16/2036

Issuer Properties:

Common Name	VeriSign Class 3 Public Primary Certification Authority - G5
Organization	VeriSign, Inc.
Organizational Unit	VeriSign Trust Network
Organizational Unit	(c) 2006 VeriSign, Inc. - For authorized use only
Country	United States

Subject Properties:

Common Name	VeriSign Class 3 Public Primary Certification Authority - G5
Organization	VeriSign, Inc.
Organizational Unit	VeriSign Trust Network
Organizational Unit	(c) 2006 VeriSign, Inc. - For authorized use only
Country	United States

Public Key Properties:

Public Key Algorithm	RSA (1.2.840.113549.1.1.1)

UpTime

Current Session:

Last Shutdown Time	4/29/2015 11:34:19 AM
Last Boot Time	4/29/2015 11:34:20 AM
Current Time	4/29/2015 11:38:56 AM
UpTime	281 sec (0 days, 0 hours, 4 min, 41 sec)

UpTime Statistics:

First Boot Time	4/11/2015 6:30:49 AM
First Shutdown Time	4/11/2015 6:29:51 AM
Total UpTime	1009812 sec (11 days, 16 hours, 30 min, 12 sec)
Total DownTime	563938 sec (6 days, 12 hours, 38 min, 58 sec)
Longest UpTime	203858 sec (2 days, 8 hours, 37 min, 38 sec)
Longest DownTime	242754 sec (2 days, 19 hours, 25 min, 54 sec)
Total Reboots	95
System Availability	64.17%

Bluescreen Statistics:

Total Bluescreens	0

Information:

Information	The above statistics are based on System Event Log entries

Share

Share Name	Type	Remark	Local Path
ADMIN$	Folder	Remote Admin	C:\Windows
B$	Folder	Default share	B:\
C$	Folder	Default share	C:\
print$	Folder	Printer Drivers	C:\Windows\system32\spool\drivers
IPC$	IPC	Remote IPC	

Account Security

Account Security Properties:

Computer Role	Primary
Domain Name	LTRANPHD
Primary Domain Controller	Not Specified
Forced Logoff Time	Disabled
Min / Max Password Age	0 / 42 days
Minimum Password Length	0 chars
Password History Length	Disabled
Lockout Threshold	Disabled
Lockout Duration	30 min
Lockout Observation Window	30 min

Logon

User	Full Name	Logon Server	Logon Domain
Liem		LTRANPHD	LTRANPHD
Liem		LTRANPHD	LTRANPHD

Users

[Administrator]

User Properties:

User Name	Administrator
Full Name	Administrator
Comment	Built-in account for administering the computer/domain
Member Of Groups	Administrators
Logon Count	3
Disk Quota	-

User Features:

Logon Script Executed	Yes
Account Disabled	Yes
Locked Out User	No

Home Folder Required	No
Password Required	Yes
Read-Only Password	No
Password Never Expires	Yes

[Guest]

User Properties:

User Name	Guest
Full Name	Guest
Comment	Built-in account for guest access to the computer/domain
Member Of Groups	Guests
Logon Count	0
Disk Quota	-

User Features:

Logon Script Executed	Yes
Account Disabled	Yes
Locked Out User	No
Home Folder Required	No
Password Required	No
Read-Only Password	Yes
Password Never Expires	Yes

[Liem]

User Properties:

User Name	Liem
Full Name	Liem
Member Of Groups	Administrators
Logon Count	130
Disk Quota	-

User Features:

Logon Script Executed	Yes
Account Disabled	No
Locked Out User	No
Home Folder Required	No
Password Required	No
Read-Only Password	No
Password Never Expires	Yes

Local Groups

[Access Control Assistance Operators]

Local Group Properties:

Comment	Members of this group can remotely query authorization attributes and permissions for resources on this computer.

[Administrators]

Local Group Properties:
Comment Administrators have complete and unrestricted access to the computer/domain

Group Members:
Administrator
Liem

[Backup Operators]

Local Group Properties:
Comment Backup Operators can override security restrictions for the sole purpose of backing up or restoring files

[Cryptographic Operators]

Local Group Properties:
Comment Members are authorized to perform cryptographic operations.

[Distributed COM Users]

Local Group Properties:
Comment Members are allowed to launch, activate and use Distributed COM objects on this machine.

[Event Log Readers]

Local Group Properties:
Comment Members of this group can read event logs from local machine

[Guests]

Local Group Properties:
Comment Guests have the same access as members of the Users group by default, except for the Guest account which is further restricted

Group Members:
Guest

[Hyper-V Administrators]

Local Group Properties:
Comment Members of this group have complete and unrestricted access to all features of Hyper-V.

[IIS_IUSRS]

Local Group Properties:
Comment Built-in group used by Internet Information Services.

Group Members:
IUSR

[Network Configuration Operators]

Local Group Properties:

Comment	Members in this group can have some administrative privileges to manage configuration of networking features

[Performance Log Users]

Local Group Properties:

Comment	Members of this group may schedule logging of performance counters, enable trace providers, and collect event traces both locally and via remote access to this computer

[Performance Monitor Users]

Local Group Properties:

Comment	Members of this group can access performance counter data locally and remotely

[Power Users]

Local Group Properties:

Comment	Power Users are included for backwards compatibility and possess limited administrative powers

[Remote Desktop Users]

Local Group Properties:

Comment	Members in this group are granted the right to logon remotely

[Remote Management Users]

Local Group Properties:

Comment	Members of this group can access WMI resources over management protocols (such as WS-Management via the Windows Remote Management service). This applies only to WMI namespaces that grant access to the user.

[Replicator]

Local Group Properties:

Comment	Supports file replication in a domain

[Users]

Local Group Properties:

Comment	Users are prevented from making accidental or intentional system-wide changes and can run most applications

Group Members:

Authenticated Users
INTERACTIVE

[WinRMRemoteWMIUsers__]

Local Group Properties:

Comment	Members of this group can access WMI resources over management protocols (such as WS-Management via the Windows Remote Management service). This applies only to WMI namespaces that grant access to the user.

Global Groups

[None]

Global Group Properties:

Comment	Ordinary users

Group Members:

Administrator
Guest
Liem

Windows Video

[Intel(R) HD Graphics 4000]

Video Adapter Properties:

Device Description	Intel(R) HD Graphics 4000
Adapter String	Intel(R) HD Graphics 4000
BIOS String	Intel Video BIOS
Chip Type	Intel(R) HD Graphics Family
DAC Type	Internal
Driver Date	9/29/2014
Driver Version	10.18.10.3958
Driver Provider	Intel Corporation
Memory Size	2112 MB

Installed Drivers:

igdumdim64	10.18.10.3958
igd10iumd64	10.18.10.3958
igd10iumd64	10.18.10.3958
igdumdim32	10.18.10.3958
igd10iumd32	10.18.10.3958
igd10iumd32	10.18.10.3958

Video Adapter Manufacturer:

Company Name	Intel Corporation
Product Information	http://www.intel.com/products/chipsets
Driver Download	http://support.intel.com/support/graphics
Driver Update	http://www.aida64.com/driver-updates

[Intel(R) HD Graphics 4000]

Video Adapter Properties:

Device Description	Intel(R) HD Graphics 4000
Adapter String	Intel(R) HD Graphics 4000
BIOS String	Intel Video BIOS
Chip Type	Intel(R) HD Graphics Family
DAC Type	Internal
Driver Date	9/29/2014
Driver Version	10.18.10.3958

Driver Provider	Intel Corporation
Memory Size	2112 MB

Installed Drivers:

igdumdim64	10.18.10.3958
igd10iumd64	10.18.10.3958
igd10iumd64	10.18.10.3958
igdumdim32	10.18.10.3958
igd10iumd32	10.18.10.3958
igd10iumd32	10.18.10.3958

Video Adapter Manufacturer:

Company Name	Intel Corporation
Product Information	http://www.intel.com/products/chipsets
Driver Download	http://support.intel.com/support/graphics
Driver Update	http://www.aida64.com/driver-updates

[Intel(R) HD Graphics 4000]

Video Adapter Properties:

Device Description	Intel(R) HD Graphics 4000
Adapter String	Intel(R) HD Graphics 4000
BIOS String	Intel Video BIOS
Chip Type	Intel(R) HD Graphics Family
DAC Type	Internal
Driver Date	9/29/2014
Driver Version	10.18.10.3958
Driver Provider	Intel Corporation
Memory Size	2112 MB

Installed Drivers:

igdumdim64	10.18.10.3958
igd10iumd64	10.18.10.3958
igd10iumd64	10.18.10.3958
igdumdim32	10.18.10.3958
igd10iumd32	10.18.10.3958
igd10iumd32	10.18.10.3958

Video Adapter Manufacturer:

Company Name	Intel Corporation
Product Information	http://www.intel.com/products/chipsets
Driver Download	http://support.intel.com/support/graphics
Driver Update	http://www.aida64.com/driver-updates

PCI / AGP Video

Device Description	Device Type
Intel HD Graphics 4000	Video Adapter
Intel HD Graphics 4000	3D Accelerator

GPU

[Integrated: Intel Ivy Bridge-MB - Integrated Graphics Controller (MB GT2)]

Graphics Processor Properties:

Video Adapter	Intel Ivy Bridge-MB - Integrated Graphics Controller (MB GT2)
BIOS Version	Build Number: 2137 PC 14.34 03/14/2012 20:10:50
BIOS Date	3/14/2012
GPU Code Name	Ivy Bridge-MB GT2
PCI Device	8086-0166 / 1025-0649 (Rev 09)
Process Technology	22 nm
Bus Type	Integrated
GPU Clock	349 MHz (original: 649 MHz)
GPU Clock (Turbo)	349 - 1247 MHz
RAMDAC Clock	350 MHz
Pixel Pipelines	4
TMU Per Pipeline	1
Unified Shaders	64 (v5.0)
DirectX Hardware Support	DirectX v11.1
WDDM Version	WDDM 1.3

Architecture:

Architecture	Intel Gen7
Execution Units (EU)	16
L1 Instruction Cache	32 KB
L1 Texture Cache	4 KB
L2 Texture Cache	24 KB
L3 Cache	256 KB
Unified Return Buffer	256 KB

Theoretical Peak Performance:

Pixel Fillrate	1396 MPixel/s @ 349 MHz
Texel Fillrate	1396 MTexel/s @ 349 MHz
Single-Precision FLOPS	89.3 GFLOPS @ 349 MHz

Utilization:

Dedicated Memory	13 MB
Dynamic Memory	51 MB

Graphics Processor Manufacturer:

Company Name	Intel Corporation
Product Information	http://www.intel.com/products/chipsets
Driver Download	http://support.intel.com/support/graphics
Driver Update	http://www.aida64.com/driver-updates

Monitor

[AU Optronics B156XW02 V6]

Monitor Properties:

Monitor Name	AU Optronics B156XW02 V6
Monitor ID	AUO26EC
Manufacturer	AUO
Model	B156XW02 V6
Monitor Type	15.6" LCD (WXGA)
Manufacture Date	Week 1 / 2009
Serial Number	None
Max. Visible Display Size	344 mm x 193 mm (15.5")
Picture Aspect Ratio	16:9
Horizontal Frequency	30 - 83 kHz
Vertical Frequency	56 - 75 Hz
Maximum Resolution	1366 x 768
Gamma	2.20
DPMS Mode Support	None

Supported Video Modes:

1366 x 768	Pixel Clock: 71.80 MHz

Monitor Manufacturer:

Company Name	AU Optronics Corp.
Product Information	http://www.auo.com/?sn=149&lang=en-US&c=33
Driver Download	http://www.auo.com/?sn=171&lang=en-US
Driver Update	http://www.aida64.com/driver-updates

Desktop

Desktop Properties:

Device Technology	Raster Display
Resolution	1366 x 768
Color Depth	32-bit
Color Planes	1
Font Resolution	96 dpi
Pixel Width / Height	36 / 36
Pixel Diagonal	51
Vertical Refresh Rate	60 Hz

Desktop Effects:

Combo-Box Animation	Disabled
Drop Shadow Effect	Disabled
Flat Menu Effect	Enabled
Font Smoothing	Enabled
ClearType	Enabled
Full Window Dragging	Disabled
Gradient Window Title Bars	Enabled
Hide Menu Access Keys	Enabled
Hot Tracking Effect	Enabled
Icon Title Wrapping	Enabled
List-Box Smooth Scrolling	Disabled
Menu Animation	Disabled
Menu Fade Effect	Enabled
Minimize/Restore Animation	Disabled
Mouse Cursor Shadow	Disabled

Selection Fade Effect	Disabled
ShowSounds Accessibility Feature	Disabled
ToolTip Animation	Disabled
ToolTip Fade Effect	Enabled
Windows Aero	Enabled
Windows Plus! Extension	Disabled

Multi-Monitor

Device ID	Primary	Upper Left Corner	Bottom Right Corner
\\.\DISPLAY1	Yes	(0,0)	(1366,768)

Video Modes

Resolution	Color Depth	Refresh Rate
320 x 200	32-bit	60 Hz
320 x 200	32-bit	60 Hz
320 x 200	32-bit	60 Hz
320 x 240	32-bit	60 Hz
320 x 240	32-bit	60 Hz
320 x 240	32-bit	60 Hz
400 x 300	32-bit	60 Hz
400 x 300	32-bit	60 Hz
400 x 300	32-bit	60 Hz
512 x 384	32-bit	60 Hz
512 x 384	32-bit	60 Hz
512 x 384	32-bit	60 Hz
640 x 400	32-bit	60 Hz
640 x 400	32-bit	60 Hz
640 x 400	32-bit	60 Hz
640 x 480	32-bit	60 Hz
640 x 480	32-bit	60 Hz
640 x 480	32-bit	60 Hz
800 x 600	32-bit	60 Hz
800 x 600	32-bit	60 Hz
800 x 600	32-bit	60 Hz
1024 x 768	32-bit	60 Hz
1024 x 768	32-bit	60 Hz
1024 x 768	32-bit	60 Hz
1280 x 600	32-bit	60 Hz
1280 x 600	32-bit	60 Hz
1280 x 600	32-bit	60 Hz
1280 x 720	32-bit	60 Hz
1280 x 720	32-bit	60 Hz
1280 x 720	32-bit	60 Hz
1280 x 768	32-bit	60 Hz
1280 x 768	32-bit	60 Hz
1280 x 768	32-bit	60 Hz
1360 x 768	32-bit	60 Hz

1360 x 768	32-bit	60 Hz
1360 x 768	32-bit	60 Hz
1366 x 768	32-bit	60 Hz

OpenGL

OpenGL Properties:

Vendor	Intel
Renderer	Intel(R) HD Graphics 4000
Version	4.0.0 - Build 10.18.10.3958
Shading Language Version	4.00 - Build 10.18.10.3958
OpenGL DLL	6.3.9600.17415(winblue_r4.141028-1500)
Multitexture Texture Units	8
Occlusion Query Counter Bits	64
Sub-Pixel Precision	4-bit
Max Viewport Size	16384 x 16384
Max Cube Map Texture Size	16384 x 16384
Max Rectangle Texture Size	16384 x 16384
Max 3D Texture Size	2048 x 2048 x 2048
Max Anisotropy	16
Max Clipping Planes	8
Max Display-List Nesting Level	64
Max Draw Buffers	8
Max Evaluator Order	32
Max Light Sources	8
Max Pixel Map Table Size	65536
Min / Max Program Texel Offset	-8 / 7
Max Texture Array Layers	2048
Max Texture LOD Bias	15

OpenGL Compliancy:

OpenGL 1.1	Yes (100%)
OpenGL 1.2	Yes (100%)
OpenGL 1.3	Yes (100%)
OpenGL 1.4	Yes (100%)
OpenGL 1.5	Yes (100%)
OpenGL 2.0	Yes (100%)
OpenGL 2.1	Yes (100%)
OpenGL 3.0	Yes (100%)
OpenGL 3.1	Yes (100%)
OpenGL 3.2	Yes (100%)
OpenGL 3.3	Yes (100%)
OpenGL 4.0	Yes (100%)
OpenGL 4.1	No (85%)
OpenGL 4.2	No (83%)
OpenGL 4.3	No (42%)
OpenGL 4.4	No (11%)
OpenGL 4.5	No (0%)

Max Stack Depth:

Attribute Stack	16
Client Attribute Stack	16

Modelview Matrix Stack	32
Name Stack	128
Projection Matrix Stack	4
Texture Matrix Stack	10

Draw Range Elements:

Max Index Count	1048576
Max Vertex Count	1048576

Transform Feedback:

Max Interleaved Components	128
Max Separate Attributes	4
Max Separate Components	4

Framebuffer Object:

Max Color Attachments	8
Max Render Buffer Size	16384 x 16384

Vertex Shader:

Max Uniform Vertex Components	4096
Max Varying Floats	64
Max Vertex Texture Image Units	16
Max Combined Texture Image Units	96

Geometry Shader:

Max Geometry Texture Units	16
Max Varying Components	64
Max Geometry Varying Components	64
Max Vertex Varying Components	32
Max Geometry Uniform Components	4096
Max Geometry Output Vertices	256
Max Geometry Total Output Components	1024

Fragment Shader:

Max Uniform Fragment Components	4096

Vertex Program:

Max Local Parameters	256
Max Environment Parameters	300
Max Program Matrices	8
Max Program Matrix Stack Depth	2
Max Vertex Attributes	16
Max Instructions	1024
Max Native Instructions	1024
Max Temporaries	31
Max Native Temporaries	31
Max Parameters	512
Max Native Parameters	400
Max Attributes	16
Max Native Attributes	16
Max Address Registers	1
Max Native Address Registers	1

Fragment Program:

Max Local Parameters	256
Max Environment Parameters	256
Max Texture Coordinates	8
Max Texture Image Units	16
Max Instructions	1447
Max Native Instructions	1447
Max Temporaries	256
Max Native Temporaries	256
Max Parameters	512
Max Native Parameters	32
Max Attributes	13
Max Native Attributes	13
Max Address Registers	0
Max Native Address Registers	0
Max ALU Instructions	1447
Max Native ALU Instructions	1447
Max Texture Instructions	1447
Max Native Texture Instructions	1447
Max Texture Indirections	128
Max Native Texture Indirections	128

OpenGL Extensions:

Total / Supported Extensions	1007 / 188
GL_3DFX_multisample	Not Supported
GL_3DFX_tbuffer	Not Supported
GL_3DFX_texture_compression_FXT1	Supported
GL_3DL_direct_texture_access2	Not Supported
GL_3Dlabs_multisample_transparency_id	Not Supported
GL_3Dlabs_multisample_transparency_range	Not Supported
GL_AMD_blend_minmax_factor	Not Supported
GL_AMD_compressed_3DC_texture	Not Supported
GL_AMD_compressed_ATC_texture	Not Supported
GL_AMD_conservative_depth	Not Supported
GL_AMD_debug_output	Not Supported
GL_AMD_depth_clamp_separate	Not Supported
GL_AMD_draw_buffers_blend	Not Supported
GL_AMD_framebuffer_sample_positions	Not Supported
GL_AMD_gcn_shader	Not Supported
GL_AMD_gpu_shader_half_float	Not Supported
GL_AMD_gpu_shader_half_float2	Not Supported
GL_AMD_gpu_shader_int64	Not Supported
GL_AMD_interleaved_elements	Not Supported
GL_AMD_multi_draw_indirect	Not Supported
GL_AMD_name_gen_delete	Not Supported
GL_AMD_occlusion_query_event	Not Supported
GL_AMD_performance_monitor	Not Supported
GL_AMD_pinned_memory	Not Supported
GL_AMD_program_binary_Z400	Not Supported
GL_AMD_query_buffer_object	Not Supported
GL_AMD_sample_positions	Not Supported
GL_AMD_seamless_cubemap_per_texture	Not Supported
GL_AMD_shader_atomic_counter_ops	Not Supported
GL_AMD_shader_stencil_export	Not Supported
GL_AMD_shader_stencil_value_export	Not Supported

GL_AMD_shader_trace	Not Supported
GL_AMD_shader_trinary_minmax	Not Supported
GL_AMD_sparse_texture	Not Supported
GL_AMD_sparse_texture_pool	Not Supported
GL_AMD_stencil_operation_extended	Not Supported
GL_AMD_texture_compression_dxt6	Not Supported
GL_AMD_texture_compression_dxt7	Not Supported
GL_AMD_texture_cube_map_array	Not Supported
GL_AMD_texture_texture4	Not Supported
GL_AMD_texture_tile_pool	Not Supported
GL_AMD_transform_feedback3_lines_triangles	Not Supported
GL_AMD_transform_feedback4	Not Supported
GL_AMD_vertex_shader_layer	Not Supported
GL_AMD_vertex_shader_tessellator	Not Supported
GL_AMD_vertex_shader_viewport_index	Not Supported
GL_AMDX_debug_output	Not Supported
GL_AMDX_name_gen_delete	Not Supported
GL_AMDX_random_access_target	Not Supported
GL_AMDX_vertex_shader_tessellator	Not Supported
GL_ANDROID_extension_pack_es31a	Not Supported
GL_ANGLE_depth_texture	Not Supported
GL_ANGLE_framebuffer_blit	Not Supported
GL_ANGLE_framebuffer_multisample	Not Supported
GL_ANGLE_instanced_arrays	Not Supported
GL_ANGLE_pack_reverse_row_order	Not Supported
GL_ANGLE_program_binary	Not Supported
GL_ANGLE_texture_compression_dxt1	Not Supported
GL_ANGLE_texture_compression_dxt3	Not Supported
GL_ANGLE_texture_compression_dxt5	Not Supported
GL_ANGLE_texture_usage	Not Supported
GL_ANGLE_translated_shader_source	Not Supported
GL_APPLE_aux_depth_stencil	Not Supported
GL_APPLE_client_storage	Not Supported
GL_APPLE_copy_texture_levels	Not Supported
GL_APPLE_element_array	Not Supported
GL_APPLE_fence	Not Supported
GL_APPLE_float_pixels	Not Supported
GL_APPLE_flush_buffer_range	Not Supported
GL_APPLE_flush_render	Not Supported
GL_APPLE_framebuffer_multisample	Not Supported
GL_APPLE_object_purgeable	Not Supported
GL_APPLE_packed_pixel	Not Supported
GL_APPLE_packed_pixels	Not Supported
GL_APPLE_pixel_buffer	Not Supported
GL_APPLE_rgb_422	Not Supported
GL_APPLE_row_bytes	Not Supported
GL_APPLE_specular_vector	Not Supported
GL_APPLE_sync	Not Supported
GL_APPLE_texture_2D_limited_npot	Not Supported
GL_APPLE_texture_format_BGRA8888	Not Supported
GL_APPLE_texture_max_level	Not Supported
GL_APPLE_texture_range	Not Supported
GL_APPLE_transform_hint	Not Supported
GL_APPLE_vertex_array_object	Not Supported

GL_APPLE_vertex_array_range	Not Supported
GL_APPLE_vertex_point_size	Not Supported
GL_APPLE_vertex_program_evaluators	Not Supported
GL_APPLE_ycbcr_422	Not Supported
GL_ARB_arrays_of_arrays	Supported
GL_ARB_base_instance	Supported
GL_ARB_bindless_texture	Not Supported
GL_ARB_blend_func_extended	Supported
GL_ARB_buffer_storage	Supported
GL_ARB_cl_event	Not Supported
GL_ARB_clear_buffer_object	Not Supported
GL_ARB_clear_texture	Not Supported
GL_ARB_clip_control	Not Supported
GL_ARB_color_buffer_float	Supported
GL_ARB_compatibility	Supported
GL_ARB_compressed_texture_pixel_storage	Supported
GL_ARB_compute_shader	Not Supported
GL_ARB_compute_variable_group_size	Not Supported
GL_ARB_conditional_render_inverted	Not Supported
GL_ARB_conservative_depth	Supported
GL_ARB_context_flush_control	Not Supported
GL_ARB_copy_buffer	Supported
GL_ARB_copy_image	Not Supported
GL_ARB_cull_distance	Not Supported
GL_ARB_debug_group	Not Supported
GL_ARB_debug_label	Not Supported
GL_ARB_debug_output	Supported
GL_ARB_debug_output2	Not Supported
GL_ARB_depth_buffer_float	Supported
GL_ARB_depth_clamp	Supported
GL_ARB_depth_texture	Supported
GL_ARB_derivative_control	Not Supported
GL_ARB_direct_state_access	Not Supported
GL_ARB_draw_buffers	Supported
GL_ARB_draw_buffers_blend	Supported
GL_ARB_draw_elements_base_vertex	Supported
GL_ARB_draw_indirect	Supported
GL_ARB_draw_instanced	Supported
GL_ARB_enhanced_layouts	Not Supported
GL_ARB_ES2_compatibility	Supported
GL_ARB_ES3_1_compatibility	Not Supported
GL_ARB_ES3_compatibility	Supported
GL_ARB_explicit_attrib_location	Supported
GL_ARB_explicit_uniform_location	Not Supported
GL_ARB_fragment_coord_conventions	Supported
GL_ARB_fragment_layer_viewport	Not Supported
GL_ARB_fragment_program	Supported
GL_ARB_fragment_program_shadow	Supported
GL_ARB_fragment_shader	Supported
GL_ARB_framebuffer_no_attachments	Supported
GL_ARB_framebuffer_object	Supported
GL_ARB_framebuffer_sRGB	Supported
GL_ARB_geometry_shader4	Supported
GL_ARB_get_program_binary	Supported

GL_ARB_get_texture_sub_image	Not Supported
GL_ARB_gpu_shader_fp64	Supported
GL_ARB_gpu_shader5	Supported
GL_ARB_half_float_pixel	Supported
GL_ARB_half_float_vertex	Supported
GL_ARB_imaging	Not Supported
GL_ARB_indirect_parameters	Not Supported
GL_ARB_instanced_arrays	Supported
GL_ARB_internalformat_query	Supported
GL_ARB_internalformat_query2	Supported
GL_ARB_invalidate_subdata	Not Supported
GL_ARB_make_current_read	Not Supported
GL_ARB_map_buffer_alignment	Supported
GL_ARB_map_buffer_range	Supported
GL_ARB_matrix_palette	Not Supported
GL_ARB_multi_bind	Not Supported
GL_ARB_multi_draw_indirect	Supported
GL_ARB_multisample	Supported
GL_ARB_multitexture	Supported
GL_ARB_occlusion_query	Supported
GL_ARB_occlusion_query2	Supported
GL_ARB_pipeline_statistics_query	Not Supported
GL_ARB_pixel_buffer_object	Supported
GL_ARB_point_parameters	Supported
GL_ARB_point_sprite	Supported
GL_ARB_program_interface_query	Supported
GL_ARB_provoking_vertex	Supported
GL_ARB_query_buffer_object	Not Supported
GL_ARB_robust_buffer_access_behavior	Not Supported
GL_ARB_robustness	Supported
GL_ARB_robustness_isolation	Not Supported
GL_ARB_sample_shading	Supported
GL_ARB_sampler_objects	Supported
GL_ARB_seamless_cube_map	Supported
GL_ARB_seamless_cubemap_per_texture	Not Supported
GL_ARB_separate_shader_objects	Supported
GL_ARB_shader_atomic_counters	Supported
GL_ARB_shader_bit_encoding	Supported
GL_ARB_shader_draw_parameters	Not Supported
GL_ARB_shader_group_vote	Not Supported
GL_ARB_shader_image_load_store	Not Supported
GL_ARB_shader_image_size	Not Supported
GL_ARB_shader_objects	Supported
GL_ARB_shader_precision	Supported
GL_ARB_shader_stencil_export	Not Supported
GL_ARB_shader_storage_buffer_object	Not Supported
GL_ARB_shader_subroutine	Supported
GL_ARB_shader_texture_image_samples	Not Supported
GL_ARB_shader_texture_lod	Not Supported
GL_ARB_shading_language_100	Supported
GL_ARB_shading_language_120	Not Supported
GL_ARB_shading_language_420pack	Supported
GL_ARB_shading_language_include	Not Supported
GL_ARB_shading_language_packing	Supported

GL_ARB_shadow	Supported
GL_ARB_shadow_ambient	Not Supported
GL_ARB_sparse_buffer	Not Supported
GL_ARB_sparse_texture	Not Supported
GL_ARB_stencil_texturing	Supported
GL_ARB_swap_buffers	Not Supported
GL_ARB_sync	Supported
GL_ARB_tessellation_shader	Supported
GL_ARB_texture_barrier	Not Supported
GL_ARB_texture_border_clamp	Supported
GL_ARB_texture_buffer_object	Not Supported
GL_ARB_texture_buffer_object_rgb32	Supported
GL_ARB_texture_buffer_range	Supported
GL_ARB_texture_compression	Supported
GL_ARB_texture_compression_bptc	Supported
GL_ARB_texture_compression_rgtc	Supported
GL_ARB_texture_compression_rtgc	Not Supported
GL_ARB_texture_cube_map	Supported
GL_ARB_texture_cube_map_array	Supported
GL_ARB_texture_env_add	Supported
GL_ARB_texture_env_combine	Supported
GL_ARB_texture_env_crossbar	Supported
GL_ARB_texture_env_dot3	Supported
GL_ARB_texture_float	Supported
GL_ARB_texture_gather	Supported
GL_ARB_texture_mirror_clamp_to_edge	Not Supported
GL_ARB_texture_mirrored_repeat	Not Supported
GL_ARB_texture_multisample	Supported
GL_ARB_texture_non_power_of_two	Supported
GL_ARB_texture_query_levels	Not Supported
GL_ARB_texture_query_lod	Supported
GL_ARB_texture_rectangle	Supported
GL_ARB_texture_rg	Supported
GL_ARB_texture_rgb10_a2ui	Supported
GL_ARB_texture_snorm	Not Supported
GL_ARB_texture_stencil8	Not Supported
GL_ARB_texture_storage	Supported
GL_ARB_texture_storage_multisample	Supported
GL_ARB_texture_swizzle	Supported
GL_ARB_texture_view	Not Supported
GL_ARB_timer_query	Supported
GL_ARB_transform_feedback_instanced	Supported
GL_ARB_transform_feedback_overflow_query	Not Supported
GL_ARB_transform_feedback2	Supported
GL_ARB_transform_feedback3	Supported
GL_ARB_transpose_matrix	Supported
GL_ARB_uber_buffers	Not Supported
GL_ARB_uber_mem_image	Not Supported
GL_ARB_uber_vertex_array	Not Supported
GL_ARB_uniform_buffer_object	Supported
GL_ARB_vertex_array_bgra	Supported
GL_ARB_vertex_array_object	Supported
GL_ARB_vertex_attrib_64bit	Supported
GL_ARB_vertex_attrib_binding	Supported

GL_ARB_vertex_blend	Not Supported
GL_ARB_vertex_buffer_object	Supported
GL_ARB_vertex_program	Supported
GL_ARB_vertex_shader	Supported
GL_ARB_vertex_type_10f_11f_11f_rev	Not Supported
GL_ARB_vertex_type_2_10_10_10_rev	Supported
GL_ARB_viewport_array	Supported
GL_ARB_window_pos	Supported
GL_ARM_mali_program_binary	Not Supported
GL_ARM_mali_shader_binary	Not Supported
GL_ARM_rgba8	Not Supported
GL_ARM_shader_framebuffer_fetch	Not Supported
GL_ARM_shader_framebuffer_fetch_depth_stencil	Not Supported
GL_ATI_array_rev_comps_in_4_bytes	Not Supported
GL_ATI_blend_equation_separate	Not Supported
GL_ATI_blend_weighted_minmax	Not Supported
GL_ATI_draw_buffers	Not Supported
GL_ATI_element_array	Not Supported
GL_ATI_envmap_bumpmap	Not Supported
GL_ATI_fragment_shader	Not Supported
GL_ATI_lock_texture	Not Supported
GL_ATI_map_object_buffer	Not Supported
GL_ATI_meminfo	Not Supported
GL_ATI_pixel_format_float	Not Supported
GL_ATI_pn_triangles	Not Supported
GL_ATI_point_cull_mode	Not Supported
GL_ATI_separate_stencil	Supported
GL_ATI_shader_texture_lod	Not Supported
GL_ATI_text_fragment_shader	Not Supported
GL_ATI_texture_compression_3dc	Not Supported
GL_ATI_texture_env_combine3	Not Supported
GL_ATI_texture_float	Not Supported
GL_ATI_texture_mirror_once	Not Supported
GL_ATI_vertex_array_object	Not Supported
GL_ATI_vertex_attrib_array_object	Not Supported
GL_ATI_vertex_blend	Not Supported
GL_ATI_vertex_shader	Not Supported
GL_ATI_vertex_streams	Not Supported
GL_ATIX_pn_triangles	Not Supported
GL_ATIX_texture_env_combine3	Not Supported
GL_ATIX_texture_env_route	Not Supported
GL_ATIX_vertex_shader_output_point_size	Not Supported
GL_Autodesk_facet_normal	Not Supported
GL_Autodesk_valid_back_buffer_hint	Not Supported
GL_CR_bounding_box	Not Supported
GL_CR_cursor_position	Not Supported
GL_CR_head_spu_name	Not Supported
GL_CR_performance_info	Not Supported
GL_CR_print_string	Not Supported
GL_CR_readback_barrier_size	Not Supported
GL_CR_saveframe	Not Supported
GL_CR_server_id_sharing	Not Supported
GL_CR_server_matrix	Not Supported
GL_CR_state_parameter	Not Supported

GL_CR_synchronization	Not Supported
GL_CR_tile_info	Not Supported
GL_CR_tilesort_info	Not Supported
GL_CR_window_size	Not Supported
GL_DIMD_YUV	Not Supported
GL_DMP_shader_binary	Not Supported
GL_EXT_422_pixels	Not Supported
GL_EXT_abgr	Supported
GL_EXT_bgra	Supported
GL_EXT_bindable_uniform	Not Supported
GL_EXT_blend_color	Supported
GL_EXT_blend_equation_separate	Supported
GL_EXT_blend_func_separate	Supported
GL_EXT_blend_logic_op	Not Supported
GL_EXT_blend_minmax	Supported
GL_EXT_blend_subtract	Supported
GL_EXT_Cg_shader	Not Supported
GL_EXT_clip_control	Not Supported
GL_EXT_clip_volume_hint	Supported
GL_EXT_cmyka	Not Supported
GL_EXT_color_buffer_float	Not Supported
GL_EXT_color_buffer_half_float	Not Supported
GL_EXT_color_matrix	Not Supported
GL_EXT_color_subtable	Not Supported
GL_EXT_color_table	Not Supported
GL_EXT_compiled_vertex_array	Supported
GL_EXT_convolution	Not Supported
GL_EXT_convolution_border_modes	Not Supported
GL_EXT_coordinate_frame	Not Supported
GL_EXT_copy_buffer	Not Supported
GL_EXT_copy_image	Not Supported
GL_EXT_copy_texture	Not Supported
GL_EXT_cull_vertex	Not Supported
GL_EXT_debug_label	Not Supported
GL_EXT_debug_marker	Not Supported
GL_EXT_depth_bounds_test	Not Supported
GL_EXT_depth_buffer_float	Not Supported
GL_EXT_direct_state_access	Not Supported
GL_EXT_discard_framebuffer	Not Supported
GL_EXT_disjoint_timer_query	Not Supported
GL_EXT_draw_buffers	Not Supported
GL_EXT_draw_buffers_indexed	Not Supported
GL_EXT_draw_buffers2	Supported
GL_EXT_draw_indirect	Not Supported
GL_EXT_draw_instanced	Not Supported
GL_EXT_draw_range_elements	Supported
GL_EXT_fog_coord	Supported
GL_EXT_fog_function	Not Supported
GL_EXT_fog_offset	Not Supported
GL_EXT_frag_depth	Not Supported
GL_EXT_fragment_lighting	Not Supported
GL_EXT_framebuffer_blit	Supported
GL_EXT_framebuffer_multisample	Supported
GL_EXT_framebuffer_multisample_blit_scaled	Not Supported

GL_EXT_framebuffer_object	Supported
GL_EXT_framebuffer_sRGB	Not Supported
GL_EXT_generate_mipmap	Not Supported
GL_EXT_geometry_point_size	Not Supported
GL_EXT_geometry_shader	Not Supported
GL_EXT_geometry_shader4	Supported
GL_EXT_glx_stereo_tree	Not Supported
GL_EXT_gpu_program_parameters	Supported
GL_EXT_gpu_shader_fp64	Not Supported
GL_EXT_gpu_shader4	Supported
GL_EXT_gpu_shader5	Not Supported
GL_EXT_histogram	Not Supported
GL_EXT_import_sync_object	Not Supported
GL_EXT_index_array_formats	Not Supported
GL_EXT_index_func	Not Supported
GL_EXT_index_material	Not Supported
GL_EXT_index_texture	Not Supported
GL_EXT_instanced_arrays	Not Supported
GL_EXT_interlace	Not Supported
GL_EXT_light_texture	Not Supported
GL_EXT_map_buffer_range	Not Supported
GL_EXT_misc_attribute	Not Supported
GL_EXT_multi_draw_arrays	Supported
GL_EXT_multisample	Not Supported
GL_EXT_multisampled_render_to_texture	Not Supported
GL_EXT_multiview_draw_buffers	Not Supported
GL_EXT_occlusion_query_boolean	Not Supported
GL_EXT_packed_depth_stencil	Supported
GL_EXT_packed_float	Supported
GL_EXT_packed_pixels	Supported
GL_EXT_packed_pixels_12	Not Supported
GL_EXT_paletted_texture	Not Supported
GL_EXT_pixel_buffer_object	Not Supported
GL_EXT_pixel_format	Not Supported
GL_EXT_pixel_texture	Not Supported
GL_EXT_pixel_transform	Not Supported
GL_EXT_pixel_transform_color_table	Not Supported
GL_EXT_point_parameters	Not Supported
GL_EXT_polygon_offset	Not Supported
GL_EXT_polygon_offset_clamp	Not Supported
GL_EXT_post_depth_coverage	Not Supported
GL_EXT_primitive_bounding_box	Not Supported
GL_EXT_provoking_vertex	Not Supported
GL_EXT_pvrtc_sRGB	Not Supported
GL_EXT_raster_multisample	Not Supported
GL_EXT_read_format_bgra	Not Supported
GL_EXT_rescale_normal	Supported
GL_EXT_robustness	Not Supported
GL_EXT_scene_marker	Not Supported
GL_EXT_secondary_color	Supported
GL_EXT_separate_shader_objects	Not Supported
GL_EXT_separate_specular_color	Supported
GL_EXT_shader_atomic_counters	Not Supported
GL_EXT_shader_framebuffer_fetch	Not Supported

GL_EXT_shader_image_load_formatted	Not Supported
GL_EXT_shader_image_load_store	Not Supported
GL_EXT_shader_implicit_conversions	Not Supported
GL_EXT_shader_integer_mix	Supported
GL_EXT_shader_io_blocks	Not Supported
GL_EXT_shader_pixel_local_storage	Not Supported
GL_EXT_shader_subroutine	Not Supported
GL_EXT_shader_texture_lod	Not Supported
GL_EXT_shadow_funcs	Supported
GL_EXT_shadow_samplers	Not Supported
GL_EXT_shared_texture_palette	Not Supported
GL_EXT_sparse_texture2	Not Supported
GL_EXT_sRGB	Not Supported
GL_EXT_sRGB_write_control	Not Supported
GL_EXT_static_vertex_array	Not Supported
GL_EXT_stencil_clear_tag	Not Supported
GL_EXT_stencil_two_side	Supported
GL_EXT_stencil_wrap	Supported
GL_EXT_subtexture	Not Supported
GL_EXT_swap_control	Not Supported
GL_EXT_tessellation_point_size	Not Supported
GL_EXT_tessellation_shader	Not Supported
GL_EXT_texgen_reflection	Not Supported
GL_EXT_texture	Not Supported
GL_EXT_texture_array	Supported
GL_EXT_texture_border_clamp	Not Supported
GL_EXT_texture_buffer	Supported
GL_EXT_texture_buffer_object	Not Supported
GL_EXT_texture_buffer_object_rgb32	Not Supported
GL_EXT_texture_color_table	Not Supported
GL_EXT_texture_compression_bptc	Not Supported
GL_EXT_texture_compression_dxt1	Not Supported
GL_EXT_texture_compression_latc	Not Supported
GL_EXT_texture_compression_rgtc	Not Supported
GL_EXT_texture_compression_s3tc	Supported
GL_EXT_texture_cube_map	Not Supported
GL_EXT_texture_cube_map_array	Not Supported
GL_EXT_texture_edge_clamp	Supported
GL_EXT_texture_env	Not Supported
GL_EXT_texture_env_add	Supported
GL_EXT_texture_env_combine	Supported
GL_EXT_texture_env_dot3	Not Supported
GL_EXT_texture_filter_anisotropic	Supported
GL_EXT_texture_filter_minmax	Not Supported
GL_EXT_texture_format_BGRA8888	Not Supported
GL_EXT_texture_integer	Supported
GL_EXT_texture_lod	Not Supported
GL_EXT_texture_lod_bias	Supported
GL_EXT_texture_mirror_clamp	Not Supported
GL_EXT_texture_object	Not Supported
GL_EXT_texture_perturb_normal	Not Supported
GL_EXT_texture_rectangle	Supported
GL_EXT_texture_rg	Not Supported
GL_EXT_texture_shared_exponent	Supported

GL_EXT_texture_snorm	Supported
GL_EXT_texture_sRGB	Supported
GL_EXT_texture_sRGB_decode	Supported
GL_EXT_texture_storage	Supported
GL_EXT_texture_swizzle	Supported
GL_EXT_texture_type_2_10_10_10_REV	Not Supported
GL_EXT_texture_view	Not Supported
GL_EXT_texture3D	Supported
GL_EXT_texture4D	Not Supported
GL_EXT_timer_query	Not Supported
GL_EXT_transform_feedback	Supported
GL_EXT_transform_feedback2	Not Supported
GL_EXT_transform_feedback3	Not Supported
GL_EXT_unpack_subimage	Not Supported
GL_EXT_vertex_array	Not Supported
GL_EXT_vertex_array_bgra	Not Supported
GL_EXT_vertex_array_set	Not Supported
GL_EXT_vertex_array_setXXX	Not Supported
GL_EXT_vertex_attrib_64bit	Not Supported
GL_EXT_vertex_shader	Not Supported
GL_EXT_vertex_weighting	Not Supported
GL_EXT_x11_sync_object	Not Supported
GL_EXTX_framebuffer_mixed_formats	Not Supported
GL_EXTX_packed_depth_stencil	Not Supported
GL_FGL_lock_texture	Not Supported
GL_FJ_shader_binary_GCCSO	Not Supported
GL_GL2_geometry_shader	Not Supported
GL_GREMEDY_frame_terminator	Not Supported
GL_GREMEDY_string_marker	Not Supported
GL_HP_convolution_border_modes	Not Supported
GL_HP_image_transform	Not Supported
GL_HP_occlusion_test	Not Supported
GL_HP_texture_lighting	Not Supported
GL_I3D_argb	Not Supported
GL_I3D_color_clamp	Not Supported
GL_I3D_interlace_read	Not Supported
GL_IBM_clip_check	Not Supported
GL_IBM_cull_vertex	Not Supported
GL_IBM_load_named_matrix	Not Supported
GL_IBM_multi_draw_arrays	Not Supported
GL_IBM_multimode_draw_arrays	Not Supported
GL_IBM_occlusion_cull	Not Supported
GL_IBM_pixel_filter_hint	Not Supported
GL_IBM_rasterpos_clip	Not Supported
GL_IBM_rescale_normal	Not Supported
GL_IBM_static_data	Not Supported
GL_IBM_texture_clamp_nodraw	Not Supported
GL_IBM_texture_mirrored_repeat	Supported
GL_IBM_vertex_array_lists	Not Supported
GL_IBM_YCbCr	Not Supported
GL_IMG_multisampled_render_to_texture	Not Supported
GL_IMG_program_binary	Not Supported
GL_IMG_read_format	Not Supported
GL_IMG_sgx_binary	Not Supported

GL_IMG_shader_binary	Not Supported
GL_IMG_texture_compression_pvrtc	Not Supported
GL_IMG_texture_compression_pvrtc2	Not Supported
GL_IMG_texture_env_enhanced_fixed_function	Not Supported
GL_IMG_texture_format_BGRA8888	Not Supported
GL_IMG_user_clip_plane	Not Supported
GL_IMG_vertex_program	Not Supported
GL_INGR_blend_func_separate	Not Supported
GL_INGR_color_clamp	Not Supported
GL_INGR_interlace_read	Not Supported
GL_INGR_multiple_palette	Not Supported
GL_INTEL_compute_shader_lane_shift	Not Supported
GL_INTEL_conservative_rasterization	Not Supported
GL_INTEL_fragment_shader_ordering	Not Supported
GL_INTEL_fragment_shader_span_sharing	Not Supported
GL_INTEL_image_serialize	Not Supported
GL_INTEL_map_texture	Supported
GL_INTEL_multi_rate_fragment_shader	Not Supported
GL_INTEL_parallel_arrays	Not Supported
GL_INTEL_performance_queries	Supported
GL_INTEL_performance_query	Supported
GL_INTEL_texture_scissor	Not Supported
GL_KHR_blend_equation_advanced	Supported
GL_KHR_blend_equation_advanced_coherent	Not Supported
GL_KHR_context_flush_control	Not Supported
GL_KHR_debug	Supported
GL_KHR_robust_buffer_access_behavior	Not Supported
GL_KHR_robustness	Not Supported
GL_KHR_texture_compression_astc_hdr	Not Supported
GL_KHR_texture_compression_astc_ldr	Not Supported
GL_KTX_buffer_region	Not Supported
GL_MESA_pack_invert	Not Supported
GL_MESA_program_debug	Not Supported
GL_MESA_resize_buffers	Not Supported
GL_MESA_texture_array	Not Supported
GL_MESA_texture_signed_rgba	Not Supported
GL_MESA_window_pos	Not Supported
GL_MESA_ycbcr_texture	Not Supported
GL_MESAX_texture_float	Not Supported
GL_MESAX_texture_stack	Not Supported
GL_MTX_fragment_shader	Not Supported
GL_MTX_precision_dpi	Not Supported
GL_NV_3dvision_settings	Not Supported
GL_NV_alpha_test	Not Supported
GL_NV_bgr	Not Supported
GL_NV_bindless_multi_draw_indirect	Not Supported
GL_NV_bindless_multi_draw_indirect_count	Not Supported
GL_NV_bindless_texture	Not Supported
GL_NV_blend_equation_advanced	Not Supported
GL_NV_blend_equation_advanced_coherent	Not Supported
GL_NV_blend_minmax	Not Supported
GL_NV_blend_square	Supported
GL_NV_centroid_sample	Not Supported
GL_NV_command_list	Not Supported

GL_NV_complex_primitives	Not Supported
GL_NV_compute_program5	Not Supported
GL_NV_conditional_render	Supported
GL_NV_conservative_raster	Not Supported
GL_NV_copy_buffer	Not Supported
GL_NV_copy_depth_to_color	Not Supported
GL_NV_copy_image	Not Supported
GL_NV_coverage_sample	Not Supported
GL_NV_deep_texture3D	Not Supported
GL_NV_depth_buffer_float	Not Supported
GL_NV_depth_clamp	Not Supported
GL_NV_depth_nonlinear	Not Supported
GL_NV_depth_range_unclamped	Not Supported
GL_NV_draw_buffers	Not Supported
GL_NV_draw_instanced	Not Supported
GL_NV_draw_texture	Not Supported
GL_NV_EGL_stream_consumer_external	Not Supported
GL_NV_ES1_1_compatibility	Not Supported
GL_NV_ES3_1_compatibility	Not Supported
GL_NV_evaluators	Not Supported
GL_NV_explicit_attrib_location	Not Supported
GL_NV_explicit_multisample	Not Supported
GL_NV_fbo_color_attachments	Not Supported
GL_NV_fence	Not Supported
GL_NV_fill_rectangle	Not Supported
GL_NV_float_buffer	Not Supported
GL_NV_fog_distance	Not Supported
GL_NV_fragdepth	Not Supported
GL_NV_fragment_coverage_to_color	Not Supported
GL_NV_fragment_program	Not Supported
GL_NV_fragment_program_option	Not Supported
GL_NV_fragment_program2	Not Supported
GL_NV_fragment_program4	Not Supported
GL_NV_fragment_shader_interlock	Not Supported
GL_NV_framebuffer_blit	Not Supported
GL_NV_framebuffer_mixed_samples	Not Supported
GL_NV_framebuffer_multisample	Not Supported
GL_NV_framebuffer_multisample_coverage	Not Supported
GL_NV_framebuffer_multisample_ex	Not Supported
GL_NV_generate_mipmap_sRGB	Not Supported
GL_NV_geometry_program4	Not Supported
GL_NV_geometry_shader_passthrough	Not Supported
GL_NV_geometry_shader4	Not Supported
GL_NV_gpu_program_fp64	Not Supported
GL_NV_gpu_program4	Not Supported
GL_NV_gpu_program4_1	Not Supported
GL_NV_gpu_program5	Not Supported
GL_NV_gpu_program5_mem_extended	Not Supported
GL_NV_gpu_shader5	Not Supported
GL_NV_half_float	Not Supported
GL_NV_instanced_arrays	Not Supported
GL_NV_internalformat_sample_query	Not Supported
GL_NV_light_max_exponent	Not Supported
GL_NV_multisample_coverage	Not Supported

GL_NV_multisample_filter_hint	Not Supported
GL_NV_non_square_matrices	Not Supported
GL_NV_occlusion_query	Not Supported
GL_NV_pack_subimage	Not Supported
GL_NV_packed_depth_stencil	Not Supported
GL_NV_packed_float	Not Supported
GL_NV_packed_float_linear	Not Supported
GL_NV_parameter_buffer_object	Not Supported
GL_NV_parameter_buffer_object2	Not Supported
GL_NV_path_rendering	Not Supported
GL_NV_path_rendering_shared_edge	Not Supported
GL_NV_pixel_buffer_object	Not Supported
GL_NV_pixel_data_range	Not Supported
GL_NV_platform_binary	Not Supported
GL_NV_point_sprite	Not Supported
GL_NV_present_video	Not Supported
GL_NV_primitive_restart	Supported
GL_NV_read_buffer	Not Supported
GL_NV_read_buffer_front	Not Supported
GL_NV_read_depth	Not Supported
GL_NV_read_depth_stencil	Not Supported
GL_NV_read_stencil	Not Supported
GL_NV_register_combiners	Not Supported
GL_NV_register_combiners2	Not Supported
GL_NV_sample_locations	Not Supported
GL_NV_sample_mask_override_coverage	Not Supported
GL_NV_shader_atomic_counters	Not Supported
GL_NV_shader_atomic_float	Not Supported
GL_NV_shader_atomic_fp16_vector	Not Supported
GL_NV_shader_atomic_int64	Not Supported
GL_NV_shader_buffer_load	Not Supported
GL_NV_shader_buffer_store	Not Supported
GL_NV_shader_storage_buffer_object	Not Supported
GL_NV_shader_thread_group	Not Supported
GL_NV_shader_thread_shuffle	Not Supported
GL_NV_shadow_samplers_array	Not Supported
GL_NV_shadow_samplers_cube	Not Supported
GL_NV_sRGB_formats	Not Supported
GL_NV_tessellation_program5	Not Supported
GL_NV_texgen_emboss	Not Supported
GL_NV_texgen_reflection	Supported
GL_NV_texture_array	Not Supported
GL_NV_texture_barrier	Not Supported
GL_NV_texture_border_clamp	Not Supported
GL_NV_texture_compression_latc	Not Supported
GL_NV_texture_compression_s3tc	Not Supported
GL_NV_texture_compression_s3tc_update	Not Supported
GL_NV_texture_compression_vtc	Not Supported
GL_NV_texture_env_combine4	Not Supported
GL_NV_texture_expand_normal	Not Supported
GL_NV_texture_lod_clamp	Not Supported
GL_NV_texture_multisample	Not Supported
GL_NV_texture_npot_2D_mipmap	Not Supported
GL_NV_texture_rectangle	Not Supported

GL_NV_texture_shader	Not Supported
GL_NV_texture_shader2	Not Supported
GL_NV_texture_shader3	Not Supported
GL_NV_timer_query	Not Supported
GL_NV_transform_feedback	Not Supported
GL_NV_transform_feedback2	Not Supported
GL_NV_uniform_buffer_unified_memory	Not Supported
GL_NV_vdpau_interop	Not Supported
GL_NV_vertex_array_range	Not Supported
GL_NV_vertex_array_range2	Not Supported
GL_NV_vertex_attrib_64bit	Not Supported
GL_NV_vertex_attrib_integer_64bit	Not Supported
GL_NV_vertex_buffer_unified_memory	Not Supported
GL_NV_vertex_program	Not Supported
GL_NV_vertex_program1_1	Not Supported
GL_NV_vertex_program2	Not Supported
GL_NV_vertex_program2_option	Not Supported
GL_NV_vertex_program3	Not Supported
GL_NV_vertex_program4	Not Supported
GL_NV_video_capture	Not Supported
GL_NV_viewport_array2	Not Supported
GL_NVX_conditional_render	Not Supported
GL_NVX_flush_hold	Not Supported
GL_NVX_gpu_memory_info	Not Supported
GL_NVX_instanced_arrays	Not Supported
GL_NVX_nvenc_interop	Not Supported
GL_NVX_shader_thread_group	Not Supported
GL_NVX_shader_thread_shuffle	Not Supported
GL_NVX_shared_sync_object	Not Supported
GL_NVX_sysmem_buffer	Not Supported
GL_NVX_ycrcb	Not Supported
GL_OES_blend_equation_separate	Not Supported
GL_OES_blend_func_separate	Not Supported
GL_OES_blend_subtract	Not Supported
GL_OES_byte_coordinates	Not Supported
GL_OES_compressed_EAC_R11_signed_texture	Not Supported
GL_OES_compressed_EAC_R11_unsigned_texture	Not Supported
GL_OES_compressed_EAC_RG11_signed_texture	Not Supported
GL_OES_compressed_EAC_RG11_unsigned_texture	Not Supported
GL_OES_compressed_ETC1_RGB8_texture	Not Supported
GL_OES_compressed_ETC2_punchthroughA_RGBA8_texture	Not Supported
GL_OES_compressed_ETC2_punchthroughA_sRGB8_alpha_texture	Not Supported
GL_OES_compressed_ETC2_RGB8_texture	Not Supported
GL_OES_compressed_ETC2_RGBA8_texture	Not Supported
GL_OES_compressed_ETC2_sRGB8_alpha8_texture	Not Supported
GL_OES_compressed_ETC2_sRGB8_texture	Not Supported
GL_OES_compressed_paletted_texture	Not Supported
GL_OES_conditional_query	Not Supported
GL_OES_depth_texture	Not Supported
GL_OES_depth_texture_cube_map	Not Supported
GL_OES_depth24	Not Supported
GL_OES_depth32	Not Supported
GL_OES_draw_texture	Not Supported
GL_OES_EGL_image	Not Supported

GL_OES_EGL_image_external	Not Supported
GL_OES_EGL_sync	Not Supported
GL_OES_element_index_uint	Not Supported
GL_OES_extended_matrix_palette	Not Supported
GL_OES_fbo_render_mipmap	Not Supported
GL_OES_fixed_point	Not Supported
GL_OES_fragment_precision_high	Not Supported
GL_OES_framebuffer_object	Not Supported
GL_OES_get_program_binary	Not Supported
GL_OES_mapbuffer	Not Supported
GL_OES_matrix_get	Not Supported
GL_OES_matrix_palette	Not Supported
GL_OES_packed_depth_stencil	Not Supported
GL_OES_point_size_array	Not Supported
GL_OES_point_sprite	Not Supported
GL_OES_query_matrix	Not Supported
GL_OES_read_format	Not Supported
GL_OES_required_internalformat	Not Supported
GL_OES_rgb8_rgba8	Not Supported
GL_OES_sample_shading	Not Supported
GL_OES_sample_variables	Not Supported
GL_OES_shader_image_atomic	Not Supported
GL_OES_shader_multisample_interpolation	Not Supported
GL_OES_single_precision	Not Supported
GL_OES_standard_derivatives	Not Supported
GL_OES_stencil_wrap	Not Supported
GL_OES_stencil1	Not Supported
GL_OES_stencil4	Not Supported
GL_OES_stencil8	Not Supported
GL_OES_surfaceless_context	Not Supported
GL_OES_texture_3D	Not Supported
GL_OES_texture_compression_astc	Not Supported
GL_OES_texture_cube_map	Not Supported
GL_OES_texture_env_crossbar	Not Supported
GL_OES_texture_float	Not Supported
GL_OES_texture_float_linear	Not Supported
GL_OES_texture_half_float	Not Supported
GL_OES_texture_half_float_linear	Not Supported
GL_OES_texture_mirrored_repeat	Not Supported
GL_OES_texture_npot	Not Supported
GL_OES_texture_stencil8	Not Supported
GL_OES_texture_storage_multisample_2d_array	Not Supported
GL_OES_vertex_array_object	Not Supported
GL_OES_vertex_half_float	Not Supported
GL_OES_vertex_type_10_10_10_2	Not Supported
GL_OML_interlace	Not Supported
GL_OML_resample	Not Supported
GL_OML_subsample	Not Supported
GL_PGI_misc_hints	Not Supported
GL_PGI_vertex_hints	Not Supported
GL_QCOM_alpha_test	Not Supported
GL_QCOM_binning_control	Not Supported
GL_QCOM_driver_control	Not Supported
GL_QCOM_extended_get	Not Supported

GL_QCOM_extended_get2	Not Supported
GL_QCOM_perfmon_global_mode	Not Supported
GL_QCOM_tiled_rendering	Not Supported
GL_QCOM_writeonly_rendering	Not Supported
GL_REND_screen_coordinates	Not Supported
GL_S3_performance_analyzer	Not Supported
GL_S3_s3tc	Not Supported
GL_SGI_color_matrix	Not Supported
GL_SGI_color_table	Not Supported
GL_SGI_compiled_vertex_array	Not Supported
GL_SGI_cull_vertex	Not Supported
GL_SGI_index_array_formats	Not Supported
GL_SGI_index_func	Not Supported
GL_SGI_index_material	Not Supported
GL_SGI_index_texture	Not Supported
GL_SGI_make_current_read	Not Supported
GL_SGI_texture_add_env	Not Supported
GL_SGI_texture_color_table	Not Supported
GL_SGI_texture_edge_clamp	Not Supported
GL_SGI_texture_lod	Not Supported
GL_SGIS_color_range	Not Supported
GL_SGIS_detail_texture	Not Supported
GL_SGIS_fog_function	Not Supported
GL_SGIS_generate_mipmap	Supported
GL_SGIS_multisample	Not Supported
GL_SGIS_multitexture	Not Supported
GL_SGIS_pixel_texture	Not Supported
GL_SGIS_point_line_texgen	Not Supported
GL_SGIS_sharpen_texture	Not Supported
GL_SGIS_texture_border_clamp	Not Supported
GL_SGIS_texture_color_mask	Not Supported
GL_SGIS_texture_edge_clamp	Supported
GL_SGIS_texture_filter4	Not Supported
GL_SGIS_texture_lod	Supported
GL_SGIS_texture_select	Not Supported
GL_SGIS_texture4D	Not Supported
GL_SGIX_async	Not Supported
GL_SGIX_async_histogram	Not Supported
GL_SGIX_async_pixel	Not Supported
GL_SGIX_blend_alpha_minmax	Not Supported
GL_SGIX_clipmap	Not Supported
GL_SGIX_convolution_accuracy	Not Supported
GL_SGIX_depth_pass_instrument	Not Supported
GL_SGIX_depth_texture	Not Supported
GL_SGIX_flush_raster	Not Supported
GL_SGIX_fog_offset	Not Supported
GL_SGIX_fog_texture	Not Supported
GL_SGIX_fragment_specular_lighting	Not Supported
GL_SGIX_framezoom	Not Supported
GL_SGIX_instruments	Not Supported
GL_SGIX_interlace	Not Supported
GL_SGIX_ir_instrument1	Not Supported
GL_SGIX_list_priority	Not Supported
GL_SGIX_pbuffer	Not Supported

GL_SGIX_pixel_texture	Not Supported
GL_SGIX_pixel_texture_bits	Not Supported
GL_SGIX_reference_plane	Not Supported
GL_SGIX_resample	Not Supported
GL_SGIX_shadow	Not Supported
GL_SGIX_shadow_ambient	Not Supported
GL_SGIX_sprite	Not Supported
GL_SGIX_subsample	Not Supported
GL_SGIX_tag_sample_buffer	Not Supported
GL_SGIX_texture_add_env	Not Supported
GL_SGIX_texture_coordinate_clamp	Not Supported
GL_SGIX_texture_lod_bias	Not Supported
GL_SGIX_texture_multi_buffer	Not Supported
GL_SGIX_texture_range	Not Supported
GL_SGIX_texture_scale_bias	Not Supported
GL_SGIX_vertex_preclip	Not Supported
GL_SGIX_vertex_preclip_hint	Not Supported
GL_SGIX_ycrcb	Not Supported
GL_SGIX_ycrcb_subsample	Not Supported
GL_SUN_convolution_border_modes	Not Supported
GL_SUN_global_alpha	Not Supported
GL_SUN_mesh_array	Not Supported
GL_SUN_multi_draw_arrays	Supported
GL_SUN_read_video_pixels	Not Supported
GL_SUN_slice_accum	Not Supported
GL_SUN_triangle_list	Not Supported
GL_SUN_vertex	Not Supported
GL_SUNX_constant_data	Not Supported
GL_VIV_shader_binary	Not Supported
GL_WGL_ARB_extensions_string	Not Supported
GL_WGL_EXT_extensions_string	Not Supported
GL_WGL_EXT_swap_control	Not Supported
GL_WIN_phong_shading	Not Supported
GL_WIN_specular_fog	Not Supported
GL_WIN_swap_hint	Supported
GLU_EXT_nurbs_tessellator	Not Supported
GLU_EXT_object_space_tess	Not Supported
GLU_SGI_filter4_parameters	Not Supported
GLX_AMD_gpu_association	Not Supported
GLX_ARB_create_context	Not Supported
GLX_ARB_create_context_profile	Not Supported
GLX_ARB_create_context_robustness	Not Supported
GLX_ARB_fbconfig_float	Not Supported
GLX_ARB_framebuffer_sRGB	Not Supported
GLX_ARB_get_proc_address	Not Supported
GLX_ARB_multisample	Not Supported
GLX_ARB_robustness_application_isolation	Not Supported
GLX_ARB_robustness_share_group_isolation	Not Supported
GLX_ARB_vertex_buffer_object	Not Supported
GLX_EXT_buffer_age	Not Supported
GLX_EXT_create_context_es_profile	Not Supported
GLX_EXT_create_context_es2_profile	Not Supported
GLX_EXT_fbconfig_packed_float	Not Supported
GLX_EXT_framebuffer_sRGB	Not Supported

GLX_EXT_import_context	Not Supported
GLX_EXT_scene_marker	Not Supported
GLX_EXT_swap_control	Not Supported
GLX_EXT_swap_control_tear	Not Supported
GLX_EXT_texture_from_pixmap	Not Supported
GLX_EXT_visual_info	Not Supported
GLX_EXT_visual_rating	Not Supported
GLX_INTEL_swap_event	Not Supported
GLX_MESA_agp_offset	Not Supported
GLX_MESA_copy_sub_buffer	Not Supported
GLX_MESA_multithread_makecurrent	Not Supported
GLX_MESA_pixmap_colormap	Not Supported
GLX_MESA_query_renderer	Not Supported
GLX_MESA_release_buffers	Not Supported
GLX_MESA_set_3dfx_mode	Not Supported
GLX_MESA_swap_control	Not Supported
GLX_NV_copy_image	Not Supported
GLX_NV_delay_before_swap	Not Supported
GLX_NV_float_buffer	Not Supported
GLX_NV_multisample_coverage	Not Supported
GLX_NV_present_video	Not Supported
GLX_NV_swap_group	Not Supported
GLX_NV_video_capture	Not Supported
GLX_NV_video_out	Not Supported
GLX_NV_video_output	Not Supported
GLX_OML_interlace	Not Supported
GLX_OML_swap_method	Not Supported
GLX_OML_sync_control	Not Supported
GLX_SGI_cushion	Not Supported
GLX_SGI_make_current_read	Not Supported
GLX_SGI_swap_control	Not Supported
GLX_SGI_video_sync	Not Supported
GLX_SGIS_blended_overlay	Not Supported
GLX_SGIS_color_range	Not Supported
GLX_SGIS_multisample	Not Supported
GLX_SGIX_dm_buffer	Not Supported
GLX_SGIX_fbconfig	Not Supported
GLX_SGIX_hyperpipe	Not Supported
GLX_SGIX_pbuffer	Not Supported
GLX_SGIX_swap_barrier	Not Supported
GLX_SGIX_swap_group	Not Supported
GLX_SGIX_video_resize	Not Supported
GLX_SGIX_video_source	Not Supported
GLX_SGIX_visual_select_group	Not Supported
GLX_SUN_get_transparent_index	Not Supported
GLX_SUN_video_resize	Not Supported
WGL_3DFX_gamma_control	Not Supported
WGL_3DFX_multisample	Not Supported
WGL_3DL_stereo_control	Not Supported
WGL_AMD_gpu_association	Not Supported
WGL_AMDX_gpu_association	Not Supported
WGL_ARB_buffer_region	Supported
WGL_ARB_context_flush_control	Not Supported
WGL_ARB_create_context	Supported

WGL_ARB_create_context_profile	Supported
WGL_ARB_create_context_robustness	Supported
WGL_ARB_extensions_string	Supported
WGL_ARB_framebuffer_sRGB	Supported
WGL_ARB_make_current_read	Supported
WGL_ARB_multisample	Supported
WGL_ARB_pbuffer	Supported
WGL_ARB_pixel_format	Supported
WGL_ARB_pixel_format_float	Supported
WGL_ARB_render_texture	Not Supported
WGL_ARB_robustness_application_isolation	Not Supported
WGL_ARB_robustness_share_group_isolation	Not Supported
WGL_ATI_pbuffer_memory_hint	Not Supported
WGL_ATI_pixel_format_float	Not Supported
WGL_ATI_render_texture_rectangle	Not Supported
WGL_EXT_buffer_region	Not Supported
WGL_EXT_create_context_es_profile	Supported
WGL_EXT_create_context_es2_profile	Supported
WGL_EXT_depth_float	Supported
WGL_EXT_display_color_table	Not Supported
WGL_EXT_extensions_string	Supported
WGL_EXT_framebuffer_sRGB	Not Supported
WGL_EXT_framebuffer_sRGBWGL_ARB_create_context	Not Supported
WGL_EXT_gamma_control	Not Supported
WGL_EXT_make_current_read	Not Supported
WGL_EXT_multisample	Not Supported
WGL_EXT_pbuffer	Not Supported
WGL_EXT_pixel_format	Not Supported
WGL_EXT_pixel_format_packed_float	Supported
WGL_EXT_render_texture	Not Supported
WGL_EXT_swap_control	Supported
WGL_EXT_swap_control_tear	Supported
WGL_EXT_swap_interval	Not Supported
WGL_I3D_digital_video_control	Not Supported
WGL_I3D_gamma	Not Supported
WGL_I3D_genlock	Not Supported
WGL_I3D_image_buffer	Not Supported
WGL_I3D_swap_frame_lock	Not Supported
WGL_I3D_swap_frame_usage	Not Supported
WGL_MTX_video_preview	Not Supported
WGL_NV_copy_image	Not Supported
WGL_NV_delay_before_swap	Not Supported
WGL_NV_DX_interop	Supported
WGL_NV_DX_interop2	Not Supported
WGL_NV_float_buffer	Not Supported
WGL_NV_gpu_affinity	Not Supported
WGL_NV_multisample_coverage	Not Supported
WGL_NV_present_video	Not Supported
WGL_NV_render_depth_texture	Not Supported
WGL_NV_render_texture_rectangle	Not Supported
WGL_NV_swap_group	Not Supported
WGL_NV_texture_rectangle	Not Supported
WGL_NV_vertex_array_range	Not Supported
WGL_NV_video_capture	Not Supported

WGL_NV_video_output	Not Supported
WGL_NVX_DX_interop	Not Supported
WGL_OML_sync_control	Not Supported
WGL_S3_cl_sharingWGL_ARB_create_context_profile	Not Supported

Supported Compressed Texture Formats:

RGB DXT1	Supported
RGBA DXT1	Supported
RGBA DXT3	Supported
RGBA DXT5	Supported
RGB FXT1	Supported
RGBA FXT1	Supported
3Dc	Not Supported

Video Adapter Manufacturer:

Company Name	Intel Corporation
Product Information	http://www.intel.com/products/chipsets
Driver Download	http://support.intel.com/support/graphics
Driver Update	http://www.aida64.com/driver-updates

GPGPU

[Direct3D: Intel(R) HD Graphics 4000 (IVB-MB GT2)]

Device Properties:

Device Name	Intel(R) HD Graphics 4000
GPU Code Name	IVB-MB GT2
PCI Device	8086-0166 / 1025-0649 (Rev 09)
Dedicated Memory	32 MB
Driver Name	igdumdim32.dll
Driver Version	10.18.10.3958
Shader Model	SM 5.0
Max Threads	1024
Multiple UAV Access	8 UAVs
Thread Dispatch	3D
Thread Local Storage	32 KB

Device Features:

10-bit Precision Floating-Point	Not Supported
16-bit Precision Floating-Point	Not Supported
Append/Consume Buffers	Supported
Atomic Operations	Supported
Double-Precision Floating-Point	Supported
Gather4	Supported
Indirect Compute Dispatch	Supported
Map On Default Buffers	Supported

Device Manufacturer:

Company Name	Intel Corporation
Product Information	http://www.intel.com/products/chipsets
Driver Download	http://support.intel.com/support/graphics

Driver Update	http://www.aida64.com/driver-updates

[OpenCL: Intel(R) Core(TM) i7-3520M CPU @ 2.90GHz]

OpenCL Properties:

Platform Name	Intel(R) OpenCL
Platform Vendor	Intel(R) Corporation
Platform Version	OpenCL 1.2
Platform Profile	Full

Device Properties:

Device Name	Intel(R) Core(TM) i7-3520M CPU @ 2.90GHz
Device Type	CPU
Device Vendor	Intel(R) Corporation
Device Version	OpenCL 1.2 (Build 76413)
Device Profile	Full
Driver Version	3.0.1.10878
OpenCL C Version	OpenCL C 1.2
Clock Rate	2899 MHz
Compute Units	4
Address Space Size	32-bit
Max 2D Image Size	16384 x 16384
Max 3D Image Size	2048 x 2048 x 2048
Max Image Array Size	2048
Max Image Buffer Size	33552384
Max Samplers	480
Max Work-Item Size	1024 x 1024 x 1024
Max Work-Group Size	1024
Max Argument Size	3840 bytes
Max Constant Buffer Size	128 KB
Max Constant Arguments	480
Max Printf Buffer Size	1 MB
Native ISA Vector Widths	char16, short8, int2, float8, double4
Preferred Native Vector Widths	char1, short1, int1, long1, float1, double1
Profiling Timer Resolution	353 ns
OpenCL DLL	opencl.dll (1.2.11.0)

Memory Properties:

Global Memory	2047 MB
Global Memory Cache	256 KB (Read/Write, 64-byte line)
Local Memory	32 KB
Max Memory Object Allocation Size	524256 KB
Memory Base Address Alignment	1024-bit
Min Data Type Alignment	128 bytes

OpenCL Compliancy:

OpenCL 1.1	Yes (100%)
OpenCL 1.2	Yes (100%)
OpenCL 2.0	No (62%)

Device Features:

Command-Queue Out Of Order Execution	Enabled
Command-Queue Profiling	Enabled
Compiler Available	Yes

Error Correction	Not Supported
Images	Supported
Kernel Execution	Supported
Linker Available	Yes
Little-Endian Device	Yes
Native Kernel Execution	Supported
SVM Atomics	Not Supported
SVM Coarse Grain Buffer	Not Supported
SVM Fine Grain Buffer	Not Supported
SVM Fine Grain System	Not Supported
Thread Trace	Not Supported
Unified Memory	Yes

Half-Precision Floating-Point Capabilities:

Correctly Rounded Divide and Sqrt	Not Supported
Denorms	Not Supported
IEEE754-2008 FMA	Not Supported
INF and NaNs	Not Supported
Rounding to Infinity	Not Supported
Rounding to Nearest Even	Not Supported
Rounding to Zero	Not Supported
Software Basic Floating-Point Operations	No

Single-Precision Floating-Point Capabilities:

Correctly Rounded Divide and Sqrt	Not Supported
Denorms	Supported
IEEE754-2008 FMA	Not Supported
INF and NaNs	Supported
Rounding to Infinity	Not Supported
Rounding to Nearest Even	Supported
Rounding to Zero	Not Supported
Software Basic Floating-Point Operations	No

Double-Precision Floating-Point Capabilities:

Correctly Rounded Divide and Sqrt	Not Supported
Denorms	Supported
IEEE754-2008 FMA	Supported
INF and NaNs	Supported
Rounding to Infinity	Supported
Rounding to Nearest Even	Supported
Rounding to Zero	Supported
Software Basic Floating-Point Operations	No

Device Extensions:

Total / Supported Extensions	88 / 14
cl_altera_compiler_mode	Not Supported
cl_altera_device_temperature	Not Supported
cl_altera_live_object_tracking	Not Supported
cl_amd_bus_addressable_memory	Not Supported
cl_amd_c1x_atomics	Not Supported
cl_amd_compile_options	Not Supported
cl_amd_core_id	Not Supported
cl_amd_d3d10_interop	Not Supported
cl_amd_d3d9_interop	Not Supported

cl_amd_device_attribute_query	Not Supported
cl_amd_device_board_name	Not Supported
cl_amd_device_memory_flags	Not Supported
cl_amd_device_persistent_memory	Not Supported
cl_amd_device_profiling_timer_offset	Not Supported
cl_amd_device_topology	Not Supported
cl_amd_event_callback	Not Supported
cl_amd_fp64	Not Supported
cl_amd_hsa	Not Supported
cl_amd_image2d_from_buffer_read_only	Not Supported
cl_amd_media_ops	Not Supported
cl_amd_media_ops2	Not Supported
cl_amd_offline_devices	Not Supported
cl_amd_popcnt	Not Supported
cl_amd_predefined_macros	Not Supported
cl_amd_printf	Not Supported
cl_amd_svm	Not Supported
cl_amd_vec3	Not Supported
cl_apple_contextloggingfunctions	Not Supported
cl_apple_gl_sharing	Not Supported
cl_apple_setmemobjectdestructor	Not Supported
cl_arm_core_id	Not Supported
cl_arm_printf	Not Supported
cl_ext_atomic_counters_32	Not Supported
cl_ext_atomic_counters_64	Not Supported
cl_ext_device_fission	Supported
cl_ext_migrate_memobject	Not Supported
cl_intel_accelerator	Not Supported
cl_intel_advanced_motion_estimation	Not Supported
cl_intel_ctz	Not Supported
cl_intel_d3d11_nv12_media_sharing	Not Supported
cl_intel_device_partition_by_names	Not Supported
cl_intel_dx9_media_sharing	Supported
cl_intel_exec_by_local_thread	Supported
cl_intel_motion_estimation	Not Supported
cl_intel_printf	Supported
cl_intel_simultaneous_sharing	Not Supported
cl_intel_subgroups	Not Supported
cl_intel_thread_local_exec	Not Supported
cl_khr_3d_image_writes	Not Supported
cl_khr_byte_addressable_store	Supported
cl_khr_context_abort	Not Supported
cl_khr_d3d10_sharing	Not Supported
cl_khr_d3d11_sharing	Supported
cl_khr_depth_images	Not Supported
cl_khr_dx9_media_sharing	Supported
cl_khr_egl_event	Not Supported
cl_khr_egl_image	Not Supported
cl_khr_fp16	Not Supported
cl_khr_fp64	Supported
cl_khr_gl_depth_images	Not Supported
cl_khr_gl_event	Not Supported
cl_khr_gl_msaa_sharing	Not Supported
cl_khr_gl_sharing	Supported

cl_khr_global_int32_base_atomics	Supported
cl_khr_global_int32_extended_atomics	Supported
cl_khr_icd	Supported
cl_khr_image2d_from_buffer	Not Supported
cl_khr_initialize_memory	Not Supported
cl_khr_int64_base_atomics	Not Supported
cl_khr_int64_extended_atomics	Not Supported
cl_khr_local_int32_base_atomics	Supported
cl_khr_local_int32_extended_atomics	Supported
cl_khr_mipmap_image	Not Supported
cl_khr_mipmap_image_writes	Not Supported
cl_khr_select_fprounding_mode	Not Supported
cl_khr_spir	Not Supported
cl_khr_srgb_image_writes	Not Supported
cl_khr_subgroups	Not Supported
cl_khr_terminate_context	Not Supported
cl_nv_compiler_options	Not Supported
cl_nv_copy_opts	Not Supported
cl_nv_d3d10_sharing	Not Supported
cl_nv_d3d11_sharing	Not Supported
cl_nv_d3d9_sharing	Not Supported
cl_nv_device_attribute_query	Not Supported
cl_nv_pragma_unroll	Not Supported
cl_qcom_ext_host_ptr	Not Supported
cl_qcom_ion_host_ptr	Not Supported

Device Manufacturer:

Company Name	Intel Corporation
Product Information	http://www.intel.com/products/chipsets
Driver Download	http://support.intel.com/support/graphics
Driver Update	http://www.aida64.com/driver-updates

[OpenCL: Intel(R) HD Graphics 4000 (IVB-MB GT2)]

OpenCL Properties:

Platform Name	Intel(R) OpenCL
Platform Vendor	Intel(R) Corporation
Platform Version	OpenCL 1.2
Platform Profile	Full

Device Properties:

Device Name	Intel(R) HD Graphics 4000
GPU Code Name	IVB-MB GT2
Device Type	GPU
Device Vendor	Intel(R) Corporation
Device Version	OpenCL 1.2
Device Profile	Full
Driver Version	10.18.10.3958
OpenCL C Version	OpenCL C 1.2
Supported Built-In Kernels	block_motion_estimate_intel
Clock Rate	1250 MHz
Compute Units / Cores	16 / 64
Address Space Size	64-bit
Max 2D Image Size	16384 x 16384

Max 3D Image Size	2048 x 2048 x 2048
Max Image Array Size	2048
Max Image Buffer Size	22937600
Max Samplers	16
Max Work-Item Size	512 x 512 x 512
Max Work-Group Size	512
Max Argument Size	1 KB
Max Constant Buffer Size	64 KB
Max Constant Arguments	8
Max Printf Buffer Size	4 MB
Native ISA Vector Widths	char1, short1, int1, half1, float1
Preferred Native Vector Widths	char1, short1, int1, long1, half1, float1
Profiling Timer Resolution	80 ns
OpenCL DLL	opencl.dll (1.2.11.0)

Memory Properties:

Global Memory	1400 MB
Global Memory Cache	2048 KB (Read/Write, 64-byte line)
Local Memory	64 KB
Max Memory Object Allocation Size	350 MB
Memory Base Address Alignment	1024-bit
Min Data Type Alignment	128 bytes
Image Row Pitch Alignment	64 pixels
Image Base Address Alignment	4096 pixels

OpenCL Compliancy:

OpenCL 1.1	Yes (100%)
OpenCL 1.2	Yes (100%)
OpenCL 2.0	Yes (100%)

Device Features:

Command-Queue Out Of Order Execution	Disabled
Command-Queue Profiling	Enabled
Compiler Available	Yes
Error Correction	Not Supported
Images	Supported
Kernel Execution	Supported
Linker Available	Yes
Little-Endian Device	Yes
Native Kernel Execution	Not Supported
SVM Atomics	Not Supported
SVM Coarse Grain Buffer	Not Supported
SVM Fine Grain Buffer	Not Supported
SVM Fine Grain System	Not Supported
Thread Trace	Not Supported
Unified Memory	Yes

Half-Precision Floating-Point Capabilities:

Correctly Rounded Divide and Sqrt	Not Supported
Denorms	Not Supported
IEEE754-2008 FMA	Not Supported
INF and NaNs	Not Supported
Rounding to Infinity	Not Supported
Rounding to Nearest Even	Not Supported

Rounding to Zero	Not Supported
Software Basic Floating-Point Operations	No

Single-Precision Floating-Point Capabilities:

Correctly Rounded Divide and Sqrt	Supported
Denorms	Not Supported
IEEE754-2008 FMA	Not Supported
INF and NaNs	Supported
Rounding to Infinity	Supported
Rounding to Nearest Even	Supported
Rounding to Zero	Supported
Software Basic Floating-Point Operations	No

Double-Precision Floating-Point Capabilities:

Correctly Rounded Divide and Sqrt	Not Supported
Denorms	Not Supported
IEEE754-2008 FMA	Not Supported
INF and NaNs	Not Supported
Rounding to Infinity	Not Supported
Rounding to Nearest Even	Not Supported
Rounding to Zero	Not Supported
Software Basic Floating-Point Operations	No

Device Extensions:

Total / Supported Extensions	88 / 20
cl_altera_compiler_mode	Not Supported
cl_altera_device_temperature	Not Supported
cl_altera_live_object_tracking	Not Supported
cl_amd_bus_addressable_memory	Not Supported
cl_amd_c1x_atomics	Not Supported
cl_amd_compile_options	Not Supported
cl_amd_core_id	Not Supported
cl_amd_d3d10_interop	Not Supported
cl_amd_d3d9_interop	Not Supported
cl_amd_device_attribute_query	Not Supported
cl_amd_device_board_name	Not Supported
cl_amd_device_memory_flags	Not Supported
cl_amd_device_persistent_memory	Not Supported
cl_amd_device_profiling_timer_offset	Not Supported
cl_amd_device_topology	Not Supported
cl_amd_event_callback	Not Supported
cl_amd_fp64	Not Supported
cl_amd_hsa	Not Supported
cl_amd_image2d_from_buffer_read_only	Not Supported
cl_amd_media_ops	Not Supported
cl_amd_media_ops2	Not Supported
cl_amd_offline_devices	Not Supported
cl_amd_popcnt	Not Supported
cl_amd_predefined_macros	Not Supported
cl_amd_printf	Not Supported
cl_amd_svm	Not Supported
cl_amd_vec3	Not Supported
cl_apple_contextloggingfunctions	Not Supported
cl_apple_gl_sharing	Not Supported

cl_apple_setmemobjectdestructor	Not Supported
cl_arm_core_id	Not Supported
cl_arm_printf	Not Supported
cl_ext_atomic_counters_32	Not Supported
cl_ext_atomic_counters_64	Not Supported
cl_ext_device_fission	Not Supported
cl_ext_migrate_memobject	Not Supported
cl_intel_accelerator	Supported
cl_intel_advanced_motion_estimation	Not Supported
cl_intel_ctz	Not Supported
cl_intel_d3d11_nv12_media_sharing	Supported
cl_intel_device_partition_by_names	Not Supported
cl_intel_dx9_media_sharing	Supported
cl_intel_exec_by_local_thread	Not Supported
cl_intel_motion_estimation	Supported
cl_intel_printf	Not Supported
cl_intel_simultaneous_sharing	Not Supported
cl_intel_subgroups	Not Supported
cl_intel_thread_local_exec	Not Supported
cl_khr_3d_image_writes	Supported
cl_khr_byte_addressable_store	Supported
cl_khr_context_abort	Not Supported
cl_khr_d3d10_sharing	Supported
cl_khr_d3d11_sharing	Supported
cl_khr_depth_images	Supported
cl_khr_dx9_media_sharing	Supported
cl_khr_egl_event	Not Supported
cl_khr_egl_image	Not Supported
cl_khr_fp16	Not Supported
cl_khr_fp64	Not Supported
cl_khr_gl_depth_images	Supported
cl_khr_gl_event	Supported
cl_khr_gl_msaa_sharing	Supported
cl_khr_gl_sharing	Supported
cl_khr_global_int32_base_atomics	Supported
cl_khr_global_int32_extended_atomics	Supported
cl_khr_icd	Supported
cl_khr_image2d_from_buffer	Supported
cl_khr_initialize_memory	Not Supported
cl_khr_int64_base_atomics	Not Supported
cl_khr_int64_extended_atomics	Not Supported
cl_khr_local_int32_base_atomics	Supported
cl_khr_local_int32_extended_atomics	Supported
cl_khr_mipmap_image	Not Supported
cl_khr_mipmap_image_writes	Not Supported
cl_khr_select_fprounding_mode	Not Supported
cl_khr_spir	Not Supported
cl_khr_srgb_image_writes	Not Supported
cl_khr_subgroups	Not Supported
cl_khr_terminate_context	Not Supported
cl_nv_compiler_options	Not Supported
cl_nv_copy_opts	Not Supported
cl_nv_d3d10_sharing	Not Supported
cl_nv_d3d11_sharing	Not Supported

cl_nv_d3d9_sharing	Not Supported
cl_nv_device_attribute_query	Not Supported
cl_nv_pragma_unroll	Not Supported
cl_qcom_ext_host_ptr	Not Supported
cl_qcom_ion_host_ptr	Not Supported

Device Manufacturer:

Company Name	Intel Corporation
Product Information	http://www.intel.com/products/chipsets
Driver Download	http://support.intel.com/support/graphics
Driver Update	http://www.aida64.com/driver-updates

Fonts

Font Family	Type	Style	Character Set	Char. Size	Char. Weight
@Arial Unicode MS	Swiss	Regular	Arabic	14 x 43	40 %
@Arial Unicode MS	Swiss	Regular	Baltic	14 x 43	40 %
@Arial Unicode MS	Swiss	Regular	Central European	14 x 43	40 %
@Arial Unicode MS	Swiss	Regular	CHINESE_BIG5	14 x 43	40 %
@Arial Unicode MS	Swiss	Regular	CHINESE_GB2312	14 x 43	40 %
@Arial Unicode MS	Swiss	Regular	Cyrillic	14 x 43	40 %
@Arial Unicode MS	Swiss	Regular	Greek	14 x 43	40 %
@Arial Unicode MS	Swiss	Regular	Hangul(Johab)	14 x 43	40 %
@Arial Unicode MS	Swiss	Regular	Hangul	14 x 43	40 %
@Arial Unicode MS	Swiss	Regular	Hebrew	14 x 43	40 %
@Arial Unicode MS	Swiss	Regular	Japanese	14 x 43	40 %
@Arial Unicode MS	Swiss	Regular	Thai	14 x 43	40 %
@Arial Unicode MS	Swiss	Regular	Turkish	14 x 43	40 %
@Arial Unicode MS	Swiss	Regular	Vietnamese	14 x 43	40 %
@Arial Unicode MS	Swiss	Regular	Western	14 x 43	40 %
@Batang	Roman	Regular	Baltic	16 x 32	40 %
@Batang	Roman	Regular	Central European	16 x 32	40 %
@Batang	Roman	Regular	Cyrillic	16 x 32	40 %
@Batang	Roman	Regular	Greek	16 x 32	40 %
@Batang	Roman	Regular	Hangul	16 x 32	40 %
@Batang	Roman	Regular	Turkish	16 x 32	40 %
@Batang	Roman	Regular	Western	16 x 32	40 %
@BatangChe	Modern	Regular	Baltic	16 x 32	40 %
@BatangChe	Modern	Regular	Central European	16 x 32	40 %
@BatangChe	Modern	Regular	Cyrillic	16 x 32	40 %
@BatangChe	Modern	Regular	Greek	16 x 32	40 %
@BatangChe	Modern	Regular	Hangul	16 x 32	40 %
@BatangChe	Modern	Regular	Turkish	16 x 32	40 %
@BatangChe	Modern	Regular	Western	16 x 32	40 %
@DFKai-SB	Script	Regular	CHINESE_BIG5	16 x 32	40 %
@DFKai-SB	Script	Regular	Western	16 x 32	40 %
@Dotum	Swiss	Regular	Baltic	16 x 32	40 %
@Dotum	Swiss	Regular	Central European	16 x 32	40 %
@Dotum	Swiss	Regular	Cyrillic	16 x 32	40 %
@Dotum	Swiss	Regular	Greek	16 x 32	40 %
@Dotum	Swiss	Regular	Hangul	16 x 32	40 %
@Dotum	Swiss	Regular	Turkish	16 x 32	40 %

@Dotum	Swiss	Regular	Western	16 x 32	40 %
@DotumChe	Modern	Regular	Baltic	16 x 32	40 %
@DotumChe	Modern	Regular	Central European	16 x 32	40 %
@DotumChe	Modern	Regular	Cyrillic	16 x 32	40 %
@DotumChe	Modern	Regular	Greek	16 x 32	40 %
@DotumChe	Modern	Regular	Hangul	16 x 32	40 %
@DotumChe	Modern	Regular	Turkish	16 x 32	40 %
@DotumChe	Modern	Regular	Western	16 x 32	40 %
@FangSong	Modern	Regular	CHINESE_GB2312	16 x 32	40 %
@FangSong	Modern	Regular	Western	16 x 32	40 %
@Gulim	Swiss	Regular	Baltic	16 x 32	40 %
@Gulim	Swiss	Regular	Central European	16 x 32	40 %
@Gulim	Swiss	Regular	Cyrillic	16 x 32	40 %
@Gulim	Swiss	Regular	Greek	16 x 32	40 %
@Gulim	Swiss	Regular	Hangul	16 x 32	40 %
@Gulim	Swiss	Regular	Turkish	16 x 32	40 %
@Gulim	Swiss	Regular	Western	16 x 32	40 %
@GulimChe	Modern	Regular	Baltic	16 x 32	40 %
@GulimChe	Modern	Regular	Central European	16 x 32	40 %
@GulimChe	Modern	Regular	Cyrillic	16 x 32	40 %
@GulimChe	Modern	Regular	Greek	16 x 32	40 %
@GulimChe	Modern	Regular	Hangul	16 x 32	40 %
@GulimChe	Modern	Regular	Turkish	16 x 32	40 %
@GulimChe	Modern	Regular	Western	16 x 32	40 %
@Gungsuh	Roman	Regular	Baltic	16 x 32	40 %
@Gungsuh	Roman	Regular	Central European	16 x 32	40 %
@Gungsuh	Roman	Regular	Cyrillic	16 x 32	40 %
@Gungsuh	Roman	Regular	Greek	16 x 32	40 %
@Gungsuh	Roman	Regular	Hangul	16 x 32	40 %
@Gungsuh	Roman	Regular	Turkish	16 x 32	40 %
@Gungsuh	Roman	Regular	Western	16 x 32	40 %
@GungsuhChe	Modern	Regular	Baltic	16 x 32	40 %
@GungsuhChe	Modern	Regular	Central European	16 x 32	40 %
@GungsuhChe	Modern	Regular	Cyrillic	16 x 32	40 %
@GungsuhChe	Modern	Regular	Greek	16 x 32	40 %
@GungsuhChe	Modern	Regular	Hangul	16 x 32	40 %
@GungsuhChe	Modern	Regular	Turkish	16 x 32	40 %
@GungsuhChe	Modern	Regular	Western	16 x 32	40 %
@KaiTi	Modern	Regular	CHINESE_GB2312	16 x 32	40 %
@KaiTi	Modern	Regular	Western	16 x 32	40 %
@Malgun Gothic	Swiss	Regular	Hangul	15 x 43	40 %
@Malgun Gothic	Swiss	Regular	Western	15 x 43	40 %
@Meiryo UI	Swiss	Regular	Baltic	17 x 41	40 %
@Meiryo UI	Swiss	Regular	Central European	17 x 41	40 %
@Meiryo UI	Swiss	Regular	Cyrillic	17 x 41	40 %
@Meiryo UI	Swiss	Regular	Greek	17 x 41	40 %
@Meiryo UI	Swiss	Regular	Japanese	17 x 41	40 %
@Meiryo UI	Swiss	Regular	Turkish	17 x 41	40 %
@Meiryo UI	Swiss	Regular	Western	17 x 41	40 %
@Meiryo	Swiss	Regular	Baltic	31 x 48	40 %
@Meiryo	Swiss	Regular	Central European	31 x 48	40 %
@Meiryo	Swiss	Regular	Cyrillic	31 x 48	40 %
@Meiryo	Swiss	Regular	Greek	31 x 48	40 %
@Meiryo	Swiss	Regular	Japanese	31 x 48	40 %

@Meiryo	Swiss	Regular	Turkish	31 x 48	40 %
@Meiryo	Swiss	Regular	Western	31 x 48	40 %
@Microsoft JhengHei Light	Swiss	Regular	Baltic	32 x 43	29 %
@Microsoft JhengHei Light	Swiss	Regular	Central European	32 x 43	29 %
@Microsoft JhengHei Light	Swiss	Regular	CHINESE_BIG5	32 x 43	29 %
@Microsoft JhengHei Light	Swiss	Regular	CHINESE_GB2312	32 x 43	29 %
@Microsoft JhengHei Light	Swiss	Regular	Cyrillic	32 x 43	29 %
@Microsoft JhengHei Light	Swiss	Regular	Greek	32 x 43	29 %
@Microsoft JhengHei Light	Swiss	Regular	Hangul(Johab)	32 x 43	29 %
@Microsoft JhengHei Light	Swiss	Regular	Hangul	32 x 43	29 %
@Microsoft JhengHei Light	Swiss	Regular	Hebrew	32 x 43	29 %
@Microsoft JhengHei Light	Swiss	Regular	Japanese	32 x 43	29 %
@Microsoft JhengHei Light	Swiss	Regular	Turkish	32 x 43	29 %
@Microsoft JhengHei Light	Swiss	Regular	Vietnamese	32 x 43	29 %
@Microsoft JhengHei Light	Swiss	Regular	Western	32 x 43	29 %
@Microsoft JhengHei UI Light	Swiss	Regular	Baltic	32 x 41	29 %
@Microsoft JhengHei UI Light	Swiss	Regular	Central European	32 x 41	29 %
@Microsoft JhengHei UI Light	Swiss	Regular	CHINESE_BIG5	32 x 41	29 %
@Microsoft JhengHei UI Light	Swiss	Regular	CHINESE_GB2312	32 x 41	29 %
@Microsoft JhengHei UI Light	Swiss	Regular	Cyrillic	32 x 41	29 %
@Microsoft JhengHei UI Light	Swiss	Regular	Greek	32 x 41	29 %
@Microsoft JhengHei UI Light	Swiss	Regular	Hangul(Johab)	32 x 41	29 %
@Microsoft JhengHei UI Light	Swiss	Regular	Hangul	32 x 41	29 %
@Microsoft JhengHei UI Light	Swiss	Regular	Hebrew	32 x 41	29 %
@Microsoft JhengHei UI Light	Swiss	Regular	Japanese	32 x 41	29 %
@Microsoft JhengHei UI Light	Swiss	Regular	Turkish	32 x 41	29 %
@Microsoft JhengHei UI Light	Swiss	Regular	Vietnamese	32 x 41	29 %
@Microsoft JhengHei UI Light	Swiss	Regular	Western	32 x 41	29 %
@Microsoft JhengHei UI	Swiss	Regular	CHINESE_BIG5	15 x 41	40 %
@Microsoft JhengHei UI	Swiss	Regular	Greek	15 x 41	40 %
@Microsoft JhengHei UI	Swiss	Regular	Western	15 x 41	40 %
@Microsoft JhengHei	Swiss	Regular	CHINESE_BIG5	15 x 43	40 %
@Microsoft JhengHei	Swiss	Regular	Greek	15 x 43	40 %
@Microsoft JhengHei	Swiss	Regular	Western	15 x 43	40 %
@Microsoft YaHei Light	Swiss	Regular	Central European	15 x 41	29 %
@Microsoft YaHei Light	Swiss	Regular	CHINESE_GB2312	15 x 41	29 %
@Microsoft YaHei Light	Swiss	Regular	Cyrillic	15 x 41	29 %
@Microsoft YaHei Light	Swiss	Regular	Greek	15 x 41	29 %
@Microsoft YaHei Light	Swiss	Regular	Western	15 x 41	29 %
@Microsoft YaHei UI Light	Swiss	Regular	Central European	15 x 42	29 %
@Microsoft YaHei UI Light	Swiss	Regular	CHINESE_GB2312	15 x 42	29 %
@Microsoft YaHei UI Light	Swiss	Regular	Cyrillic	15 x 42	29 %
@Microsoft YaHei UI Light	Swiss	Regular	Greek	15 x 42	29 %
@Microsoft YaHei UI Light	Swiss	Regular	Western	15 x 42	29 %
@Microsoft YaHei UI	Swiss	Regular	Central European	15 x 41	40 %
@Microsoft YaHei UI	Swiss	Regular	CHINESE_GB2312	15 x 41	40 %
@Microsoft YaHei UI	Swiss	Regular	Cyrillic	15 x 41	40 %
@Microsoft YaHei UI	Swiss	Regular	Greek	15 x 41	40 %
@Microsoft YaHei UI	Swiss	Regular	Turkish	15 x 41	40 %
@Microsoft YaHei UI	Swiss	Regular	Western	15 x 41	40 %
@Microsoft YaHei	Swiss	Regular	Central European	15 x 42	40 %
@Microsoft YaHei	Swiss	Regular	CHINESE_GB2312	15 x 42	40 %
@Microsoft YaHei	Swiss	Regular	Cyrillic	15 x 42	40 %
@Microsoft YaHei	Swiss	Regular	Greek	15 x 42	40 %

@Microsoft YaHei	Swiss	Regular	Turkish	15 x 42	40 %
@Microsoft YaHei	Swiss	Regular	Western	15 x 42	40 %
@MingLiU_HKSCS	Roman	Regular	CHINESE_BIG5	16 x 32	40 %
@MingLiU_HKSCS	Roman	Regular	Western	16 x 32	40 %
@MingLiU_HKSCS-ExtB	Roman	Regular	CHINESE_BIG5	16 x 32	40 %
@MingLiU_HKSCS-ExtB	Roman	Regular	Western	16 x 32	40 %
@MingLiU	Modern	Regular	CHINESE_BIG5	16 x 32	40 %
@MingLiU	Modern	Regular	Western	16 x 32	40 %
@MingLiU-ExtB	Roman	Regular	CHINESE_BIG5	16 x 32	40 %
@MingLiU-ExtB	Roman	Regular	Western	16 x 32	40 %
@MS Gothic	Modern	Regular	Baltic	16 x 32	40 %
@MS Gothic	Modern	Regular	Central European	16 x 32	40 %
@MS Gothic	Modern	Regular	Cyrillic	16 x 32	40 %
@MS Gothic	Modern	Regular	Greek	16 x 32	40 %
@MS Gothic	Modern	Regular	Japanese	16 x 32	40 %
@MS Gothic	Modern	Regular	Turkish	16 x 32	40 %
@MS Gothic	Modern	Regular	Western	16 x 32	40 %
@MS Mincho	Modern	Regular	Baltic	16 x 32	40 %
@MS Mincho	Modern	Regular	Central European	16 x 32	40 %
@MS Mincho	Modern	Regular	Cyrillic	16 x 32	40 %
@MS Mincho	Modern	Regular	Greek	16 x 32	40 %
@MS Mincho	Modern	Regular	Japanese	16 x 32	40 %
@MS Mincho	Modern	Regular	Turkish	16 x 32	40 %
@MS Mincho	Modern	Regular	Western	16 x 32	40 %
@MS PGothic	Swiss	Regular	Baltic	13 x 32	40 %
@MS PGothic	Swiss	Regular	Central European	13 x 32	40 %
@MS PGothic	Swiss	Regular	Cyrillic	13 x 32	40 %
@MS PGothic	Swiss	Regular	Greek	13 x 32	40 %
@MS PGothic	Swiss	Regular	Japanese	13 x 32	40 %
@MS PGothic	Swiss	Regular	Turkish	13 x 32	40 %
@MS PGothic	Swiss	Regular	Western	13 x 32	40 %
@MS PMincho	Roman	Regular	Baltic	13 x 32	40 %
@MS PMincho	Roman	Regular	Central European	13 x 32	40 %
@MS PMincho	Roman	Regular	Cyrillic	13 x 32	40 %
@MS PMincho	Roman	Regular	Greek	13 x 32	40 %
@MS PMincho	Roman	Regular	Japanese	13 x 32	40 %
@MS PMincho	Roman	Regular	Turkish	13 x 32	40 %
@MS PMincho	Roman	Regular	Western	13 x 32	40 %
@MS UI Gothic	Swiss	Regular	Baltic	13 x 32	40 %
@MS UI Gothic	Swiss	Regular	Central European	13 x 32	40 %
@MS UI Gothic	Swiss	Regular	Cyrillic	13 x 32	40 %
@MS UI Gothic	Swiss	Regular	Greek	13 x 32	40 %
@MS UI Gothic	Swiss	Regular	Japanese	13 x 32	40 %
@MS UI Gothic	Swiss	Regular	Turkish	13 x 32	40 %
@MS UI Gothic	Swiss	Regular	Western	13 x 32	40 %
@NSimSun	Modern	Regular	CHINESE_GB2312	16 x 32	40 %
@NSimSun	Modern	Regular	Western	16 x 32	40 %
@PMingLiU	Roman	Regular	CHINESE_BIG5	16 x 32	40 %
@PMingLiU	Roman	Regular	Western	16 x 32	40 %
@PMingLiU-ExtB	Roman	Regular	CHINESE_BIG5	16 x 32	40 %
@PMingLiU-ExtB	Roman	Regular	Western	16 x 32	40 %
@SimHei	Modern	Regular	CHINESE_GB2312	16 x 32	40 %
@SimHei	Modern	Regular	Western	16 x 32	40 %
@SimSun	Special	Regular	CHINESE_GB2312	16 x 32	40 %

@SimSun	Special	Regular	Western	16 x 32	40 %
@SimSun-ExtB	Modern	Regular	CHINESE_GB2312	16 x 32	40 %
@SimSun-ExtB	Modern	Regular	Western	16 x 32	40 %
@Yu Gothic Light	Swiss	Regular	Baltic	31 x 41	30 %
@Yu Gothic Light	Swiss	Regular	Central European	31 x 41	30 %
@Yu Gothic Light	Swiss	Regular	Cyrillic	31 x 41	30 %
@Yu Gothic Light	Swiss	Regular	Greek	31 x 41	30 %
@Yu Gothic Light	Swiss	Regular	Japanese	31 x 41	30 %
@Yu Gothic Light	Swiss	Regular	Turkish	31 x 41	30 %
@Yu Gothic Light	Swiss	Regular	Western	31 x 41	30 %
@Yu Gothic	Swiss	Regular	Baltic	31 x 41	40 %
@Yu Gothic	Swiss	Regular	Central European	31 x 41	40 %
@Yu Gothic	Swiss	Regular	Cyrillic	31 x 41	40 %
@Yu Gothic	Swiss	Regular	Greek	31 x 41	40 %
@Yu Gothic	Swiss	Regular	Japanese	31 x 41	40 %
@Yu Gothic	Swiss	Regular	Turkish	31 x 41	40 %
@Yu Gothic	Swiss	Regular	Western	31 x 41	40 %
@Yu Mincho Demibold	Roman	Bold	Baltic	31 x 41	60 %
@Yu Mincho Demibold	Roman	Bold	Central European	31 x 41	60 %
@Yu Mincho Demibold	Roman	Bold	Cyrillic	31 x 41	60 %
@Yu Mincho Demibold	Roman	Bold	Greek	31 x 41	60 %
@Yu Mincho Demibold	Roman	Bold	Japanese	31 x 41	60 %
@Yu Mincho Demibold	Roman	Bold	Turkish	31 x 41	60 %
@Yu Mincho Demibold	Roman	Bold	Western	31 x 41	60 %
@Yu Mincho Light	Roman	Regular	Baltic	31 x 41	30 %
@Yu Mincho Light	Roman	Regular	Central European	31 x 41	30 %
@Yu Mincho Light	Roman	Regular	Cyrillic	31 x 41	30 %
@Yu Mincho Light	Roman	Regular	Greek	31 x 41	30 %
@Yu Mincho Light	Roman	Regular	Japanese	31 x 41	30 %
@Yu Mincho Light	Roman	Regular	Turkish	31 x 41	30 %
@Yu Mincho Light	Roman	Regular	Western	31 x 41	30 %
@Yu Mincho	Roman	Regular	Baltic	31 x 41	40 %
@Yu Mincho	Roman	Regular	Central European	31 x 41	40 %
@Yu Mincho	Roman	Regular	Cyrillic	31 x 41	40 %
@Yu Mincho	Roman	Regular	Greek	31 x 41	40 %
@Yu Mincho	Roman	Regular	Japanese	31 x 41	40 %
@Yu Mincho	Roman	Regular	Turkish	31 x 41	40 %
@Yu Mincho	Roman	Regular	Western	31 x 41	40 %
Agency FB	Swiss	Regular	Western	10 x 36	40 %
Aharoni	Special	Bold	Hebrew	15 x 32	70 %
Aharoni	Special	Bold	Western	15 x 32	70 %
Aldhabi	Special	Regular	Arabic	16 x 56	40 %
Aldhabi	Special	Regular	Western	16 x 56	40 %
Algerian	Decorative	Regular	Western	17 x 36	40 %
Andalus	Roman	Regular	Arabic	15 x 49	40 %
Andalus	Roman	Regular	Western	15 x 49	40 %
Angsana New	Roman	Regular	Thai	8 x 43	40 %
Angsana New	Roman	Regular	Western	8 x 43	40 %
AngsanaUPC	Roman	Regular	Thai	8 x 43	40 %
AngsanaUPC	Roman	Regular	Western	8 x 43	40 %
Aparajita	Swiss	Regular	Western	16 x 38	40 %
Arabic Typesetting	Script	Regular	Arabic	9 x 36	40 %
Arabic Typesetting	Script	Regular	Baltic	9 x 36	40 %
Arabic Typesetting	Script	Regular	Central European	9 x 36	40 %

Arabic Typesetting	Script	Regular	Turkish	9 x 36	40 %
Arabic Typesetting	Script	Regular	Western	9 x 36	40 %
Arial Black	Swiss	Regular	Baltic	18 x 45	90 %
Arial Black	Swiss	Regular	Central European	18 x 45	90 %
Arial Black	Swiss	Regular	Cyrillic	18 x 45	90 %
Arial Black	Swiss	Regular	Greek	18 x 45	90 %
Arial Black	Swiss	Regular	Turkish	18 x 45	90 %
Arial Black	Swiss	Regular	Western	18 x 45	90 %
Arial Narrow	Swiss	Regular	Baltic	12 x 36	40 %
Arial Narrow	Swiss	Regular	Central European	12 x 36	40 %
Arial Narrow	Swiss	Regular	Cyrillic	12 x 36	40 %
Arial Narrow	Swiss	Regular	Greek	12 x 36	40 %
Arial Narrow	Swiss	Regular	Turkish	12 x 36	40 %
Arial Narrow	Swiss	Regular	Western	12 x 36	40 %
Arial Rounded MT Bold	Swiss	Regular	Western	15 x 37	40 %
Arial Unicode MS	Swiss	Regular	Arabic	14 x 43	40 %
Arial Unicode MS	Swiss	Regular	Baltic	14 x 43	40 %
Arial Unicode MS	Swiss	Regular	Central European	14 x 43	40 %
Arial Unicode MS	Swiss	Regular	CHINESE_BIG5	14 x 43	40 %
Arial Unicode MS	Swiss	Regular	CHINESE_GB2312	14 x 43	40 %
Arial Unicode MS	Swiss	Regular	Cyrillic	14 x 43	40 %
Arial Unicode MS	Swiss	Regular	Greek	14 x 43	40 %
Arial Unicode MS	Swiss	Regular	Hangul(Johab)	14 x 43	40 %
Arial Unicode MS	Swiss	Regular	Hangul	14 x 43	40 %
Arial Unicode MS	Swiss	Regular	Hebrew	14 x 43	40 %
Arial Unicode MS	Swiss	Regular	Japanese	14 x 43	40 %
Arial Unicode MS	Swiss	Regular	Thai	14 x 43	40 %
Arial Unicode MS	Swiss	Regular	Turkish	14 x 43	40 %
Arial Unicode MS	Swiss	Regular	Vietnamese	14 x 43	40 %
Arial Unicode MS	Swiss	Regular	Western	14 x 43	40 %
Arial	Swiss	Regular	Arabic	14 x 36	40 %
Arial	Swiss	Regular	Baltic	14 x 36	40 %
Arial	Swiss	Regular	Central European	14 x 36	40 %
Arial	Swiss	Regular	Cyrillic	14 x 36	40 %
Arial	Swiss	Regular	Greek	14 x 36	40 %
Arial	Swiss	Regular	Hebrew	14 x 36	40 %
Arial	Swiss	Regular	Turkish	14 x 36	40 %
Arial	Swiss	Regular	Vietnamese	14 x 36	40 %
Arial	Swiss	Regular	Western	14 x 36	40 %
Baskerville Old Face	Roman	Regular	Western	13 x 37	40 %
Batang	Roman	Regular	Baltic	16 x 32	40 %
Batang	Roman	Regular	Central European	16 x 32	40 %
Batang	Roman	Regular	Cyrillic	16 x 32	40 %
Batang	Roman	Regular	Greek	16 x 32	40 %
Batang	Roman	Regular	Hangul	16 x 32	40 %
Batang	Roman	Regular	Turkish	16 x 32	40 %
Batang	Roman	Regular	Western	16 x 32	40 %
BatangChe	Modern	Regular	Baltic	16 x 32	40 %
BatangChe	Modern	Regular	Central European	16 x 32	40 %
BatangChe	Modern	Regular	Cyrillic	16 x 32	40 %
BatangChe	Modern	Regular	Greek	16 x 32	40 %
BatangChe	Modern	Regular	Hangul	16 x 32	40 %
BatangChe	Modern	Regular	Turkish	16 x 32	40 %
BatangChe	Modern	Regular	Western	16 x 32	40 %

Bauhaus 93	Decorative	Regular	Western	14 x 36	40 %
Bell MT	Roman	Regular	Western	13 x 35	40 %
Berlin Sans FB Demi	Swiss	Bold	Western	14 x 36	70 %
Berlin Sans FB	Swiss	Regular	Western	13 x 35	40 %
Bernard MT Condensed	Roman	Regular	Western	12 x 38	40 %
Blackadder ITC	Decorative	Regular	Western	10 x 41	40 %
Bodoni MT Black	Roman	Regular	Western	16 x 37	90 %
Bodoni MT Condensed	Roman	Regular	Western	9 x 38	40 %
Bodoni MT Poster Compressed	Roman	Regular	Turkish	8 x 37	30 %
Bodoni MT Poster Compressed	Roman	Regular	Western	8 x 37	30 %
Bodoni MT	Roman	Regular	Western	13 x 38	40 %
Book Antiqua	Roman	Regular	Baltic	14 x 40	40 %
Book Antiqua	Roman	Regular	Central European	14 x 40	40 %
Book Antiqua	Roman	Regular	Cyrillic	14 x 40	40 %
Book Antiqua	Roman	Regular	Greek	14 x 40	40 %
Book Antiqua	Roman	Regular	Turkish	14 x 40	40 %
Book Antiqua	Roman	Regular	Western	14 x 40	40 %
Bookman Old Style	Roman	Regular	Baltic	16 x 36	30 %
Bookman Old Style	Roman	Regular	Central European	16 x 36	30 %
Bookman Old Style	Roman	Regular	Cyrillic	16 x 36	30 %
Bookman Old Style	Roman	Regular	Greek	16 x 36	30 %
Bookman Old Style	Roman	Regular	Turkish	16 x 36	30 %
Bookman Old Style	Roman	Regular	Western	16 x 36	30 %
Bookshelf Symbol 7	Special	Regular	Symbol	21 x 32	40 %
Bradley Hand ITC	Script	Regular	Western	13 x 40	40 %
Britannic Bold	Swiss	Regular	Western	14 x 35	40 %
Broadway	Decorative	Regular	Western	17 x 36	40 %
Browallia New	Swiss	Regular	Thai	9 x 40	40 %
Browallia New	Swiss	Regular	Western	9 x 40	40 %
BrowalliaUPC	Swiss	Regular	Thai	9 x 40	40 %
BrowalliaUPC	Swiss	Regular	Western	9 x 40	40 %
Brush Script MT	Script	Italic	Western	10 x 39	40 %
Calibri Light	Swiss	Regular	Baltic	17 x 39	30 %
Calibri Light	Swiss	Regular	Central European	17 x 39	30 %
Calibri Light	Swiss	Regular	Cyrillic	17 x 39	30 %
Calibri Light	Swiss	Regular	Greek	17 x 39	30 %
Calibri Light	Swiss	Regular	Turkish	17 x 39	30 %
Calibri Light	Swiss	Regular	Vietnamese	17 x 39	30 %
Calibri Light	Swiss	Regular	Western	17 x 39	30 %
Calibri	Swiss	Regular	Baltic	17 x 39	40 %
Calibri	Swiss	Regular	Central European	17 x 39	40 %
Calibri	Swiss	Regular	Cyrillic	17 x 39	40 %
Calibri	Swiss	Regular	Greek	17 x 39	40 %
Calibri	Swiss	Regular	Turkish	17 x 39	40 %
Calibri	Swiss	Regular	Vietnamese	17 x 39	40 %
Calibri	Swiss	Regular	Western	17 x 39	40 %
Californian FB	Roman	Regular	Western	13 x 36	40 %
Calisto MT	Roman	Regular	Western	13 x 37	40 %
Cambria Math	Roman	Regular	Baltic	20 x 179	40 %
Cambria Math	Roman	Regular	Central European	20 x 179	40 %
Cambria Math	Roman	Regular	Cyrillic	20 x 179	40 %
Cambria Math	Roman	Regular	Greek	20 x 179	40 %
Cambria Math	Roman	Regular	Turkish	20 x 179	40 %
Cambria Math	Roman	Regular	Vietnamese	20 x 179	40 %

Cambria Math	Roman	Regular	Western	20 x 179	40 %
Cambria	Roman	Regular	Baltic	20 x 38	40 %
Cambria	Roman	Regular	Central European	20 x 38	40 %
Cambria	Roman	Regular	Cyrillic	20 x 38	40 %
Cambria	Roman	Regular	Greek	20 x 38	40 %
Cambria	Roman	Regular	Turkish	20 x 38	40 %
Cambria	Roman	Regular	Vietnamese	20 x 38	40 %
Cambria	Roman	Regular	Western	20 x 38	40 %
Candara	Swiss	Regular	Baltic	17 x 39	40 %
Candara	Swiss	Regular	Central European	17 x 39	40 %
Candara	Swiss	Regular	Cyrillic	17 x 39	40 %
Candara	Swiss	Regular	Greek	17 x 39	40 %
Candara	Swiss	Regular	Turkish	17 x 39	40 %
Candara	Swiss	Regular	Vietnamese	17 x 39	40 %
Candara	Swiss	Regular	Western	17 x 39	40 %
Castellar	Roman	Regular	Western	21 x 39	40 %
Centaur	Roman	Regular	Western	12 x 36	40 %
Century Gothic	Swiss	Regular	Baltic	16 x 38	40 %
Century Gothic	Swiss	Regular	Central European	16 x 38	40 %
Century Gothic	Swiss	Regular	Cyrillic	16 x 38	40 %
Century Gothic	Swiss	Regular	Greek	16 x 38	40 %
Century Gothic	Swiss	Regular	Turkish	16 x 38	40 %
Century Gothic	Swiss	Regular	Western	16 x 38	40 %
Century Schoolbook	Roman	Regular	Baltic	15 x 38	40 %
Century Schoolbook	Roman	Regular	Central European	15 x 38	40 %
Century Schoolbook	Roman	Regular	Cyrillic	15 x 38	40 %
Century Schoolbook	Roman	Regular	Greek	15 x 38	40 %
Century Schoolbook	Roman	Regular	Turkish	15 x 38	40 %
Century Schoolbook	Roman	Regular	Western	15 x 38	40 %
Century	Roman	Regular	Baltic	15 x 38	40 %
Century	Roman	Regular	Central European	15 x 38	40 %
Century	Roman	Regular	Cyrillic	15 x 38	40 %
Century	Roman	Regular	Greek	15 x 38	40 %
Century	Roman	Regular	Turkish	15 x 38	40 %
Century	Roman	Regular	Western	15 x 38	40 %
Chiller	Decorative	Regular	Western	9 x 37	40 %
Colonna MT	Decorative	Regular	Western	13 x 34	40 %
Comic Sans MS	Script	Regular	Baltic	15 x 45	40 %
Comic Sans MS	Script	Regular	Central European	15 x 45	40 %
Comic Sans MS	Script	Regular	Cyrillic	15 x 45	40 %
Comic Sans MS	Script	Regular	Greek	15 x 45	40 %
Comic Sans MS	Script	Regular	Turkish	15 x 45	40 %
Comic Sans MS	Script	Regular	Western	15 x 45	40 %
Consolas	Modern	Regular	Baltic	18 x 37	40 %
Consolas	Modern	Regular	Central European	18 x 37	40 %
Consolas	Modern	Regular	Cyrillic	18 x 37	40 %
Consolas	Modern	Regular	Greek	18 x 37	40 %
Consolas	Modern	Regular	Turkish	18 x 37	40 %
Consolas	Modern	Regular	Vietnamese	18 x 37	40 %
Consolas	Modern	Regular	Western	18 x 37	40 %
Constantia	Roman	Regular	Baltic	17 x 39	40 %
Constantia	Roman	Regular	Central European	17 x 39	40 %
Constantia	Roman	Regular	Cyrillic	17 x 39	40 %
Constantia	Roman	Regular	Greek	17 x 39	40 %

Constantia	Roman	Regular	Turkish	17 x 39	40 %
Constantia	Roman	Regular	Vietnamese	17 x 39	40 %
Constantia	Roman	Regular	Western	17 x 39	40 %
Cooper Black	Roman	Regular	Western	16 x 37	40 %
Copperplate Gothic Bold	Swiss	Regular	Western	19 x 36	40 %
Copperplate Gothic Light	Swiss	Regular	Western	18 x 35	40 %
Corbel	Swiss	Regular	Baltic	17 x 39	40 %
Corbel	Swiss	Regular	Central European	17 x 39	40 %
Corbel	Swiss	Regular	Cyrillic	17 x 39	40 %
Corbel	Swiss	Regular	Greek	17 x 39	40 %
Corbel	Swiss	Regular	Turkish	17 x 39	40 %
Corbel	Swiss	Regular	Vietnamese	17 x 39	40 %
Corbel	Swiss	Regular	Western	17 x 39	40 %
Cordia New	Swiss	Regular	Thai	9 x 44	40 %
Cordia New	Swiss	Regular	Western	9 x 44	40 %
CordiaUPC	Swiss	Regular	Thai	9 x 44	40 %
CordiaUPC	Swiss	Regular	Western	9 x 44	40 %
Courier New	Modern	Regular	Arabic	19 x 36	40 %
Courier New	Modern	Regular	Baltic	19 x 36	40 %
Courier New	Modern	Regular	Central European	19 x 36	40 %
Courier New	Modern	Regular	Cyrillic	19 x 36	40 %
Courier New	Modern	Regular	Greek	19 x 36	40 %
Courier New	Modern	Regular	Hebrew	19 x 36	40 %
Courier New	Modern	Regular	Turkish	19 x 36	40 %
Courier New	Modern	Regular	Vietnamese	19 x 36	40 %
Courier New	Modern	Regular	Western	19 x 36	40 %
Courier	Modern		Western	8 x 13	40 %
Curlz MT	Decorative	Regular	Western	12 x 42	40 %
DaunPenh	Special	Regular	Western	12 x 43	40 %
David	Swiss	Regular	Hebrew	16 x 31	40 %
David	Swiss	Regular	Western	16 x 31	40 %
DFKai-SB	Script	Regular	CHINESE_BIG5	16 x 32	40 %
DFKai-SB	Script	Regular	Western	16 x 32	40 %
DilleniaUPC	Roman	Regular	Thai	9 x 42	40 %
DilleniaUPC	Roman	Regular	Western	9 x 42	40 %
DokChampa	Swiss	Regular	Thai	19 x 62	40 %
DokChampa	Swiss	Regular	Western	19 x 62	40 %
Dotum	Swiss	Regular	Baltic	16 x 32	40 %
Dotum	Swiss	Regular	Central European	16 x 32	40 %
Dotum	Swiss	Regular	Cyrillic	16 x 32	40 %
Dotum	Swiss	Regular	Greek	16 x 32	40 %
Dotum	Swiss	Regular	Hangul	16 x 32	40 %
Dotum	Swiss	Regular	Turkish	16 x 32	40 %
Dotum	Swiss	Regular	Western	16 x 32	40 %
DotumChe	Modern	Regular	Baltic	16 x 32	40 %
DotumChe	Modern	Regular	Central European	16 x 32	40 %
DotumChe	Modern	Regular	Cyrillic	16 x 32	40 %
DotumChe	Modern	Regular	Greek	16 x 32	40 %
DotumChe	Modern	Regular	Hangul	16 x 32	40 %
DotumChe	Modern	Regular	Turkish	16 x 32	40 %
DotumChe	Modern	Regular	Western	16 x 32	40 %
Ebrima	Special	Regular	Baltic	19 x 43	40 %
Ebrima	Special	Regular	Central European	19 x 43	40 %
Ebrima	Special	Regular	Turkish	19 x 43	40 %

Ebrima	Special	Regular	Western	19 x 43	40 %
Edwardian Script ITC	Script	Regular	Western	8 x 38	40 %
Elephant	Roman	Regular	Western	16 x 41	40 %
Engravers MT	Roman	Regular	Western	25 x 37	50 %
Eras Bold ITC	Swiss	Regular	Western	16 x 37	40 %
Eras Demi ITC	Swiss	Regular	Western	15 x 36	40 %
Eras Light ITC	Swiss	Regular	Western	13 x 36	40 %
Eras Medium ITC	Swiss	Regular	Western	14 x 36	40 %
Estrangelo Edessa	Script	Regular	Western	16 x 36	40 %
EucrosiaUPC	Roman	Regular	Thai	9 x 39	40 %
EucrosiaUPC	Roman	Regular	Western	9 x 39	40 %
Euphemia	Swiss	Regular	Western	22 x 42	40 %
FangSong	Modern	Regular	CHINESE_GB2312	16 x 32	40 %
FangSong	Modern	Regular	Western	16 x 32	40 %
Felix Titling	Decorative	Regular	Western	19 x 37	40 %
Fixedsys	Modern		Western	8 x 15	40 %
Footlight MT Light	Roman	Regular	Western	13 x 34	30 %
Forte	Script	Regular	Western	14 x 35	40 %
Franklin Gothic Book	Swiss	Regular	Baltic	13 x 36	40 %
Franklin Gothic Book	Swiss	Regular	Central European	13 x 36	40 %
Franklin Gothic Book	Swiss	Regular	Cyrillic	13 x 36	40 %
Franklin Gothic Book	Swiss	Regular	Greek	13 x 36	40 %
Franklin Gothic Book	Swiss	Regular	Turkish	13 x 36	40 %
Franklin Gothic Book	Swiss	Regular	Western	13 x 36	40 %
Franklin Gothic Demi Cond	Swiss	Regular	Baltic	12 x 36	40 %
Franklin Gothic Demi Cond	Swiss	Regular	Central European	12 x 36	40 %
Franklin Gothic Demi Cond	Swiss	Regular	Cyrillic	12 x 36	40 %
Franklin Gothic Demi Cond	Swiss	Regular	Greek	12 x 36	40 %
Franklin Gothic Demi Cond	Swiss	Regular	Turkish	12 x 36	40 %
Franklin Gothic Demi Cond	Swiss	Regular	Western	12 x 36	40 %
Franklin Gothic Demi	Swiss	Regular	Baltic	14 x 36	40 %
Franklin Gothic Demi	Swiss	Regular	Central European	14 x 36	40 %
Franklin Gothic Demi	Swiss	Regular	Cyrillic	14 x 36	40 %
Franklin Gothic Demi	Swiss	Regular	Greek	14 x 36	40 %
Franklin Gothic Demi	Swiss	Regular	Turkish	14 x 36	40 %
Franklin Gothic Demi	Swiss	Regular	Western	14 x 36	40 %
Franklin Gothic Heavy	Swiss	Regular	Baltic	15 x 36	40 %
Franklin Gothic Heavy	Swiss	Regular	Central European	15 x 36	40 %
Franklin Gothic Heavy	Swiss	Regular	Cyrillic	15 x 36	40 %
Franklin Gothic Heavy	Swiss	Regular	Greek	15 x 36	40 %
Franklin Gothic Heavy	Swiss	Regular	Turkish	15 x 36	40 %
Franklin Gothic Heavy	Swiss	Regular	Western	15 x 36	40 %
Franklin Gothic Medium Cond	Swiss	Regular	Baltic	12 x 36	40 %
Franklin Gothic Medium Cond	Swiss	Regular	Central European	12 x 36	40 %
Franklin Gothic Medium Cond	Swiss	Regular	Cyrillic	12 x 36	40 %
Franklin Gothic Medium Cond	Swiss	Regular	Greek	12 x 36	40 %
Franklin Gothic Medium Cond	Swiss	Regular	Turkish	12 x 36	40 %
Franklin Gothic Medium Cond	Swiss	Regular	Western	12 x 36	40 %
Franklin Gothic Medium	Swiss	Regular	Baltic	14 x 36	40 %
Franklin Gothic Medium	Swiss	Regular	Central European	14 x 36	40 %
Franklin Gothic Medium	Swiss	Regular	Cyrillic	14 x 36	40 %
Franklin Gothic Medium	Swiss	Regular	Greek	14 x 36	40 %
Franklin Gothic Medium	Swiss	Regular	Turkish	14 x 36	40 %
Franklin Gothic Medium	Swiss	Regular	Western	14 x 36	40 %

FrankRuehl	Swiss	Regular	Hebrew	13 x 30	40 %
FrankRuehl	Swiss	Regular	Western	13 x 30	40 %
FreesiaUPC	Swiss	Regular	Thai	9 x 38	40 %
FreesiaUPC	Swiss	Regular	Western	9 x 38	40 %
Freestyle Script	Script	Regular	Western	8 x 38	40 %
French Script MT	Script	Regular	Western	9 x 36	40 %
Gabriola	Decorative	Regular	Baltic	16 x 59	40 %
Gabriola	Decorative	Regular	Central European	16 x 59	40 %
Gabriola	Decorative	Regular	Cyrillic	16 x 59	40 %
Gabriola	Decorative	Regular	Greek	16 x 59	40 %
Gabriola	Decorative	Regular	Turkish	16 x 59	40 %
Gabriola	Decorative	Regular	Western	16 x 59	40 %
Gadugi	Swiss	Regular	Western	18 x 43	40 %
Garamond	Roman	Regular	Baltic	12 x 36	40 %
Garamond	Roman	Regular	Central European	12 x 36	40 %
Garamond	Roman	Regular	Cyrillic	12 x 36	40 %
Garamond	Roman	Regular	Greek	12 x 36	40 %
Garamond	Roman	Regular	Turkish	12 x 36	40 %
Garamond	Roman	Regular	Western	12 x 36	40 %
Gautami	Swiss	Regular	Western	18 x 56	40 %
Georgia	Roman	Regular	Baltic	14 x 36	40 %
Georgia	Roman	Regular	Central European	14 x 36	40 %
Georgia	Roman	Regular	Cyrillic	14 x 36	40 %
Georgia	Roman	Regular	Greek	14 x 36	40 %
Georgia	Roman	Regular	Turkish	14 x 36	40 %
Georgia	Roman	Regular	Western	14 x 36	40 %
Gigi	Decorative	Regular	Western	13 x 44	40 %
Gill Sans MT Condensed	Swiss	Regular	Central European	10 x 39	40 %
Gill Sans MT Condensed	Swiss	Regular	Western	10 x 39	40 %
Gill Sans MT Ext Condensed Bold	Swiss	Regular	Central European	7 x 38	40 %
Gill Sans MT Ext Condensed Bold	Swiss	Regular	Western	7 x 38	40 %
Gill Sans MT	Swiss	Regular	Central European	13 x 37	40 %
Gill Sans MT	Swiss	Regular	Western	13 x 37	40 %
Gill Sans Ultra Bold Condensed	Swiss	Regular	Central European	14 x 40	40 %
Gill Sans Ultra Bold Condensed	Swiss	Regular	Western	14 x 40	40 %
Gill Sans Ultra Bold	Swiss	Regular	Central European	20 x 40	40 %
Gill Sans Ultra Bold	Swiss	Regular	Western	20 x 40	40 %
Gisha	Swiss	Regular	Hebrew	16 x 38	40 %
Gisha	Swiss	Regular	Western	16 x 38	40 %
Gloucester MT Extra Condensed	Roman	Regular	Western	9 x 37	40 %
Goudy Old Style	Roman	Regular	Western	13 x 36	40 %
Goudy Stout	Roman	Regular	Western	36 x 44	40 %
Gulim	Swiss	Regular	Baltic	16 x 32	40 %
Gulim	Swiss	Regular	Central European	16 x 32	40 %
Gulim	Swiss	Regular	Cyrillic	16 x 32	40 %
Gulim	Swiss	Regular	Greek	16 x 32	40 %
Gulim	Swiss	Regular	Hangul	16 x 32	40 %
Gulim	Swiss	Regular	Turkish	16 x 32	40 %
Gulim	Swiss	Regular	Western	16 x 32	40 %
GulimChe	Modern	Regular	Baltic	16 x 32	40 %
GulimChe	Modern	Regular	Central European	16 x 32	40 %
GulimChe	Modern	Regular	Cyrillic	16 x 32	40 %
GulimChe	Modern	Regular	Greek	16 x 32	40 %
GulimChe	Modern	Regular	Hangul	16 x 32	40 %

GulimChe	Modern	Regular	Turkish	16 x 32	40 %
GulimChe	Modern	Regular	Western	16 x 32	40 %
Gungsuh	Roman	Regular	Baltic	16 x 32	40 %
Gungsuh	Roman	Regular	Central European	16 x 32	40 %
Gungsuh	Roman	Regular	Cyrillic	16 x 32	40 %
Gungsuh	Roman	Regular	Greek	16 x 32	40 %
Gungsuh	Roman	Regular	Hangul	16 x 32	40 %
Gungsuh	Roman	Regular	Turkish	16 x 32	40 %
Gungsuh	Roman	Regular	Western	16 x 32	40 %
GungsuhChe	Modern	Regular	Baltic	16 x 32	40 %
GungsuhChe	Modern	Regular	Central European	16 x 32	40 %
GungsuhChe	Modern	Regular	Cyrillic	16 x 32	40 %
GungsuhChe	Modern	Regular	Greek	16 x 32	40 %
GungsuhChe	Modern	Regular	Hangul	16 x 32	40 %
GungsuhChe	Modern	Regular	Turkish	16 x 32	40 %
GungsuhChe	Modern	Regular	Western	16 x 32	40 %
Haettenschweiler	Swiss	Regular	Baltic	10 x 33	40 %
Haettenschweiler	Swiss	Regular	Central European	10 x 33	40 %
Haettenschweiler	Swiss	Regular	Cyrillic	10 x 33	40 %
Haettenschweiler	Swiss	Regular	Greek	10 x 33	40 %
Haettenschweiler	Swiss	Regular	Turkish	10 x 33	40 %
Haettenschweiler	Swiss	Regular	Western	10 x 33	40 %
Harlow Solid Italic	Decorative	Italic	Western	12 x 40	40 %
Harrington	Decorative	Regular	Western	14 x 38	40 %
High Tower Text	Roman	Regular	Western	13 x 37	40 %
Impact	Swiss	Regular	Baltic	19 x 39	40 %
Impact	Swiss	Regular	Central European	19 x 39	40 %
Impact	Swiss	Regular	Cyrillic	19 x 39	40 %
Impact	Swiss	Regular	Greek	19 x 39	40 %
Impact	Swiss	Regular	Turkish	19 x 39	40 %
Impact	Swiss	Regular	Western	19 x 39	40 %
Imprint MT Shadow	Decorative	Regular	Western	13 x 38	40 %
Informal Roman	Script	Regular	Western	12 x 32	40 %
IrisUPC	Swiss	Regular	Thai	9 x 40	40 %
IrisUPC	Swiss	Regular	Western	9 x 40	40 %
Iskoola Pota	Swiss	Regular	Western	22 x 36	40 %
JasmineUPC	Roman	Regular	Thai	9 x 34	40 %
JasmineUPC	Roman	Regular	Western	9 x 34	40 %
Javanese Text	Special	Regular	Western	26 x 73	40 %
Jokerman	Decorative	Regular	Western	16 x 48	40 %
Juice ITC	Decorative	Regular	Western	9 x 36	40 %
KaiTi	Modern	Regular	CHINESE_GB2312	16 x 32	40 %
KaiTi	Modern	Regular	Western	16 x 32	40 %
Kalinga	Swiss	Regular	Western	19 x 48	40 %
Kartika	Roman	Regular	Western	27 x 46	40 %
Khmer UI	Swiss	Regular	Western	21 x 36	40 %
KodchiangUPC	Roman	Regular	Thai	9 x 31	40 %
KodchiangUPC	Roman	Regular	Western	9 x 31	40 %
Kokila	Swiss	Regular	Western	13 x 37	40 %
Kristen ITC	Script	Regular	Western	16 x 44	40 %
Kunstler Script	Script	Regular	Western	8 x 35	40 %
Lao UI	Swiss	Regular	Western	18 x 43	40 %
Latha	Swiss	Regular	Western	23 x 44	40 %
Leelawadee UI Semilight	Swiss	Regular	Thai	17 x 43	35 %

Leelawadee UI Semilight	Swiss	Regular	Vietnamese	17 x 43	35 %
Leelawadee UI Semilight	Swiss	Regular	Western	17 x 43	35 %
Leelawadee UI	Swiss	Regular	Thai	17 x 43	40 %
Leelawadee UI	Swiss	Regular	Vietnamese	17 x 43	40 %
Leelawadee UI	Swiss	Regular	Western	17 x 43	40 %
Leelawadee	Swiss	Regular	Thai	17 x 38	40 %
Leelawadee	Swiss	Regular	Western	17 x 38	40 %
Levenim MT	Special	Regular	Hebrew	16 x 42	40 %
Levenim MT	Special	Regular	Western	16 x 42	40 %
LilyUPC	Swiss	Regular	Thai	9 x 30	40 %
LilyUPC	Swiss	Regular	Western	9 x 30	40 %
Lucida Bright	Roman	Regular	Western	16 x 36	40 %
Lucida Calligraphy	Script	Italic	Western	17 x 40	40 %
Lucida Console	Modern	Regular	Central European	19 x 32	40 %
Lucida Console	Modern	Regular	Cyrillic	19 x 32	40 %
Lucida Console	Modern	Regular	Greek	19 x 32	40 %
Lucida Console	Modern	Regular	Turkish	19 x 32	40 %
Lucida Console	Modern	Regular	Western	19 x 32	40 %
Lucida Fax	Roman	Regular	Western	16 x 37	40 %
Lucida Handwriting	Script	Italic	Western	18 x 41	40 %
Lucida Sans Typewriter	Modern	Regular	Western	19 x 36	40 %
Lucida Sans Unicode	Swiss	Regular	Baltic	16 x 49	40 %
Lucida Sans Unicode	Swiss	Regular	Central European	16 x 49	40 %
Lucida Sans Unicode	Swiss	Regular	Cyrillic	16 x 49	40 %
Lucida Sans Unicode	Swiss	Regular	Greek	16 x 49	40 %
Lucida Sans Unicode	Swiss	Regular	Hebrew	16 x 49	40 %
Lucida Sans Unicode	Swiss	Regular	Turkish	16 x 49	40 %
Lucida Sans Unicode	Swiss	Regular	Western	16 x 49	40 %
Lucida Sans	Swiss	Regular	Western	16 x 36	40 %
Magneto	Decorative	Bold	Western	18 x 39	70 %
Maiandra GD	Swiss	Regular	Western	14 x 38	40 %
Malgun Gothic	Swiss	Regular	Hangul	15 x 43	40 %
Malgun Gothic	Swiss	Regular	Western	15 x 43	40 %
Mangal	Roman	Regular	Western	19 x 54	40 %
Marlett	Special	Regular	Symbol	31 x 32	50 %
Matura MT Script Capitals	Script	Regular	Western	14 x 43	40 %
Meiryo UI	Swiss	Regular	Baltic	17 x 41	40 %
Meiryo UI	Swiss	Regular	Central European	17 x 41	40 %
Meiryo UI	Swiss	Regular	Cyrillic	17 x 41	40 %
Meiryo UI	Swiss	Regular	Greek	17 x 41	40 %
Meiryo UI	Swiss	Regular	Japanese	17 x 41	40 %
Meiryo UI	Swiss	Regular	Turkish	17 x 41	40 %
Meiryo UI	Swiss	Regular	Western	17 x 41	40 %
Meiryo	Swiss	Regular	Baltic	31 x 48	40 %
Meiryo	Swiss	Regular	Central European	31 x 48	40 %
Meiryo	Swiss	Regular	Cyrillic	31 x 48	40 %
Meiryo	Swiss	Regular	Greek	31 x 48	40 %
Meiryo	Swiss	Regular	Japanese	31 x 48	40 %
Meiryo	Swiss	Regular	Turkish	31 x 48	40 %
Meiryo	Swiss	Regular	Western	31 x 48	40 %
Microsoft Himalaya	Special	Regular	Western	13 x 32	40 %
Microsoft JhengHei Light	Swiss	Regular	Baltic	32 x 43	29 %
Microsoft JhengHei Light	Swiss	Regular	Central European	32 x 43	29 %
Microsoft JhengHei Light	Swiss	Regular	CHINESE_BIG5	32 x 43	29 %

Microsoft JhengHei Light	Swiss	Regular	CHINESE_GB2312	32 x 43	29 %
Microsoft JhengHei Light	Swiss	Regular	Cyrillic	32 x 43	29 %
Microsoft JhengHei Light	Swiss	Regular	Greek	32 x 43	29 %
Microsoft JhengHei Light	Swiss	Regular	Hangul(Johab)	32 x 43	29 %
Microsoft JhengHei Light	Swiss	Regular	Hangul	32 x 43	29 %
Microsoft JhengHei Light	Swiss	Regular	Hebrew	32 x 43	29 %
Microsoft JhengHei Light	Swiss	Regular	Japanese	32 x 43	29 %
Microsoft JhengHei Light	Swiss	Regular	Turkish	32 x 43	29 %
Microsoft JhengHei Light	Swiss	Regular	Vietnamese	32 x 43	29 %
Microsoft JhengHei Light	Swiss	Regular	Western	32 x 43	29 %
Microsoft JhengHei UI Light	Swiss	Regular	Baltic	32 x 41	29 %
Microsoft JhengHei UI Light	Swiss	Regular	Central European	32 x 41	29 %
Microsoft JhengHei UI Light	Swiss	Regular	CHINESE_BIG5	32 x 41	29 %
Microsoft JhengHei UI Light	Swiss	Regular	CHINESE_GB2312	32 x 41	29 %
Microsoft JhengHei UI Light	Swiss	Regular	Cyrillic	32 x 41	29 %
Microsoft JhengHei UI Light	Swiss	Regular	Greek	32 x 41	29 %
Microsoft JhengHei UI Light	Swiss	Regular	Hangul(Johab)	32 x 41	29 %
Microsoft JhengHei UI Light	Swiss	Regular	Hangul	32 x 41	29 %
Microsoft JhengHei UI Light	Swiss	Regular	Hebrew	32 x 41	29 %
Microsoft JhengHei UI Light	Swiss	Regular	Japanese	32 x 41	29 %
Microsoft JhengHei UI Light	Swiss	Regular	Turkish	32 x 41	29 %
Microsoft JhengHei UI Light	Swiss	Regular	Vietnamese	32 x 41	29 %
Microsoft JhengHei UI Light	Swiss	Regular	Western	32 x 41	29 %
Microsoft JhengHei UI	Swiss	Regular	CHINESE_BIG5	15 x 41	40 %
Microsoft JhengHei UI	Swiss	Regular	Greek	15 x 41	40 %
Microsoft JhengHei UI	Swiss	Regular	Western	15 x 41	40 %
Microsoft JhengHei	Swiss	Regular	CHINESE_BIG5	15 x 43	40 %
Microsoft JhengHei	Swiss	Regular	Greek	15 x 43	40 %
Microsoft JhengHei	Swiss	Regular	Western	15 x 43	40 %
Microsoft New Tai Lue	Swiss	Regular	Western	19 x 42	40 %
Microsoft PhagsPa	Swiss	Regular	Western	24 x 41	40 %
Microsoft Sans Serif	Swiss	Regular	Arabic	14 x 36	40 %
Microsoft Sans Serif	Swiss	Regular	Baltic	14 x 36	40 %
Microsoft Sans Serif	Swiss	Regular	Central European	14 x 36	40 %
Microsoft Sans Serif	Swiss	Regular	Cyrillic	14 x 36	40 %
Microsoft Sans Serif	Swiss	Regular	Greek	14 x 36	40 %
Microsoft Sans Serif	Swiss	Regular	Hebrew	14 x 36	40 %
Microsoft Sans Serif	Swiss	Regular	Thai	14 x 36	40 %
Microsoft Sans Serif	Swiss	Regular	Turkish	14 x 36	40 %
Microsoft Sans Serif	Swiss	Regular	Vietnamese	14 x 36	40 %
Microsoft Sans Serif	Swiss	Regular	Western	14 x 36	40 %
Microsoft Tai Le	Swiss	Regular	Western	19 x 41	40 %
Microsoft Uighur	Special	Regular	Arabic	13 x 32	40 %
Microsoft Uighur	Special	Regular	Western	13 x 32	40 %
Microsoft YaHei Light	Swiss	Regular	Central European	15 x 41	29 %
Microsoft YaHei Light	Swiss	Regular	CHINESE_GB2312	15 x 41	29 %
Microsoft YaHei Light	Swiss	Regular	Cyrillic	15 x 41	29 %
Microsoft YaHei Light	Swiss	Regular	Greek	15 x 41	29 %
Microsoft YaHei Light	Swiss	Regular	Western	15 x 41	29 %
Microsoft YaHei UI Light	Swiss	Regular	Central European	15 x 42	29 %
Microsoft YaHei UI Light	Swiss	Regular	CHINESE_GB2312	15 x 42	29 %
Microsoft YaHei UI Light	Swiss	Regular	Cyrillic	15 x 42	29 %
Microsoft YaHei UI Light	Swiss	Regular	Greek	15 x 42	29 %
Microsoft YaHei UI Light	Swiss	Regular	Western	15 x 42	29 %

Microsoft YaHei UI	Swiss	Regular	Central European	15 x 41	40 %
Microsoft YaHei UI	Swiss	Regular	CHINESE_GB2312	15 x 41	40 %
Microsoft YaHei UI	Swiss	Regular	Cyrillic	15 x 41	40 %
Microsoft YaHei UI	Swiss	Regular	Greek	15 x 41	40 %
Microsoft YaHei UI	Swiss	Regular	Turkish	15 x 41	40 %
Microsoft YaHei UI	Swiss	Regular	Western	15 x 41	40 %
Microsoft YaHei	Swiss	Regular	Central European	15 x 42	40 %
Microsoft YaHei	Swiss	Regular	CHINESE_GB2312	15 x 42	40 %
Microsoft YaHei	Swiss	Regular	Cyrillic	15 x 42	40 %
Microsoft YaHei	Swiss	Regular	Greek	15 x 42	40 %
Microsoft YaHei	Swiss	Regular	Turkish	15 x 42	40 %
Microsoft YaHei	Swiss	Regular	Western	15 x 42	40 %
Microsoft Yi Baiti	Script	Regular	Western	21 x 32	40 %
MingLiU_HKSCS	Roman	Regular	CHINESE_BIG5	16 x 32	40 %
MingLiU_HKSCS	Roman	Regular	Western	16 x 32	40 %
MingLiU_HKSCS-ExtB	Roman	Regular	CHINESE_BIG5	16 x 32	40 %
MingLiU_HKSCS-ExtB	Roman	Regular	Western	16 x 32	40 %
MingLiU	Modern	Regular	CHINESE_BIG5	16 x 32	40 %
MingLiU	Modern	Regular	Western	16 x 32	40 %
MingLiU-ExtB	Roman	Regular	CHINESE_BIG5	16 x 32	40 %
MingLiU-ExtB	Roman	Regular	Western	16 x 32	40 %
Miriam Fixed	Modern	Regular	Hebrew	19 x 32	40 %
Miriam Fixed	Modern	Regular	Western	19 x 32	40 %
Miriam	Swiss	Regular	Hebrew	13 x 32	40 %
Miriam	Swiss	Regular	Western	13 x 32	40 %
Mistral	Script	Regular	Baltic	10 x 39	40 %
Mistral	Script	Regular	Central European	10 x 39	40 %
Mistral	Script	Regular	Cyrillic	10 x 39	40 %
Mistral	Script	Regular	Greek	10 x 39	40 %
Mistral	Script	Regular	Turkish	10 x 39	40 %
Mistral	Script	Regular	Western	10 x 39	40 %
Modern No. 20	Roman	Regular	Western	13 x 33	40 %
Modern	Modern		OEM/DOS	19 x 37	40 %
Mongolian Baiti	Script	Regular	Western	14 x 34	40 %
Monotype Corsiva	Script	Regular	Baltic	11 x 35	40 %
Monotype Corsiva	Script	Regular	Central European	11 x 35	40 %
Monotype Corsiva	Script	Regular	Cyrillic	11 x 35	40 %
Monotype Corsiva	Script	Regular	Greek	11 x 35	40 %
Monotype Corsiva	Script	Regular	Turkish	11 x 35	40 %
Monotype Corsiva	Script	Regular	Western	11 x 35	40 %
MoolBoran	Swiss	Regular	Western	13 x 43	40 %
MS Gothic	Modern	Regular	Baltic	16 x 32	40 %
MS Gothic	Modern	Regular	Central European	16 x 32	40 %
MS Gothic	Modern	Regular	Cyrillic	16 x 32	40 %
MS Gothic	Modern	Regular	Greek	16 x 32	40 %
MS Gothic	Modern	Regular	Japanese	16 x 32	40 %
MS Gothic	Modern	Regular	Turkish	16 x 32	40 %
MS Gothic	Modern	Regular	Western	16 x 32	40 %
MS Mincho	Modern	Regular	Baltic	16 x 32	40 %
MS Mincho	Modern	Regular	Central European	16 x 32	40 %
MS Mincho	Modern	Regular	Cyrillic	16 x 32	40 %
MS Mincho	Modern	Regular	Greek	16 x 32	40 %
MS Mincho	Modern	Regular	Japanese	16 x 32	40 %
MS Mincho	Modern	Regular	Turkish	16 x 32	40 %

MS Mincho	Modern	Regular	Western	16 x 32	40 %
MS Outlook	Special	Regular	Symbol	31 x 33	40 %
MS PGothic	Swiss	Regular	Baltic	13 x 32	40 %
MS PGothic	Swiss	Regular	Central European	13 x 32	40 %
MS PGothic	Swiss	Regular	Cyrillic	13 x 32	40 %
MS PGothic	Swiss	Regular	Greek	13 x 32	40 %
MS PGothic	Swiss	Regular	Japanese	13 x 32	40 %
MS PGothic	Swiss	Regular	Turkish	13 x 32	40 %
MS PGothic	Swiss	Regular	Western	13 x 32	40 %
MS PMincho	Roman	Regular	Baltic	13 x 32	40 %
MS PMincho	Roman	Regular	Central European	13 x 32	40 %
MS PMincho	Roman	Regular	Cyrillic	13 x 32	40 %
MS PMincho	Roman	Regular	Greek	13 x 32	40 %
MS PMincho	Roman	Regular	Japanese	13 x 32	40 %
MS PMincho	Roman	Regular	Turkish	13 x 32	40 %
MS PMincho	Roman	Regular	Western	13 x 32	40 %
MS Reference Sans Serif	Swiss	Regular	Baltic	16 x 39	40 %
MS Reference Sans Serif	Swiss	Regular	Central European	16 x 39	40 %
MS Reference Sans Serif	Swiss	Regular	Cyrillic	16 x 39	40 %
MS Reference Sans Serif	Swiss	Regular	Greek	16 x 39	40 %
MS Reference Sans Serif	Swiss	Regular	Turkish	16 x 39	40 %
MS Reference Sans Serif	Swiss	Regular	Vietnamese	16 x 39	40 %
MS Reference Sans Serif	Swiss	Regular	Western	16 x 39	40 %
MS Reference Specialty	Special	Regular	Symbol	23 x 39	40 %
MS Sans Serif	Swiss		Western	5 x 13	40 %
MS Serif	Roman		Western	5 x 13	40 %
MS UI Gothic	Swiss	Regular	Baltic	13 x 32	40 %
MS UI Gothic	Swiss	Regular	Central European	13 x 32	40 %
MS UI Gothic	Swiss	Regular	Cyrillic	13 x 32	40 %
MS UI Gothic	Swiss	Regular	Greek	13 x 32	40 %
MS UI Gothic	Swiss	Regular	Japanese	13 x 32	40 %
MS UI Gothic	Swiss	Regular	Turkish	13 x 32	40 %
MS UI Gothic	Swiss	Regular	Western	13 x 32	40 %
MT Extra	Roman	Regular	Symbol	20 x 32	40 %
MV Boli	Special	Regular	Western	18 x 52	40 %
Myanmar Text	Swiss	Regular	Western	18 x 60	40 %
Narkisim	Swiss	Regular	Hebrew	12 x 32	40 %
Narkisim	Swiss	Regular	Western	12 x 32	40 %
Niagara Engraved	Decorative	Regular	Western	8 x 34	40 %
Niagara Solid	Decorative	Regular	Western	8 x 34	40 %
Nirmala UI Semilight	Swiss	Regular	Western	17 x 43	35 %
Nirmala UI	Swiss	Regular	Western	31 x 43	40 %
NSimSun	Modern	Regular	CHINESE_GB2312	16 x 32	40 %
NSimSun	Modern	Regular	Western	16 x 32	40 %
Nyala	Special	Regular	Baltic	18 x 33	40 %
Nyala	Special	Regular	Central European	18 x 33	40 %
Nyala	Special	Regular	Turkish	18 x 33	40 %
Nyala	Special	Regular	Western	18 x 33	40 %
OCR A Extended	Modern	Regular	Western	19 x 33	40 %
Old English Text MT	Script	Regular	Western	12 x 39	40 %
Onyx	Decorative	Regular	Western	8 x 37	40 %
Palace Script MT	Script	Regular	Western	7 x 30	40 %
Palatino Linotype	Roman	Regular	Baltic	14 x 43	40 %
Palatino Linotype	Roman	Regular	Central European	14 x 43	40 %

Palatino Linotype	Roman	Regular	Cyrillic	14 x 43	40 %
Palatino Linotype	Roman	Regular	Greek	14 x 43	40 %
Palatino Linotype	Roman	Regular	Turkish	14 x 43	40 %
Palatino Linotype	Roman	Regular	Vietnamese	14 x 43	40 %
Palatino Linotype	Roman	Regular	Western	14 x 43	40 %
Papyrus	Script	Regular	Western	13 x 50	40 %
Parchment	Script	Regular	Western	6 x 34	40 %
Perpetua Titling MT	Roman	Light	Western	19 x 38	30 %
Perpetua	Roman	Regular	Western	12 x 37	40 %
Plantagenet Cherokee	Roman	Regular	Western	14 x 41	40 %
Playbill	Decorative	Regular	Western	8 x 32	40 %
PMingLiU	Roman	Regular	CHINESE_BIG5	16 x 32	40 %
PMingLiU	Roman	Regular	Western	16 x 32	40 %
PMingLiU-ExtB	Roman	Regular	CHINESE_BIG5	16 x 32	40 %
PMingLiU-ExtB	Roman	Regular	Western	16 x 32	40 %
Poor Richard	Roman	Regular	Western	12 x 36	40 %
Pristina	Script	Regular	Western	10 x 42	40 %
Raavi	Swiss	Regular	Western	13 x 53	40 %
Rage Italic	Script	Regular	Western	11 x 40	40 %
Ravie	Decorative	Regular	Western	22 x 43	40 %
Rockwell Condensed	Roman	Regular	Western	11 x 38	40 %
Rockwell Extra Bold	Roman	Regular	Western	19 x 38	80 %
Rockwell	Roman	Regular	Western	15 x 38	40 %
Rod	Modern	Regular	Hebrew	19 x 31	40 %
Rod	Modern	Regular	Western	19 x 31	40 %
Roman	Roman		OEM/DOS	22 x 37	40 %
Sakkal Majalla	Special	Regular	Arabic	16 x 45	40 %
Sakkal Majalla	Special	Regular	Baltic	16 x 45	40 %
Sakkal Majalla	Special	Regular	Central European	16 x 45	40 %
Sakkal Majalla	Special	Regular	Turkish	16 x 45	40 %
Sakkal Majalla	Special	Regular	Western	16 x 45	40 %
Script MT Bold	Script	Regular	Western	13 x 39	70 %
Script	Script		OEM/DOS	16 x 36	40 %
Segoe Print	Special	Regular	Baltic	21 x 56	40 %
Segoe Print	Special	Regular	Central European	21 x 56	40 %
Segoe Print	Special	Regular	Cyrillic	21 x 56	40 %
Segoe Print	Special	Regular	Greek	21 x 56	40 %
Segoe Print	Special	Regular	Turkish	21 x 56	40 %
Segoe Print	Special	Regular	Western	21 x 56	40 %
Segoe Script	Swiss	Regular	Baltic	22 x 51	40 %
Segoe Script	Swiss	Regular	Central European	22 x 51	40 %
Segoe Script	Swiss	Regular	Cyrillic	22 x 51	40 %
Segoe Script	Swiss	Regular	Greek	22 x 51	40 %
Segoe Script	Swiss	Regular	Turkish	22 x 51	40 %
Segoe Script	Swiss	Regular	Western	22 x 51	40 %
Segoe UI Black	Swiss	Regular	Baltic	20 x 43	90 %
Segoe UI Black	Swiss	Regular	Central European	20 x 43	90 %
Segoe UI Black	Swiss	Regular	Cyrillic	20 x 43	90 %
Segoe UI Black	Swiss	Regular	Greek	20 x 43	90 %
Segoe UI Black	Swiss	Regular	Turkish	20 x 43	90 %
Segoe UI Black	Swiss	Regular	Vietnamese	20 x 43	90 %
Segoe UI Black	Swiss	Regular	Western	20 x 43	90 %
Segoe UI Emoji	Swiss	Regular	Western	23 x 43	40 %
Segoe UI Light	Swiss	Regular	Arabic	17 x 43	30 %

Segoe UI Light	Swiss	Regular	Baltic	17 x 43	30 %
Segoe UI Light	Swiss	Regular	Central European	17 x 43	30 %
Segoe UI Light	Swiss	Regular	Cyrillic	17 x 43	30 %
Segoe UI Light	Swiss	Regular	Greek	17 x 43	30 %
Segoe UI Light	Swiss	Regular	Hebrew	17 x 43	30 %
Segoe UI Light	Swiss	Regular	Turkish	17 x 43	30 %
Segoe UI Light	Swiss	Regular	Vietnamese	17 x 43	30 %
Segoe UI Light	Swiss	Regular	Western	17 x 43	30 %
Segoe UI Semibold	Swiss	Regular	Arabic	18 x 43	60 %
Segoe UI Semibold	Swiss	Regular	Baltic	18 x 43	60 %
Segoe UI Semibold	Swiss	Regular	Central European	18 x 43	60 %
Segoe UI Semibold	Swiss	Regular	Cyrillic	18 x 43	60 %
Segoe UI Semibold	Swiss	Regular	Greek	18 x 43	60 %
Segoe UI Semibold	Swiss	Regular	Hebrew	18 x 43	60 %
Segoe UI Semibold	Swiss	Regular	Turkish	18 x 43	60 %
Segoe UI Semibold	Swiss	Regular	Vietnamese	18 x 43	60 %
Segoe UI Semibold	Swiss	Regular	Western	18 x 43	60 %
Segoe UI Semilight	Swiss	Regular	Arabic	17 x 43	35 %
Segoe UI Semilight	Swiss	Regular	Baltic	17 x 43	35 %
Segoe UI Semilight	Swiss	Regular	Central European	17 x 43	35 %
Segoe UI Semilight	Swiss	Regular	Cyrillic	17 x 43	35 %
Segoe UI Semilight	Swiss	Regular	Greek	17 x 43	35 %
Segoe UI Semilight	Swiss	Regular	Hebrew	17 x 43	35 %
Segoe UI Semilight	Swiss	Regular	Turkish	17 x 43	35 %
Segoe UI Semilight	Swiss	Regular	Vietnamese	17 x 43	35 %
Segoe UI Semilight	Swiss	Regular	Western	17 x 43	35 %
Segoe UI Symbol	Swiss	Regular	Western	23 x 43	40 %
Segoe UI	Swiss	Regular	Arabic	17 x 43	40 %
Segoe UI	Swiss	Regular	Baltic	17 x 43	40 %
Segoe UI	Swiss	Regular	Central European	17 x 43	40 %
Segoe UI	Swiss	Regular	Cyrillic	17 x 43	40 %
Segoe UI	Swiss	Regular	Greek	17 x 43	40 %
Segoe UI	Swiss	Regular	Hebrew	17 x 43	40 %
Segoe UI	Swiss	Regular	Turkish	17 x 43	40 %
Segoe UI	Swiss	Regular	Vietnamese	17 x 43	40 %
Segoe UI	Swiss	Regular	Western	17 x 43	40 %
Shonar Bangla	Swiss	Regular	Western	16 x 41	40 %
Showcard Gothic	Decorative	Regular	Western	18 x 40	40 %
Shruti	Swiss	Regular	Western	14 x 54	40 %
SimHei	Modern	Regular	CHINESE_GB2312	16 x 32	40 %
SimHei	Modern	Regular	Western	16 x 32	40 %
Simplified Arabic Fixed	Modern	Regular	Arabic	19 x 35	40 %
Simplified Arabic Fixed	Modern	Regular	Western	19 x 35	40 %
Simplified Arabic	Roman	Regular	Arabic	13 x 53	40 %
Simplified Arabic	Roman	Regular	Western	13 x 53	40 %
SimSun	Special	Regular	CHINESE_GB2312	16 x 32	40 %
SimSun	Special	Regular	Western	16 x 32	40 %
SimSun-ExtB	Modern	Regular	CHINESE_GB2312	16 x 32	40 %
SimSun-ExtB	Modern	Regular	Western	16 x 32	40 %
Sitka Banner	Special	Regular	Baltic	16 x 46	40 %
Sitka Banner	Special	Regular	Central European	16 x 46	40 %
Sitka Banner	Special	Regular	Cyrillic	16 x 46	40 %
Sitka Banner	Special	Regular	Greek	16 x 46	40 %
Sitka Banner	Special	Regular	Turkish	16 x 46	40 %

Sitka Banner	Special	Regular	Vietnamese	16 x 46	40 %
Sitka Banner	Special	Regular	Western	16 x 46	40 %
Sitka Display	Special	Regular	Baltic	17 x 46	40 %
Sitka Display	Special	Regular	Central European	17 x 46	40 %
Sitka Display	Special	Regular	Cyrillic	17 x 46	40 %
Sitka Display	Special	Regular	Greek	17 x 46	40 %
Sitka Display	Special	Regular	Turkish	17 x 46	40 %
Sitka Display	Special	Regular	Vietnamese	17 x 46	40 %
Sitka Display	Special	Regular	Western	17 x 46	40 %
Sitka Heading	Special	Regular	Baltic	17 x 46	40 %
Sitka Heading	Special	Regular	Central European	17 x 46	40 %
Sitka Heading	Special	Regular	Cyrillic	17 x 46	40 %
Sitka Heading	Special	Regular	Greek	17 x 46	40 %
Sitka Heading	Special	Regular	Turkish	17 x 46	40 %
Sitka Heading	Special	Regular	Vietnamese	17 x 46	40 %
Sitka Heading	Special	Regular	Western	17 x 46	40 %
Sitka Small	Special	Regular	Baltic	21 x 47	40 %
Sitka Small	Special	Regular	Central European	21 x 47	40 %
Sitka Small	Special	Regular	Cyrillic	21 x 47	40 %
Sitka Small	Special	Regular	Greek	21 x 47	40 %
Sitka Small	Special	Regular	Turkish	21 x 47	40 %
Sitka Small	Special	Regular	Vietnamese	21 x 47	40 %
Sitka Small	Special	Regular	Western	21 x 47	40 %
Sitka Subheading	Special	Regular	Baltic	18 x 46	40 %
Sitka Subheading	Special	Regular	Central European	18 x 46	40 %
Sitka Subheading	Special	Regular	Cyrillic	18 x 46	40 %
Sitka Subheading	Special	Regular	Greek	18 x 46	40 %
Sitka Subheading	Special	Regular	Turkish	18 x 46	40 %
Sitka Subheading	Special	Regular	Vietnamese	18 x 46	40 %
Sitka Subheading	Special	Regular	Western	18 x 46	40 %
Sitka Text	Special	Regular	Baltic	19 x 46	40 %
Sitka Text	Special	Regular	Central European	19 x 46	40 %
Sitka Text	Special	Regular	Cyrillic	19 x 46	40 %
Sitka Text	Special	Regular	Greek	19 x 46	40 %
Sitka Text	Special	Regular	Turkish	19 x 46	40 %
Sitka Text	Special	Regular	Vietnamese	19 x 46	40 %
Sitka Text	Special	Regular	Western	19 x 46	40 %
Small Fonts	Swiss		Western	1 x 3	40 %
Snap ITC	Decorative	Regular	Western	19 x 41	40 %
Stencil	Decorative	Regular	Western	18 x 38	40 %
Sylfaen	Roman	Regular	Baltic	13 x 42	40 %
Sylfaen	Roman	Regular	Central European	13 x 42	40 %
Sylfaen	Roman	Regular	Cyrillic	13 x 42	40 %
Sylfaen	Roman	Regular	Greek	13 x 42	40 %
Sylfaen	Roman	Regular	Turkish	13 x 42	40 %
Sylfaen	Roman	Regular	Western	13 x 42	40 %
Symbol	Roman	Regular	Symbol	19 x 39	40 %
System	Swiss		Western	7 x 16	70 %
Tahoma	Swiss	Regular	Arabic	14 x 39	40 %
Tahoma	Swiss	Regular	Baltic	14 x 39	40 %
Tahoma	Swiss	Regular	Central European	14 x 39	40 %
Tahoma	Swiss	Regular	Cyrillic	14 x 39	40 %
Tahoma	Swiss	Regular	Greek	14 x 39	40 %
Tahoma	Swiss	Regular	Hebrew	14 x 39	40 %

Tahoma	Swiss	Regular	Thai	14 x 39	40 %
Tahoma	Swiss	Regular	Turkish	14 x 39	40 %
Tahoma	Swiss	Regular	Vietnamese	14 x 39	40 %
Tahoma	Swiss	Regular	Western	14 x 39	40 %
Tempus Sans ITC	Decorative	Regular	Western	13 x 42	40 %
Terminal	Modern		OEM/DOS	8 x 12	40 %
Times New Roman	Roman	Regular	Arabic	13 x 35	40 %
Times New Roman	Roman	Regular	Baltic	13 x 35	40 %
Times New Roman	Roman	Regular	Central European	13 x 35	40 %
Times New Roman	Roman	Regular	Cyrillic	13 x 35	40 %
Times New Roman	Roman	Regular	Greek	13 x 35	40 %
Times New Roman	Roman	Regular	Hebrew	13 x 35	40 %
Times New Roman	Roman	Regular	Turkish	13 x 35	40 %
Times New Roman	Roman	Regular	Vietnamese	13 x 35	40 %
Times New Roman	Roman	Regular	Western	13 x 35	40 %
Traditional Arabic	Roman	Regular	Arabic	15 x 48	40 %
Traditional Arabic	Roman	Regular	Western	15 x 48	40 %
Trebuchet MS	Swiss	Regular	Baltic	15 x 37	40 %
Trebuchet MS	Swiss	Regular	Central European	15 x 37	40 %
Trebuchet MS	Swiss	Regular	Cyrillic	15 x 37	40 %
Trebuchet MS	Swiss	Regular	Greek	15 x 37	40 %
Trebuchet MS	Swiss	Regular	Turkish	15 x 37	40 %
Trebuchet MS	Swiss	Regular	Western	15 x 37	40 %
Tunga	Swiss	Regular	Western	18 x 53	40 %
Tw Cen MT Condensed Extra Bold	Swiss	Regular	Central European	12 x 35	40 %
Tw Cen MT Condensed Extra Bold	Swiss	Regular	Western	12 x 35	40 %
Tw Cen MT Condensed	Swiss	Regular	Central European	10 x 34	40 %
Tw Cen MT Condensed	Swiss	Regular	Western	10 x 34	40 %
Tw Cen MT	Swiss	Regular	Central European	13 x 35	40 %
Tw Cen MT	Swiss	Regular	Western	13 x 35	40 %
Urdu Typesetting	Script	Regular	Arabic	13 x 55	40 %
Urdu Typesetting	Script	Regular	Western	13 x 55	40 %
Utsaah	Swiss	Regular	Western	13 x 36	40 %
Vani	Swiss	Regular	Western	23 x 54	40 %
Verdana	Swiss	Regular	Baltic	16 x 39	40 %
Verdana	Swiss	Regular	Central European	16 x 39	40 %
Verdana	Swiss	Regular	Cyrillic	16 x 39	40 %
Verdana	Swiss	Regular	Greek	16 x 39	40 %
Verdana	Swiss	Regular	Turkish	16 x 39	40 %
Verdana	Swiss	Regular	Vietnamese	16 x 39	40 %
Verdana	Swiss	Regular	Western	16 x 39	40 %
Vijaya	Swiss	Regular	Western	19 x 32	40 %
Viner Hand ITC	Script	Regular	Western	15 x 52	40 %
Vivaldi	Script	Italic	Western	9 x 38	40 %
Vladimir Script	Script	Regular	Western	10 x 39	40 %
Vrinda	Swiss	Regular	Western	20 x 44	40 %
Webdings	Roman	Regular	Symbol	31 x 32	40 %
Wide Latin	Roman	Regular	Western	26 x 39	40 %
Wingdings 2	Roman	Regular	Symbol	27 x 34	40 %
Wingdings 3	Roman	Regular	Symbol	25 x 36	40 %
Wingdings	Special	Regular	Symbol	28 x 36	40 %
Yu Gothic Light	Swiss	Regular	Baltic	31 x 41	30 %
Yu Gothic Light	Swiss	Regular	Central European	31 x 41	30 %
Yu Gothic Light	Swiss	Regular	Cyrillic	31 x 41	30 %

Yu Gothic Light	Swiss	Regular	Greek	31 x 41	30 %
Yu Gothic Light	Swiss	Regular	Japanese	31 x 41	30 %
Yu Gothic Light	Swiss	Regular	Turkish	31 x 41	30 %
Yu Gothic Light	Swiss	Regular	Western	31 x 41	30 %
Yu Gothic	Swiss	Regular	Baltic	31 x 41	40 %
Yu Gothic	Swiss	Regular	Central European	31 x 41	40 %
Yu Gothic	Swiss	Regular	Cyrillic	31 x 41	40 %
Yu Gothic	Swiss	Regular	Greek	31 x 41	40 %
Yu Gothic	Swiss	Regular	Japanese	31 x 41	40 %
Yu Gothic	Swiss	Regular	Turkish	31 x 41	40 %
Yu Gothic	Swiss	Regular	Western	31 x 41	40 %
Yu Mincho Demibold	Roman	Bold	Baltic	31 x 41	60 %
Yu Mincho Demibold	Roman	Bold	Central European	31 x 41	60 %
Yu Mincho Demibold	Roman	Bold	Cyrillic	31 x 41	60 %
Yu Mincho Demibold	Roman	Bold	Greek	31 x 41	60 %
Yu Mincho Demibold	Roman	Bold	Japanese	31 x 41	60 %
Yu Mincho Demibold	Roman	Bold	Turkish	31 x 41	60 %
Yu Mincho Demibold	Roman	Bold	Western	31 x 41	60 %
Yu Mincho Light	Roman	Regular	Baltic	31 x 41	30 %
Yu Mincho Light	Roman	Regular	Central European	31 x 41	30 %
Yu Mincho Light	Roman	Regular	Cyrillic	31 x 41	30 %
Yu Mincho Light	Roman	Regular	Greek	31 x 41	30 %
Yu Mincho Light	Roman	Regular	Japanese	31 x 41	30 %
Yu Mincho Light	Roman	Regular	Turkish	31 x 41	30 %
Yu Mincho Light	Roman	Regular	Western	31 x 41	30 %
Yu Mincho	Roman	Regular	Baltic	31 x 41	40 %
Yu Mincho	Roman	Regular	Central European	31 x 41	40 %
Yu Mincho	Roman	Regular	Cyrillic	31 x 41	40 %
Yu Mincho	Roman	Regular	Greek	31 x 41	40 %
Yu Mincho	Roman	Regular	Japanese	31 x 41	40 %
Yu Mincho	Roman	Regular	Turkish	31 x 41	40 %
Yu Mincho	Roman	Regular	Western	31 x 41	40 %

Windows Audio

Device	Identifier	Device Description
midi-out.0	0001 001B	Microsoft GS Wavetable Synth
mixer.0	0001 FFFF	Speakers (2- High Definition Au
mixer.1	0001 FFFF	Microphone (2- High Definition
wave-in.0	0001 FFFF	Microphone (2- High Definition
wave-out.0	0001 FFFF	Speakers (2- High Definition Au

PCI / PnP Audio

Device Description	Type
Intel Panther Point HDMI @ Intel Panther Point PCH - High Definition Audio Controller [C-1]	PCI
Realtek ALC269 @ Intel Panther Point PCH - High Definition Audio Controller [C-1]	PCI

HD Audio

[Intel Panther Point PCH - High Definition Audio Controller [C-1]]

Device Properties:

Device Description	Intel Panther Point PCH - High Definition Audio Controller [C-1]
Device Description (Windows)	High Definition Audio Controller
Bus Type	PCI
Bus / Device / Function	0 / 27 / 0
Device ID	8086-1E20
Subsystem ID	1025-0649
Revision	04
Hardware ID	PCI\VEN_8086&DEV_1E20&SUBSYS_06491025&REV_04

Device Manufacturer:

Company Name	Intel Corporation
Product Information	http://www.intel.com/products/chipsets
Driver Download	http://support.intel.com/support/chipsets
BIOS Upgrades	http://www.aida64.com/bios-updates
Driver Update	http://www.aida64.com/driver-updates

[Realtek ALC269]

Device Properties:

Device Description	Realtek ALC269
Device Description (Windows)	High Definition Audio Device
Device Type	Audio
Bus Type	HDAUDIO
Device ID	10EC-0269
Subsystem ID	1025-0649
Revision	1001
Hardware ID	HDAUDIO\FUNC_01&VEN_10EC&DEV_0269&SUBSYS_10250649&REV_1001

Device Manufacturer:

Company Name	Realtek Semiconductor Corp.
Product Information	http://www.realtek.com.tw/products/productsView.aspx?Langid=1&PNid=8&PFid=14&Level=3&Conn=2
Driver Download	http://www.realtek.com.tw/downloads
Driver Update	http://www.aida64.com/driver-updates

[Intel Panther Point HDMI]

Device Properties:

Device Description	Intel Panther Point HDMI
Device Description (Windows)	High Definition Audio Device
Device Type	Audio
Bus Type	HDAUDIO
Device ID	8086-2806
Subsystem ID	8086-0101
Revision	1000
Hardware ID	HDAUDIO\FUNC_01&VEN_8086&DEV_2806&SUBSYS_80860101&REV_1000

Device Manufacturer:

Company Name	Intel Corporation
Product Information	http://www.intel.com/products/chipsets
Driver Download	http://support.intel.com/support/chipsets
Driver Update	http://www.aida64.com/driver-updates

Audio Codecs

[Fraunhofer IIS MPEG Layer-3 Codec (decode only)]

ACM Driver Properties:

Driver Description	Fraunhofer IIS MPEG Layer-3 Codec (decode only)
Copyright Notice	Copyright © 1996-1999 Fraunhofer Institut Integrierte Schaltungen IIS
Driver Features	decoder only version
Driver Version	1.09

[Microsoft ADPCM CODEC]

ACM Driver Properties:

Driver Description	Microsoft ADPCM CODEC
Copyright Notice	Copyright (C) 1992-1996 Microsoft Corporation
Driver Features	Compresses and decompresses Microsoft ADPCM audio data.
Driver Version	4.00

[Microsoft CCITT G.711 A-Law and u-Law CODEC]

ACM Driver Properties:

Driver Description	Microsoft CCITT G.711 A-Law and u-Law CODEC
Copyright Notice	Copyright (c) 1993-1996 Microsoft Corporation
Driver Features	Compresses and decompresses CCITT G.711 A-Law and u-Law audio data.
Driver Version	4.00

[Microsoft GSM 6.10 Audio CODEC]

ACM Driver Properties:

Driver Description	Microsoft GSM 6.10 Audio CODEC
Copyright Notice	Copyright (C) 1993-1996 Microsoft Corporation
Driver Features	Compresses and decompresses audio data conforming to the ETSI-GSM (European Telecommunications Standards Institute-Groupe Special Mobile) recommendation 6.10.
Driver Version	4.00

[Microsoft IMA ADPCM CODEC]

ACM Driver Properties:

Driver Description	Microsoft IMA ADPCM CODEC
Copyright Notice	Copyright (C) 1992-1996 Microsoft Corporation
Driver Features	Compresses and decompresses IMA ADPCM audio data.
Driver Version	4.00

[Microsoft PCM Converter]

ACM Driver Properties:

Driver Description	Microsoft PCM Converter
Copyright Notice	Copyright (C) 1992-1996 Microsoft Corporation
Driver Features	Converts frequency and bits per sample of PCM audio data.
Driver Version	5.00

Video Codecs

Driver	Version	Description
iccvid.dll	1.10.0.11	Cinepak® Codec
iyuv_32.dll	6.3.9600.16384 (winblue_rtm.130821-1623)	Intel Indeo(R) Video YUV Codec
msrle32.dll	6.3.9600.16384 (winblue_rtm.130821-1623)	Microsoft RLE Compressor
msvidc32.dll	6.3.9600.16384 (winblue_rtm.130821-1623)	Microsoft Video 1 Compressor
msyuv.dll	6.3.9600.17415 (winblue_r4.141028-1500)	Microsoft UYVY Video Decompressor
tsbyuv.dll	6.3.9600.17415 (winblue_r4.141028-1500)	Toshiba Video Codec

MCI

[AVIVideo]

MCI Device Properties:

Device	AVIVideo
Name	Video for Windows
Description	Video For Windows MCI driver
Type	Digital Video Device
Driver	mciavi32.dll
Status	Enabled

MCI Device Features:

Compound Device	Yes
File Based Device	Yes
Can Eject	No
Can Play	Yes
Can Play In Reverse	Yes
Can Record	No
Can Save Data	No
Can Freeze Data	No
Can Lock Data	No
Can Stretch Frame	Yes
Can Stretch Input	No
Can Test	Yes
Audio Capable	Yes
Video Capable	Yes
Still Image Capable	No

[CDAudio]

MCI Device Properties:

Device	CDAudio
Name	CD Audio

Description	MCI driver for cdaudio devices
Type	CD Audio Device
Driver	mcicda.dll
Status	Enabled

MCI Device Features:

Compound Device	No
File Based Device	No
Can Eject	Yes
Can Play	Yes
Can Record	No
Can Save Data	No
Audio Capable	Yes
Video Capable	No

[MPEGVideo]

MCI Device Properties:

Device	MPEGVideo
Name	DirectShow
Description	DirectShow MCI Driver
Type	Digital Video Device
Driver	mciqtz32.dll
Status	Enabled

MCI Device Features:

Compound Device	Yes
File Based Device	Yes
Can Eject	No
Can Play	Yes
Can Play In Reverse	No
Can Record	No
Can Save Data	No
Can Freeze Data	No
Can Lock Data	No
Can Stretch Frame	Yes
Can Stretch Input	No
Can Test	Yes
Audio Capable	Yes
Video Capable	Yes
Still Image Capable	No

[Sequencer]

MCI Device Properties:

Device	Sequencer
Name	MIDI Sequencer
Description	MCI driver for MIDI sequencer
Type	Sequencer Device
Driver	mciseq.dll
Status	Enabled

MCI Device Features:

Compound Device	Yes
File Based Device	Yes
Can Eject	No
Can Play	Yes
Can Record	No
Can Save Data	No
Audio Capable	Yes
Video Capable	No

[WaveAudio]

MCI Device Properties:

Device	WaveAudio
Name	Sound
Description	MCI driver for waveform audio
Type	Waveform Audio Device
Driver	mciwave.dll
Status	Enabled

MCI Device Features:

Compound Device	Yes
File Based Device	Yes
Can Eject	No
Can Play	Yes
Can Record	Yes
Can Save Data	Yes
Audio Capable	Yes
Video Capable	No

SAPI

SAPI Properties:

SAPI4 Version	-
SAPI5 Version	5.3.17828.0

Voice (SAPI5):

Name	Microsoft David Desktop - English (United States)
Voice Path	C:\Windows\Speech\Engines\TTS\en-US\M1033DAV
Age	Adult
Gender	Male
Language	English (United States)
Vendor	Microsoft
Version	11.0
DLL File	C:\Windows\SysWOW64\speech\engines\tts\MSTTSEngine.dll (x86)
CLSID	{C64501F6-E6E6-451f-A150-25D0839BC510}

Voice (SAPI5):

Name	Microsoft Hazel Desktop - English (Great Britain)
Voice Path	C:\Windows\Speech\Engines\TTS\en-GB\M2057HAZ
Age	Adult
Gender	Female

Language	English (United Kingdom)
Vendor	Microsoft
Version	11.0
DLL File	C:\Windows\SysWOW64\speech\engines\tts\MSTTSEngine.dll (x86)
CLSID	{C64501F6-E6E6-451f-A150-25D0839BC510}

Voice (SAPI5):

Name	Microsoft Zira Desktop - English (United States)
Voice Path	C:\Windows\Speech\Engines\TTS\en-US\M1033ZIR
Age	Adult
Gender	Female
Language	English (United States)
Vendor	Microsoft
Version	11.0
DLL File	C:\Windows\SysWOW64\speech\engines\tts\MSTTSEngine.dll (x86)
CLSID	{C64501F6-E6E6-451f-A150-25D0839BC510}

Speech Recognizer (SAPI5):

Name	Microsoft Speech Recognizer 8.0 for Windows (English - US)
Description	Microsoft Speech Recognizer 8.0 for Windows (English - US)
FE Config Data File	C:\Windows\Speech\Engines\SR\en-US\c1033dsk.fe
Language	English (United States); English
Speaking Style	Discrete;Continuous
Supported Locales	English (United States); English (Canada); English (Philippines); English
Vendor	Microsoft
Version	8.0
DLL File	C:\Windows\System32\Speech\Engines\SR\spsreng.dll (x64)
CLSID	{DAC9F469-0C67-4643-9258-87EC128C5941}
RecoExtension	{4F4DB904-CA35-4A3A-90AF-C9D8BE7532AC}

Windows Storage

[OCZ-AGILITY4]

Device Properties:

Driver Description	OCZ-AGILITY4
Driver Date	6/21/2006
Driver Version	6.3.9600.16384
Driver Provider	Microsoft
INF File	disk.inf

SSD Physical Info:

Manufacturer	OCZ
SSD Family	Agility 4
Form Factor	2.5"
Controller Type	Indilinx Everest 2
Flash Memory Type	Intel 25nm MLC NAND
Physical Dimensions	99.8 x 69.63 x 9.3 mm
Max. Weight	101 g
Interface	SATA-III
Interface Data Rate	600 MB/s

Device Manufacturer:

Company Name	OCZ Technology Group, Inc.
Product Information	http://www.ocztechnology.com/products/solid_state_drives

[MATSHITA DVD-RAM UJ8C0]

Device Properties:

Driver Description	MATSHITA DVD-RAM UJ8C0
Driver Date	6/21/2006
Driver Version	6.3.9600.16384
Driver Provider	Microsoft
INF File	cdrom.inf

Device Manufacturer:

Company Name	Matsushita Electric Industrial Co., Ltd.
Product Information	http://www.panasonic.com/industrial/optical-drives
Firmware Download	http://www.panasonic.com/industrial/optical-drives

[Intel(R) 7 Series/C216 Chipset Family SATA AHCI Controller - 1E03]

Device Properties:

Driver Description	Intel(R) 7 Series/C216 Chipset Family SATA AHCI Controller - 1E03
Driver Date	7/25/2013
Driver Version	9.3.0.1029
Driver Provider	Intel
INF File	oem7.inf

Device Resources:

IRQ	19
Memory	C0606000-C06067FF
Port	2060-207F
Port	2080-2087
Port	2088-208F
Port	2090-2093
Port	2094-2097

[Microsoft Storage Spaces Controller]

Device Properties:

Driver Description	Microsoft Storage Spaces Controller
Driver Date	6/21/2006
Driver Version	6.3.9600.17415
Driver Provider	Microsoft
INF File	spaceport.inf

Logical Drives

Drive	Drive Type	File System	Total Size	Used Space	Free Space	% Free	Volume Serial
B:	Local Disk						
C: (Windows)	Local Disk	NTFS	283582 MB	50539 MB	233043 MB	82 %	CA6E-6344

D: Optical Drive

Physical Drives

[Drive #1 - OCZ-AGILITY4 (476 GB)]

Partition	Partition Type	Drive	Start Offset	Partition Length
#1 (Active)	NTFS	C: (Windows)	1 MB	283583 MB
#2	NTFS		283584 MB	204800 MB

Optical Drives

[D:\ MATSHITA DVD-RAM UJ8C0]

Optical Drive Properties:

Device Description	MATSHITA DVD-RAM UJ8C0
Serial Number	YN53 045898
Firmware Revision	1.00
Buffer Size	768 KB
Region Code	1
Remaining User Changes	4
Remaining Vendor Changes	4

Supported Disk Types:

BD-ROM	Not Supported
BD-R	Not Supported
BD-RE	Not Supported
HD DVD-ROM	Not Supported
HD DVD-R Dual Layer	Not Supported
HD DVD-RW Dual Layer	Not Supported
HD DVD-R	Not Supported
HD DVD-RW	Not Supported
HD DVD-RAM	Not Supported
DVD-ROM	Read
DVD+R9 Dual Layer	Read + Write
DVD+RW9 Dual Layer	Not Supported
DVD+R	Read + Write
DVD+RW	Read + Write
DVD-R9 Dual Layer	Read + Write
DVD-RW9 Dual Layer	Not Supported
DVD-R	Read + Write
DVD-RW	Read + Write
DVD-RAM	Read + Write
CD-ROM	Read
CD-R	Read + Write
CD-RW	Read + Write

Optical Drive Features:

AACS	Not Supported

BD CPS	Not Supported
Buffer Underrun Protection	Supported
C2 Error Pointers	Supported
CD+G	Not Supported
CD-Text	Supported
DVD-Download Disc Recording	Not Supported
Hybrid Disc	Not Supported
JustLink	Not Supported
CPRM	Supported
CSS	Supported
LabelFlash	Not Supported
Layer-Jump Recording	Supported
LightScribe	Not Supported
Mount Rainier	Not Supported
OSSC	Not Supported
Qflix Recording	Not Supported
SecurDisc	Not Supported
SMART	Supported
VCPS	Not Supported

ASPI

Host	ID	LUN	Device Type	Vendor	Model	Rev	Extra Information
00	00	00	Disk Drive		OCZ-AGILITY4		
00	00	00	Optical Drive	MATSHITA	DVD-RAM UJ8C0	1.00	
00	07	00	Host Adapter	storahci			

ATA

[OCZ-AGILITY4 (OCZ-3C9Y4Q3483TV35R2)]

ATA Device Properties:

Model ID	OCZ-AGILITY4
Serial Number	OCZ-3C9Y4Q3483TV35R2
Revision	1.5.2
World Wide Name	5-E83A97-10A59EBF3
Device Type	SATA-III
Parameters	992277 cylinders, 16 heads, 63 sectors per track, 512 bytes per sector
LBA Sectors	1000215216
Physical / Logical Sector Size	512 bytes / 512 bytes
Buffer	32767 KB
Multiple Sectors	16
Max. PIO Transfer Mode	PIO 4
Max. MWDMA Transfer Mode	MWDMA 2
Max. UDMA Transfer Mode	UDMA 6
Active UDMA Transfer Mode	UDMA 6
Unformatted Capacity	488386 MB
Rotational Speed	SSD
ATA Standard	ACS-2

ATA Device Features:

48-bit LBA	Supported, Enabled
Automatic Acoustic Management (AAM)	Not Supported
Device Configuration Overlay (DCO)	Not Supported
DMA Setup Auto-Activate	Supported, Enabled
Free-Fall Control	Not Supported
General Purpose Logging (GPL)	Supported, Enabled
Hardware Feature Control	Not Supported
Host Protected Area (HPA)	Supported, Enabled
HPA Security Extensions	Not Supported
Hybrid Information Feature	Not Supported
In-Order Data Delivery	Supported, Enabled
Native Command Queuing (NCQ)	Supported
NCQ Autosense	Not Supported
NCQ Priority Information	Not Supported
NCQ Queue Management Command	Not Supported
NCQ Streaming	Not Supported
Phy Event Counters	Not Supported
Read Look-Ahead	Not Supported
Release Interrupt	Not Supported
Security Mode	Supported, Disabled
Sense Data Reporting (SDR)	Not Supported
Service Interrupt	Not Supported
SMART	Supported, Enabled
SMART Error Logging	Not Supported
SMART Self-Test	Not Supported
Software Settings Preservation (SSP)	Not Supported
Streaming	Not Supported
Tagged Command Queuing (TCQ)	Not Supported
Write Cache	Supported, Enabled
Write-Read-Verify	Supported, Enabled

SSD Features:

Data Set Management	Supported
Deterministic Read After TRIM	Not Supported
TRIM Command	Supported

Power Management Features:

Advanced Power Management	Not Supported
Automatic Partial to Slumber Transitions (APST)	Disabled
Device Initiated Interface Power Management (DIPM)	Not Supported
Device Sleep (DEVSLP)	Not Supported
Extended Power Conditions (EPC)	Not Supported
Host Initiated Interface Power Management (HIPM)	Not Supported
IDLE IMMEDIATE With UNLOAD FEATURE	Not Supported
Link Power State Device Sleep	Not Supported
Power Management	Supported, Enabled
Power-Up In Standby (PUIS)	Not Supported

ATA Commands:

DEVICE RESET	Not Supported
DOWNLOAD MICROCODE	Supported, Enabled
FLUSH CACHE	Supported, Enabled

FLUSH CACHE EXT	Not Supported
NOP	Supported, Enabled
READ BUFFER	Supported, Enabled
WRITE BUFFER	Supported, Enabled

ATA Device Physical Info:

Manufacturer	OCZ
SSD Family	Agility 4
Form Factor	2.5"
Formatted Capacity	512 GB
Controller Type	Indilinx Everest 2
Flash Memory Type	Intel 25nm MLC NAND
Physical Dimensions	99.8 x 69.63 x 9.3 mm
Max. Weight	101 g
Max. Sequential Read Speed	400 MB/s
Max. Sequential Write Speed	400 MB/s
Max. Random 4 KB Read	48000 IOPS
Max. Random 4 KB Write	85000 IOPS
Interface	SATA-III
Interface Data Rate	600 MB/s

ATA Device Manufacturer:

Company Name	OCZ Technology Group, Inc.
Product Information	http://www.ocztechnology.com/products/solid_state_drives
Driver Update	http://www.aida64.com/driver-updates

SMART

[OCZ-AGILITY4 (OCZ-3C9Y4Q3483TV35R2)]

ID	Attribute Description	Threshold	Value	Worst	Data	Status
01	Raw Read Error Rate	0	6	0	6	OK: Always passes
03	Spinup Time	0	100	100	0	OK: Always passes
04	Start/Stop Count	0	100	100	0	OK: Always passes
05	Reallocated Sector Count	0	100	100	2	OK: Always passes
09	Power-On Hours Count	0	100	100	10863	OK: Always passes
0C	Power Cycle Count	0	100	100	1005	OK: Always passes
E8	Total Count of Write Sectors	0	100	100	2339742359	OK: Always passes
E9	Remaining Drive Life	0	99	0	99	OK: Always passes

Windows Network

[Bluetooth Device (Personal Area Network)]

Network Adapter Properties:

Network Adapter	Bluetooth Device (Personal Area Network)
Interface Type	Bluetooth Ethernet

Hardware Address	00-1B-10-00-2A-EC
Connection Name	Bluetooth Network Connection
Connection Speed	3 Mbps
MTU	1500 bytes
Bytes Received	0
Bytes Sent	0

[Broadcom NetLink (TM) Gigabit Ethernet]

Network Adapter Properties:

Network Adapter	Broadcom NetLink (TM) Gigabit Ethernet
Interface Type	Gigabit Ethernet
Hardware Address	DC-0E-A1-B4-F1-90
Connection Name	Ethernet
MTU	1500 bytes
Bytes Received	0
Bytes Sent	0

Network Adapter Manufacturer:

Company Name	Broadcom Corporation
Product Information	http://www.broadcom.com/products
Driver Download	http://www.broadcom.com/support/ethernet_nic
Driver Update	http://www.aida64.com/driver-updates

[Intel(R) Dual Band Wireless-AC 7260]

Network Adapter Properties:

Network Adapter	Intel(R) Dual Band Wireless-AC 7260
Interface Type	802.11 Wireless Ethernet
Hardware Address	D8-FC-93-E4-C0-EB
Connection Name	Wi-Fi 3
Connection Speed	650 Mbps
MTU	1500 bytes
DHCP Lease Obtained	4/29/2015 11:34:28 AM
DHCP Lease Expires	4/30/2015 11:34:28 AM
Bytes Received	26238315 (25.0 MB)
Bytes Sent	543076 (530.3 KB)

Network Adapter Addresses:

IP / Subnet Mask	192.168.1.109 / 255.255.255.0
Gateway	192.168.1.1
DHCP	192.168.1.1
DNS	192.168.1.1

Network Adapter Manufacturer:

Company Name	Intel Corporation
Product Information	http://www.intel.com/embedded
Driver Download	http://www.intel.com/support/network
Driver Update	http://www.aida64.com/driver-updates

[Microsoft Wi-Fi Direct Virtual Adapter #4]

Network Adapter Properties:

Network Adapter	Microsoft Wi-Fi Direct Virtual Adapter #4
Interface Type	802.11 Wireless Ethernet
Hardware Address	D8-FC-93-E4-C0-EC
Connection Name	Local Area Connection* 7
MTU	1500 bytes
Bytes Received	0
Bytes Sent	0

PCI / PnP Network

Device Description	Type
Broadcom NetLink BCM57785 PCI-E Gigabit Ethernet Controller	PCI
Intel Dual Band Wireless-AC 7260 AC 2x2 HMC WiFi Adapter	PCI

IAM

[Microsoft Communities]

Account Properties:

Account Name	Microsoft Communities
Account ID	account{9CF1CE86-F6F4-46D9-848E-024250173232}.oeaccount
Account Type	News (Default)
Application Name	Microsoft Windows Mail
Connection Name	Not Specified (IE Default)
NNTP Server	msnews.microsoft.com

Account Features:

NNTP Prompt For Password	No
NNTP Secure Authentication	No
NNTP Secure Connection	No
NNTP Use Group Descriptions	No
NNTP Post Using Plain Text Format	No
NNTP Post Using HTML Format	No

[Active Directory]

Account Properties:

Account Name	Active Directory
Account ID	account{621776FD-2E84-4AFF-88BB-EA0A12623C25}.oeaccount
Account Type	LDAP
Application Name	Microsoft Windows Mail
Connection Name	Not Specified (IE Default)
LDAP Server	NULL:3268
LDAP User Name	NULL
LDAP Search Base	NULL
LDAP Search Timeout	1 min

Account Features:

LDAP Authentication Required	Yes

LDAP Secure Authentication	Yes
LDAP Secure Connection	No
LDAP Simple Search Filter	No

[VeriSign Internet Directory Service]

Account Properties:

Account Name	VeriSign Internet Directory Service
Account ID	account{6D721CDD-D594-4058-8672-97F3A14A5827}.oeaccount
Account Type	LDAP
Application Name	Microsoft Windows Mail
Connection Name	Not Specified (IE Default)
LDAP Server	directory.verisign.com
LDAP URL	http://www.verisign.com
LDAP Search Base	NULL
LDAP Search Timeout	1 min

Account Features:

LDAP Authentication Required	No
LDAP Secure Authentication	No
LDAP Secure Connection	No
LDAP Simple Search Filter	Yes

Internet

Internet Settings:

Start Page	google.com
Search Page	http://go.microsoft.com/fwlink/?LinkId=54896
Local Page	C:\Windows\system32\blank.htm
Download Folder	

Current Proxy:

Proxy Status	Disabled

LAN Proxy:

Proxy Status	Disabled

Routes

Type	Net Destination	Netmask	Gateway	Metric	Interface
Active	0.0.0.0	0.0.0.0	192.168.1.1	10	192.168.1.109 (Intel(R) Dual Band Wireless-AC 7260)
Active	127.0.0.0	255.0.0.0	127.0.0.1	306	127.0.0.1 (Software Loopback Interface 1)
Active	127.0.0.1	255.255.255.255	127.0.0.1	306	127.0.0.1 (Software Loopback Interface 1)
Active	127.255.255.255	255.255.255.255	127.0.0.1	306	127.0.0.1 (Software Loopback Interface 1)
Active	192.168.1.0	255.255.255.0	192.168.1.109	266	192.168.1.109 (Intel(R) Dual Band Wireless-AC 7260)
Active	192.168.1.109	255.255.255.255	192.168.1.109	266	192.168.1.109 (Intel(R) Dual Band Wireless-AC 7260)
Active	192.168.1.255	255.255.255.255	192.168.1.109	266	192.168.1.109 (Intel(R) Dual Band Wireless-AC 7260)
Active	224.0.0.0	240.0.0.0	127.0.0.1	306	127.0.0.1 (Software Loopback Interface 1)
Active	224.0.0.0	240.0.0.0	192.168.1.109	266	192.168.1.109 (Intel(R) Dual Band Wireless-AC 7260)

Active	255.255.255.255	255.255.255.255	127.0.0.1	306	127.0.0.1 (Software Loopback Interface 1)
Active	255.255.255.255	255.255.255.255	192.168.1.109	266	192.168.1.109 (Intel(R) Dual Band Wireless-AC 7260)

IE Cookie

Last Access	URL
2015-04-26 08:56:45	liem@hwinfo.com/

Browser History

Last Access	URL
2015-04-26 13:29:33	Liem@http://google.com/
2015-04-26 13:29:33	Liem@http://www.google.com/
2015-04-26 13:29:34	Liem@https://www.google.com/?gws_rd=ssl
2015-04-26 13:29:42	Liem@https://www.bios-mods.com/forum/member.php?action=register
2015-04-26 13:31:29	Liem@https://www.bios-mods.com/forum/member.php?action=activate
2015-04-26 13:31:43	Liem@https://www.bios-mods.com/forum/member.php

DirectX Files

Name	Version	Type	Language	Size	Date
amstream.dll	6.06.9600.17415	Final Retail	English	80384	4/11/2015 9:49:52 AM
bdaplgin.ax	6.03.9600.17415	Final Retail	English	80896	4/11/2015 9:50:34 AM
d2d1.dll	6.03.9600.17415	Final Retail	English	4067840	4/11/2015 9:49:48 AM
d3d10.dll	6.03.9600.17415	Final Retail	English	1065472	4/11/2015 9:49:48 AM
d3d10_1.dll	6.03.9600.17415	Final Retail	English	161792	4/11/2015 9:49:48 AM
d3d10_1core.dll	6.03.9600.17415	Final Retail	English	352768	4/11/2015 9:49:48 AM
d3d10core.dll	6.03.9600.17415	Final Retail	English	316928	4/11/2015 9:49:48 AM
d3d10level9.dll	6.03.9600.17415	Final Retail	English	616704	4/11/2015 9:49:48 AM
d3d10warp.dll	6.03.9600.17415	Final Retail	English	2174976	4/11/2015 9:49:48 AM
d3d11.dll	6.03.9600.17415	Final Retail	English	1946144	4/11/2015 9:49:48 AM
d3d8.dll	6.03.9600.17415	Final Retail	English	1065984	4/11/2015 9:49:47 AM
d3d8thk.dll	6.03.9600.17415	Final Retail	English	12288	4/11/2015 9:49:48 AM
d3d9.dll	6.03.9600.17415	Final Retail	English	1907384	4/11/2015 9:49:48 AM
d3dim.dll	6.03.9600.17415	Final Retail	English	401408	4/11/2015 9:49:47 AM
d3dim700.dll	6.03.9600.17415	Final Retail	English	887808	4/11/2015 9:49:47 AM
d3dramp.dll	6.03.9600.17415	Final Retail	English	594944	4/11/2015 9:49:47 AM
d3dxof.dll	6.03.9600.17415	Final Retail	English	58368	4/11/2015 9:49:47 AM
ddraw.dll	6.03.9600.17415	Final Retail	English	544256	4/11/2015 9:49:47 AM
ddrawex.dll	6.03.9600.17415	Final Retail	English	43008	4/11/2015 9:49:47 AM
devenum.dll	6.06.9600.17415	Final Retail	English	81008	4/11/2015 9:49:52 AM
dinput.dll	6.03.9600.17415	Final Retail	English	136192	4/11/2015 9:50:34 AM
dinput8.dll	6.03.9600.17415	Final Retail	English	171520	4/11/2015 9:50:34 AM
dmband.dll	6.03.9600.17415	Final Retail	English	34304	4/11/2015 9:49:50 AM
dmcompos.dll	6.03.9600.17415	Final Retail	English	75776	4/11/2015 9:49:50 AM
dmime.dll	6.03.9600.17415	Final Retail	English	207360	4/11/2015 9:49:50 AM
dmloader.dll	6.03.9600.17415	Final Retail	English	41472	4/11/2015 9:49:50 AM

dmscript.dll	6.03.9600.17415	Final Retail	English	95744	4/11/2015 9:49:50 AM
dmstyle.dll	6.03.9600.17415	Final Retail	English	122368	4/11/2015 9:49:50 AM
dmsynth.dll	6.03.9600.17415	Final Retail	English	109568	4/11/2015 9:49:50 AM
dmusic.dll	6.03.9600.17415	Final Retail	English	111104	4/11/2015 9:49:50 AM
dplaysvr.exe	6.03.9600.16384	Final Retail	English	8192	8/21/2013 9:05:19 PM
dplayx.dll	6.03.9600.16384	Final Retail	English	8192	8/21/2013 9:05:19 PM
dpmodemx.dll	6.03.9600.16384	Final Retail	English	8192	8/21/2013 9:05:19 PM
dpnaddr.dll	6.03.9600.16384	Final Retail	English	8192	8/21/2013 9:05:19 PM
dpnathlp.dll	6.03.9600.16384	Final Retail	English	8192	8/21/2013 9:05:20 PM
dpnet.dll	6.03.9600.16384	Final Retail	English	8192	8/21/2013 9:05:19 PM
dpnhpast.dll	6.03.9600.16384	Final Retail	English	8192	8/21/2013 9:05:19 PM
dpnhupnp.dll	6.03.9600.16384	Final Retail	English	8192	8/21/2013 9:05:19 PM
dpnlobby.dll	6.03.9600.16384	Final Retail	English	8192	8/21/2013 9:05:19 PM
dpnsvr.exe	6.03.9600.16384	Final Retail	English	8192	8/21/2013 9:05:19 PM
dpwsockx.dll	6.03.9600.16384	Final Retail	English	8192	8/21/2013 9:05:19 PM
dsdmo.dll	6.03.9600.17415	Final Retail	English	182784	4/11/2015 9:49:53 AM
dsound.dll	6.03.9600.17415	Final Retail	English	517120	4/11/2015 9:49:53 AM
dswave.dll	6.03.9600.17415	Final Retail	English	23040	4/11/2015 9:49:50 AM
dwrite.dll	6.03.9600.17415	Final Retail	English	1560576	4/11/2015 9:49:48 AM
dxdiagn.dll	6.03.9600.17415	Final Retail	English	264192	4/11/2015 9:49:47 AM
dxgi.dll	6.03.9600.17415	Final Retail	English	430176	4/11/2015 9:49:48 AM
dxmasf.dll	12.00.9600.17415	Final Retail	English	4608	4/11/2015 9:50:28 AM
dxtmsft.dll	11.00.9600.17631	Final Retail	English	418304	1/11/2015 6:45:52 PM
dxtrans.dll	11.00.9600.17690	Final Retail	English	285696	2/20/2015 5:27:56 PM
dxva2.dll	6.03.9600.17415	Final Retail	English	116696	4/11/2015 9:49:48 AM
encapi.dll	6.03.9600.17415	Final Retail	English	20992	4/11/2015 9:49:52 AM
gcdef.dll	6.03.9600.17415	Final Retail	English	123392	4/11/2015 9:50:34 AM
iac25_32.ax	2.00.0005.0053	Final Retail	English	197632	8/21/2013 6:43:11 PM
ir41_32.ax	6.03.9600.17415	Final Retail	English	8704	4/11/2015 9:49:50 AM
ir41_qc.dll	6.03.9600.17415	Final Retail	English	8192	4/11/2015 9:49:50 AM
ir41_qcx.dll	6.03.9600.17415	Final Retail	English	8192	4/11/2015 9:49:50 AM
ir50_32.dll	6.03.9600.17415	Final Retail	English	8704	4/11/2015 9:49:50 AM
ir50_qc.dll	6.03.9600.17415	Final Retail	English	8192	4/11/2015 9:49:50 AM
ir50_qcx.dll	6.03.9600.17415	Final Retail	English	8192	4/11/2015 9:49:50 AM
ivfsrc.ax	5.10.0002.0051	Final Retail	English	146944	8/21/2013 6:43:11 PM
joy.cpl	6.03.9600.17415	Final Retail	English	136704	4/11/2015 9:50:34 AM
ksproxy.ax	6.03.9600.17415	Final Retail	English	245760	4/11/2015 9:49:52 AM
kstvtune.ax	6.03.9600.17415	Final Retail	English	95232	4/11/2015 9:50:34 AM
ksuser.dll	6.03.9600.17415	Final Retail	English	19096	4/11/2015 9:49:52 AM
kswdmcap.ax	6.03.9600.17415	Final Retail	English	116224	4/11/2015 9:49:52 AM
ksxbar.ax	6.03.9600.17415	Final Retail	English	58880	4/11/2015 9:50:34 AM
mciqtz32.dll	6.06.9600.17415	Final Retail	English	38912	4/11/2015 9:49:52 AM
mfc40.dll	4.01.0000.6140	Final Retail	English	924944	8/21/2013 4:35:15 PM
mfc42.dll	6.06.8063.0000	Beta Retail	English	1204224	1/29/2015 6:42:37 PM
mpeg2data.ax	6.06.9600.17415	Final Retail	English	85504	4/11/2015 9:50:34 AM
mpg2splt.ax	6.06.9600.17415	Final Retail	English	233984	4/11/2015 9:50:31 AM
msdmo.dll	6.06.9600.17415	Final Retail	English	39720	4/11/2015 9:49:52 AM
msdvbnp.ax	6.06.9600.17415	Final Retail	English	71680	4/11/2015 9:50:34 AM
msvidctl.dll	6.05.9600.17415	Final Retail	English	2410496	4/11/2015 9:50:34 AM
msyuv.dll	6.03.9600.17415	Final Retail	English	23040	4/11/2015 9:49:52 AM
pid.dll	6.03.9600.17415	Final Retail	English	37376	4/11/2015 9:50:34 AM
psisdecd.dll	6.06.9600.17415	Final Retail	English	512512	4/11/2015 9:50:34 AM
psisrndr.ax	6.06.9600.17415	Final Retail	English	93696	4/11/2015 9:50:34 AM
qasf.dll	12.00.9600.17415	Final Retail	English	229376	4/11/2015 9:50:34 AM

qcap.dll	6.06.9600.16384	Final Retail	English	179200	8/21/2013 8:50:04 PM
qdv.dll	6.06.9600.17415	Final Retail	English	293376	4/11/2015 9:49:52 AM
qdvd.dll	6.06.9600.17415	Final Retail	English	519680	4/11/2015 9:49:52 AM
qedit.dll	6.06.9600.17415	Final Retail	English	561664	4/11/2015 9:49:50 AM
qedwipes.dll	6.06.9600.16384	Final Retail	English	733184	8/21/2013 9:16:59 PM
quartz.dll	6.06.9600.17415	Final Retail	English	1500672	4/11/2015 9:49:53 AM
vbisurf.ax	6.03.9600.17415	Final Retail	English	40960	4/11/2015 9:50:34 AM
vfwwdm32.dll	6.03.9600.17415	Final Retail	English	57344	4/11/2015 9:49:52 AM
wsock32.dll	6.03.9600.17415	Final Retail	English	16384	4/11/2015 9:50:20 AM

DirectX Video

[Primary Display Driver]

DirectDraw Device Properties:

DirectDraw Driver Name	display
DirectDraw Driver Description	Primary Display Driver
Hardware Driver	igdumdim32.dll (10.18.10.3958)
Hardware Description	Intel(R) HD Graphics 4000

Direct3D Device Properties:

Rendering Bit Depths	8, 16, 32
Z-Buffer Bit Depths	16, 24, 32
Multisample Anti-Aliasing Modes	MSAA 2x, MSAA 4x, MSAA 8x
Min Texture Size	1 x 1
Max Texture Size	8192 x 8192
Unified Shader Version	5.0
DirectX Hardware Support	DirectX v11.0

Direct3D Device Features:

Additive Texture Blending	Supported
AGP Texturing	Not Supported
Anisotropic Filtering	Supported
Automatic Mipmap Generation	Supported
Bilinear Filtering	Supported
Compute Shader	Supported
Cubic Environment Mapping	Supported
Cubic Filtering	Not Supported
Decal-Alpha Texture Blending	Supported
Decal Texture Blending	Supported
Directional Lights	Supported
DirectX Texture Compression	Not Supported
DirectX Volumetric Texture Compression	Not Supported
Dithering	Supported
Dot3 Texture Blending	Supported
Double-Precision Floating-Point	Supported
Driver Concurrent Creates	Supported
Driver Command Lists	Not Supported
Dynamic Textures	Supported
Edge Anti-Aliasing	Not Supported
Environmental Bump Mapping	Supported

Environmental Bump Mapping + Luminance	Supported
Factor Alpha Blending	Supported
Geometric Hidden-Surface Removal	Not Supported
Geometry Shader	Supported
Guard Band	Supported
Hardware Scene Rasterization	Supported
Hardware Transform & Lighting	Supported
Legacy Depth Bias	Supported
Map On Default Buffers	Supported
Mipmap LOD Bias Adjustments	Supported
Mipmapped Cube Textures	Supported
Mipmapped Volume Textures	Supported
Modulate-Alpha Texture Blending	Supported
Modulate Texture Blending	Supported
Non-Square Textures	Supported
N-Patches	Not Supported
Perspective Texture Correction	Supported
Point Lights	Supported
Point Sampling	Supported
Projective Textures	Supported
Quintic Bezier Curves & B-Splines	Not Supported
Range-Based Fog	Supported
Rectangular & Triangular Patches	Not Supported
Rendering In Windowed Mode	Supported
Runtime Shader Linking	Supported
Scissor Test	Supported
Slope-Scale Based Depth Bias	Supported
Specular Flat Shading	Supported
Specular Gouraud Shading	Supported
Specular Phong Shading	Not Supported
Spherical Mapping	Supported
Spot Lights	Supported
Stencil Buffers	Supported
Sub-Pixel Accuracy	Supported
Subtractive Texture Blending	Supported
Table Fog	Supported
Texture Alpha Blending	Supported
Texture Clamping	Supported
Texture Mirroring	Supported
Texture Transparency	Supported
Texture Wrapping	Supported
Tiled Resources	Not Supported
Triangle Culling	Not Supported
Trilinear Filtering	Supported
Two-Sided Stencil Test	Supported
Vertex Alpha Blending	Supported
Vertex Fog	Supported
Vertex Tweening	Supported
Volume Textures	Supported
W-Based Fog	Supported
W-Buffering	Not Supported
Z-Based Fog	Supported
Z-Bias	Supported
Z-Test	Supported

Supported FourCC Codes:

AI44	Supported
AYUV	Supported
I420	Supported
IA44	Supported
IMC1	Supported
IMC2	Supported
IMC3	Supported
IMC4	Supported
IYUV	Supported
NV11	Supported
NV12	Supported
P208	Supported
UYVY	Supported
VYUY	Supported
YUY2	Supported
YV12	Supported
YVU9	Supported
YVYU	Supported

Video Adapter Manufacturer:

Company Name	Intel Corporation
Product Information	http://www.intel.com/products/chipsets
Driver Download	http://support.intel.com/support/graphics
Driver Update	http://www.aida64.com/driver-updates

DirectX Sound

[Primary Sound Driver]

DirectSound Device Properties:

Device Description	Primary Sound Driver
Driver Module	
Primary Buffers	1
Min / Max Secondary Buffers Sample Rate	100 / 200000 Hz
Primary Buffers Sound Formats	8-bit, 16-bit, Mono, Stereo
Secondary Buffers Sound Formats	8-bit, 16-bit, Mono, Stereo
Total / Free Sound Buffers	1 / 0
Total / Free Static Sound Buffers	1 / 0
Total / Free Streaming Sound Buffers	1 / 0
Total / Free 3D Sound Buffers	0 / 0
Total / Free 3D Static Sound Buffers	0 / 0
Total / Free 3D Streaming Sound Buffers	0 / 0

DirectSound Device Features:

Certified Driver	No
Emulated Device	No
Precise Sample Rate	Supported
DirectSound3D	Not Supported
Creative EAX 1.0	Not Supported

Creative EAX 2.0	Not Supported
Creative EAX 3.0	Not Supported
Creative EAX 4.0	Not Supported
Creative EAX 5.0	Not Supported
I3DL2	Not Supported
Sensaura ZoomFX	Not Supported

[Speakers (2- High Definition Audio Device)]

DirectSound Device Properties:

Device Description	Speakers (2- High Definition Audio Device)
Driver Module	{0.0.0.00000000}.{819410b2-d1eb-4014-ac4c-31359644fbb5}
Primary Buffers	1
Min / Max Secondary Buffers Sample Rate	100 / 200000 Hz
Primary Buffers Sound Formats	8-bit, 16-bit, Mono, Stereo
Secondary Buffers Sound Formats	8-bit, 16-bit, Mono, Stereo
Total / Free Sound Buffers	1 / 0
Total / Free Static Sound Buffers	1 / 0
Total / Free Streaming Sound Buffers	1 / 0
Total / Free 3D Sound Buffers	0 / 0
Total / Free 3D Static Sound Buffers	0 / 0
Total / Free 3D Streaming Sound Buffers	0 / 0

DirectSound Device Features:

Certified Driver	No
Emulated Device	No
Precise Sample Rate	Supported
DirectSound3D	Not Supported
Creative EAX 1.0	Not Supported
Creative EAX 2.0	Not Supported
Creative EAX 3.0	Not Supported
Creative EAX 4.0	Not Supported
Creative EAX 5.0	Not Supported
I3DL2	Not Supported
Sensaura ZoomFX	Not Supported

DirectX Input

[Mouse]

DirectInput Device Properties:

Device Description	Mouse
Device Type	Unknown
Device Subtype	Unknown
Axes	3
Buttons/Keys	8

DirectInput Device Features:

Emulated Device	Yes
Alias Device	No
Polled Device	No

Polled Data Format	No
Attack Force Feedback	Not Supported
Deadband Force Feedback	Not Supported
Fade Force Feedback	Not Supported
Force Feedback	Not Supported
Saturation Force Feedback	Not Supported
+/- Force Feedback Coefficients	Not Supported
+/- Force Feedback Saturation	Not Supported

[Keyboard]

DirectInput Device Properties:

Device Description	Keyboard
Device Type	Unknown
Device Subtype	Unknown
Buttons/Keys	128

DirectInput Device Features:

Emulated Device	Yes
Alias Device	No
Polled Device	No
Polled Data Format	No
Attack Force Feedback	Not Supported
Deadband Force Feedback	Not Supported
Fade Force Feedback	Not Supported
Force Feedback	Not Supported
Saturation Force Feedback	Not Supported
+/- Force Feedback Coefficients	Not Supported
+/- Force Feedback Saturation	Not Supported

Windows Devices

[Devices]

Audio inputs and outputs:

Microphone (2- High Definition Audio Device)	6.3.9600.16384
Speakers (2- High Definition Audio Device)	6.3.9600.16384

Batteries:

Microsoft AC Adapter	6.3.9600.16384
Microsoft ACPI-Compliant Control Method Battery	6.3.9600.16384

Bluetooth Auxiliary:

Bluetooth Server	17.1.1501.510
Phonebook Access Profile (PSE)	17.1.1501.510

Bluetooth:

Audio Source Service	6.3.9600.17673
AV Remote Target Service	6.3.9600.17673
Galaxy Note 4	6.3.9600.17673
Generic Bluetooth Radio	6.3.9600.17673

Handsfree Audio Gateway Service	6.3.9600.17673
Headset Audio Gateway Service	6.3.9600.17673
HY-525-BT	6.3.9600.17673
Microsoft Bluetooth Enumerator	6.3.9600.17673
Object Push Service	6.3.9600.17673
Personal Area Network NAP Service	6.3.9600.17673

Computer:

ACPI x64-based PC	6.3.9600.16384

Disk drives:

OCZ-AGILITY4	6.3.9600.16384

Display adapters:

Intel(R) HD Graphics 4000	10.18.10.3958

DVD/CD-ROM drives:

MATSHITA DVD-RAM UJ8C0	6.3.9600.16384

Human Interface Devices:

Galaxy Note 4 Audio/Video Remote Control HID	6.3.9600.16384
HY-525-BT Audio/Video Remote Control HID	6.3.9600.16384
USB Input Device	6.3.9600.17041

IDE ATA/ATAPI controllers:

Intel(R) 7 Series/C216 Chipset Family SATA AHCI Controller - 1E03	9.3.0.1029

Imaging devices:

HD Webcam	6.3.9600.17217

Keyboards:

Standard PS/2 Keyboard	6.3.9600.17480

Mice and other pointing devices:

HID-compliant mouse	6.3.9600.17480
PS/2 Compatible Mouse	6.3.9600.17480

Monitors:

Generic PnP Monitor	6.3.9600.16384

Network adapters:

Bluetooth Device (Personal Area Network)	6.3.9600.17238
Bluetooth Device (RFCOMM Protocol TDI)	6.3.9600.17673
Broadcom NetLink (TM) Gigabit Ethernet	15.6.0.14
Intel(R) Dual Band Wireless-AC 7260	16.5.3.6
Microsoft Kernel Debug Network Adapter	6.3.9600.16384
Microsoft Wi-Fi Direct Virtual Adapter #4	6.3.9600.16384

Network Infrastructure Devices:

Community	1.0.0.2

Print queues:

Fax	6.3.9600.16384
Microsoft XPS Document Writer	6.3.9600.16384

Root Print Queue	6.3.9600.16384
Send To OneNote 2013	6.3.9600.16384

Processors:

Intel(R) Core(TM) i7-3520M CPU @ 2.90GHz	6.3.9600.16384
Intel(R) Core(TM) i7-3520M CPU @ 2.90GHz	6.3.9600.16384
Intel(R) Core(TM) i7-3520M CPU @ 2.90GHz	6.3.9600.16384
Intel(R) Core(TM) i7-3520M CPU @ 2.90GHz	6.3.9600.16384

Software devices:

LANDevice:1	6.3.9600.16384
Microsoft Device Association Root Enumerator	6.3.9600.16384
WANConnectionDevice:1	6.3.9600.16384
WANDevice:1	6.3.9600.16384

Sound, video and game controllers:

High Definition Audio Device	6.3.9600.16384
High Definition Audio Device	6.3.9600.16384
HY-525-BT Stereo	6.3.9600.17673

Storage controllers:

Microsoft Storage Spaces Controller	6.3.9600.17415

Storage volume shadow copies:

Generic volume shadow copy	6.3.9600.16384
Generic volume shadow copy	6.3.9600.16384
Generic volume shadow copy	6.3.9600.16384
Generic volume shadow copy	6.3.9600.16384

Storage volumes:

Generic volume	6.3.9600.17215
Generic volume	6.3.9600.17215

System devices:

3rd Gen Core processor DRAM Controller - 0154	6.3.9600.17238
ACPI Fixed Feature Button	6.3.9600.17238
ACPI Lid	6.3.9600.17238
ACPI Power Button	6.3.9600.17238
ACPI Sleep Button	6.3.9600.17238
Broadcom Memory Stick	1.0.8.0
Broadcom SD Host Controller	1.0.0.254
Composite Bus Enumerator	6.3.9600.16384
Direct memory access controller	6.3.9600.17238
High Definition Audio Controller	6.3.9600.17238
High precision event timer	6.3.9600.17238
Intel(R) 7 Series/C216 Chipset Family PCI Express Root Port 1 - 1E10	9.3.0.1029
Intel(R) 7 Series/C216 Chipset Family PCI Express Root Port 2 - 1E12	9.3.0.1029
Intel(R) 7 Series/C216 Chipset Family SMBus Host Controller - 1E22	9.3.0.1029
Intel(R) 82802 Firmware Hub Device	6.3.9600.17238
Intel(R) HM70 Express Chipset LPC Controller - 1E5E	9.3.0.1029
IWD Bus Enumerator	4.5.52.0
Microsoft ACPI-Compliant Embedded Controller	6.3.9600.17238
Microsoft ACPI-Compliant System	6.3.9600.17393
Microsoft Basic Display Driver	6.3.9600.16384

Microsoft Basic Render Driver	6.3.9600.17031
Microsoft System Management BIOS Driver	6.3.9600.16384
Microsoft Virtual Drive Enumerator	6.3.9600.16384
Microsoft Windows Management Interface for ACPI	6.3.9600.16384
Microsoft Windows Management Interface for ACPI	6.3.9600.16384
Motherboard resources	6.3.9600.17238
Motherboard resources	6.3.9600.17238
Motherboard resources	6.3.9600.17238
Motherboard resources	6.3.9600.17238
NDIS Virtual Network Adapter Enumerator	6.3.9600.16384
Numeric data processor	6.3.9600.17238
PCI Express Root Complex	6.3.9600.17238
Plug and Play Software Device Enumerator	6.3.9600.17415
Programmable interrupt controller	6.3.9600.17238
Remote Desktop Device Redirector Bus	6.3.9600.16384
System board	6.3.9600.17238
System CMOS/real time clock	6.3.9600.17238
System timer	6.3.9600.17238
UMBus Root Bus Enumerator	6.3.9600.16384
Volume Manager	6.3.9600.16384

Universal Serial Bus controllers:

Generic USB Hub	6.3.9600.17238
Generic USB Hub	6.3.9600.17238
Intel(R) 7 Series/C216 Chipset Family USB Enhanced Host Controller - 1E26	9.3.0.1030
Intel(R) 7 Series/C216 Chipset Family USB Enhanced Host Controller - 1E2D	9.3.0.1030
USB Composite Device	6.3.9600.17238
USB Root Hub	6.3.9600.17238
USB Root Hub	6.3.9600.17238

Unknown:

Base System Device
Bluetooth Peripheral Device
Bluetooth Peripheral Device
MAP SMS/MMS
PandoraLink
Unknown

[Audio inputs and outputs / Microphone (2- High Definition Audio Device)]

Device Properties:

Driver Description	Microphone (2- High Definition Audio Device)
Driver Date	8/22/2013
Driver Version	6.3.9600.16384
Driver Provider	Microsoft
INF File	AudioEndpoint.inf
Hardware ID	MMDEVAPI\AudioEndpoints

[Audio inputs and outputs / Speakers (2- High Definition Audio Device)]

Device Properties:

Driver Description	Speakers (2- High Definition Audio Device)
Driver Date	8/22/2013
Driver Version	6.3.9600.16384

Driver Provider	Microsoft
INF File	AudioEndpoint.inf
Hardware ID	MMDEVAPI\AudioEndpoints

[Batteries / Microsoft AC Adapter]

Device Properties:

Driver Description	Microsoft AC Adapter
Driver Date	6/21/2006
Driver Version	6.3.9600.16384
Driver Provider	Microsoft
INF File	cmbatt.inf
Hardware ID	ACPI\VEN_ACPI&DEV_0003

Device Manufacturer:

Driver Update	http://www.aida64.com/driver-updates

[Batteries / Microsoft ACPI-Compliant Control Method Battery]

Device Properties:

Driver Description	Microsoft ACPI-Compliant Control Method Battery
Driver Date	6/21/2006
Driver Version	6.3.9600.16384
Driver Provider	Microsoft
INF File	cmbatt.inf
Hardware ID	ACPI\VEN_PNP&DEV_0C0A

Device Manufacturer:

Driver Update	http://www.aida64.com/driver-updates

[Bluetooth Auxiliary / Bluetooth Server]

Device Properties:

Driver Description	Bluetooth Server
Driver Date	12/17/2014
Driver Version	17.1.1501.510
Driver Provider	Intel Corporation
INF File	oem61.inf
Hardware ID	BTHENUM\{f0b2dd71-fb14-4e30-a62d-931874bf282f}_LOCALMFG&0000

[Bluetooth Auxiliary / Phonebook Access Profile (PSE)]

Device Properties:

Driver Description	Phonebook Access Profile (PSE)
Driver Date	12/17/2014
Driver Version	17.1.1501.510
Driver Provider	Intel Corporation
INF File	oem61.inf
Hardware ID	BTHENUM\{0000112f-0000-1000-8000-00805f9b34fb}_VID&0001001d_PID&1200

[Bluetooth / Audio Source Service]

Device Properties:

Driver Description	Audio Source Service
Driver Date	6/21/2006
Driver Version	6.3.9600.17673
Driver Provider	Microsoft
INF File	bth.inf
Hardware ID	BTHENUM\{0000110a-0000-1000-8000-00805f9b34fb}_VID&0001001d_PID&1200

Device Manufacturer:

Driver Update	http://www.aida64.com/driver-updates

[Bluetooth / AV Remote Target Service]

Device Properties:

Driver Description	AV Remote Target Service
Driver Date	6/21/2006
Driver Version	6.3.9600.17673
Driver Provider	Microsoft
INF File	bth.inf
Hardware ID	BTHENUM\{0000110c-0000-1000-8000-00805f9b34fb}_VID&0001001d_PID&1200

Device Manufacturer:

Driver Update	http://www.aida64.com/driver-updates

[Bluetooth / Galaxy Note 4]

Device Properties:

Driver Description	Galaxy Note 4
Driver Date	6/21/2006
Driver Version	6.3.9600.17673
Driver Provider	Microsoft
INF File	bth.inf
Hardware ID	BTHENUM\Dev_446D6CAF0FDE

Device Manufacturer:

Driver Update	http://www.aida64.com/driver-updates

[Bluetooth / Generic Bluetooth Radio]

Device Properties:

Driver Description	Generic Bluetooth Radio
Driver Date	6/21/2006
Driver Version	6.3.9600.17673
Driver Provider	Microsoft
INF File	bth.inf
Hardware ID	USB\VID_0A12&PID_0001&REV_0100
Location Information	Port_#0002.Hub_#0003

Device Manufacturer:

Driver Update	http://www.aida64.com/driver-updates

[Bluetooth / Handsfree Audio Gateway Service]

Device Properties:

Driver Description	Handsfree Audio Gateway Service
Driver Date	6/21/2006
Driver Version	6.3.9600.17673
Driver Provider	Microsoft
INF File	bth.inf
Hardware ID	BTHENUM\{0000111f-0000-1000-8000-00805f9b34fb}_VID&0001001d_PID&1200

Device Manufacturer:

Driver Update	http://www.aida64.com/driver-updates

[Bluetooth / Headset Audio Gateway Service]

Device Properties:

Driver Description	Headset Audio Gateway Service
Driver Date	6/21/2006
Driver Version	6.3.9600.17673
Driver Provider	Microsoft
INF File	bth.inf
Hardware ID	BTHENUM\{00001112-0000-1000-8000-00805f9b34fb}_VID&0001001d_PID&1200

Device Manufacturer:

Driver Update	http://www.aida64.com/driver-updates

[Bluetooth / HY-525-BT]

Device Properties:

Driver Description	HY-525-BT
Driver Date	6/21/2006
Driver Version	6.3.9600.17673
Driver Provider	Microsoft
INF File	bth.inf
Hardware ID	BTHENUM\Dev_231F8601127D

Device Manufacturer:

Driver Update	http://www.aida64.com/driver-updates

[Bluetooth / Microsoft Bluetooth Enumerator]

Device Properties:

Driver Description	Microsoft Bluetooth Enumerator
Driver Date	6/21/2006
Driver Version	6.3.9600.17673
Driver Provider	Microsoft
INF File	bth.inf
Hardware ID	BTH\MS_BTHBRB

Device Manufacturer:

Driver Update	http://www.aida64.com/driver-updates

[Bluetooth / Object Push Service]

Device Properties:

Driver Description	Object Push Service
Driver Date	6/21/2006
Driver Version	6.3.9600.17673
Driver Provider	Microsoft
INF File	bth.inf
Hardware ID	BTHENUM\{00001105-0000-1000-8000-00805f9b34fb}_VID&0001001d_PID&1200

Device Manufacturer:

Driver Update	http://www.aida64.com/driver-updates

[Bluetooth / Personal Area Network NAP Service]

Device Properties:

Driver Description	Personal Area Network NAP Service
Driver Date	6/21/2006
Driver Version	6.3.9600.17673
Driver Provider	Microsoft
INF File	bth.inf
Hardware ID	BTHENUM\{00001116-0000-1000-8000-00805f9b34fb}_VID&0001001d_PID&1200

Device Manufacturer:

Driver Update	http://www.aida64.com/driver-updates

[Computer / ACPI x64-based PC]

Device Properties:

Driver Description	ACPI x64-based PC
Driver Date	6/21/2006
Driver Version	6.3.9600.16384
Driver Provider	Microsoft
INF File	hal.inf
Hardware ID	acpiapic

[Disk drives / OCZ-AGILITY4]

Device Properties:

Driver Description	OCZ-AGILITY4
Driver Date	6/21/2006
Driver Version	6.3.9600.16384
Driver Provider	Microsoft
INF File	disk.inf
Hardware ID	SCSI\Disk_____OCZ-AGILITY41.5.
Location Information	Bus Number 0, Target Id 0, LUN 0

Device Manufacturer:

Company Name	OCZ Technology Group, Inc.
Product Information	http://www.ocztechnology.com/products/solid_state_drives
Driver Update	http://www.aida64.com/driver-updates

[Display adapters / Intel(R) HD Graphics 4000]

Device Properties:

Driver Description	Intel(R) HD Graphics 4000

Driver Date	9/30/2014
Driver Version	10.18.10.3958
Driver Provider	Intel Corporation
INF File	oem58.inf
Hardware ID	PCI\VEN_8086&DEV_0166&SUBSYS_06491025&REV_09
Location Information	PCI bus 0, device 2, function 0
PCI Device	Intel Ivy Bridge-MB - Integrated Graphics Controller (MB GT2)

Device Resources:

IRQ	65536
Memory	000A0000-000BFFFF
Memory	B0000000-BFFFFFFF
Memory	C0000000-C03FFFFF
Port	03B0-03BB
Port	03C0-03DF
Port	2000-203F

Video Adapter Manufacturer:

Company Name	Intel Corporation
Product Information	http://www.intel.com/products/chipsets
Driver Download	http://support.intel.com/support/graphics
Driver Update	http://www.aida64.com/driver-updates

[DVD/CD-ROM drives / MATSHITA DVD-RAM UJ8C0]

Device Properties:

Driver Description	MATSHITA DVD-RAM UJ8C0
Driver Date	6/21/2006
Driver Version	6.3.9600.16384
Driver Provider	Microsoft
INF File	cdrom.inf
Hardware ID	SCSI\CdRomMATSHITADVD-RAM_UJ8C0___1.00
Location Information	Bus Number 2, Target Id 0, LUN 0

Device Manufacturer:

Company Name	Matsushita Electric Industrial Co., Ltd.
Product Information	http://www.panasonic.com/industrial/optical-drives
Firmware Download	http://www.panasonic.com/industrial/optical-drives
Driver Update	http://www.aida64.com/driver-updates

[Human Interface Devices / Galaxy Note 4 Audio/Video Remote Control HID]

Device Properties:

Driver Description	Galaxy Note 4 Audio/Video Remote Control HID
Driver Date	8/22/2013
Driver Version	6.3.9600.16384
Driver Provider	Microsoft
INF File	bthaudhid.inf
Hardware ID	BTHENUM\{0000110e-0000-1000-8000-00805f9b34fb}_VID&0001001d_PID&1200

Device Manufacturer:

Driver Update	http://www.aida64.com/driver-updates

[Human Interface Devices / HY-525-BT Audio/Video Remote Control HID]

Device Properties:

Driver Description	HY-525-BT Audio/Video Remote Control HID
Driver Date	8/22/2013
Driver Version	6.3.9600.16384
Driver Provider	Microsoft
INF File	bthaudhid.inf
Hardware ID	BTHENUM\{0000110e-0000-1000-8000-00805f9b34fb}_LOCALMFG&000f

Device Manufacturer:

Driver Update	http://www.aida64.com/driver-updates

[Human Interface Devices / USB Input Device]

Device Properties:

Driver Description	USB Input Device
Driver Date	6/21/2006
Driver Version	6.3.9600.17041
Driver Provider	Microsoft
INF File	input.inf
Hardware ID	USB\VID_17EF&PID_6020&REV_0100
Location Information	Port_#0003.Hub_#0003

Device Manufacturer:

Driver Update	http://www.aida64.com/driver-updates

[IDE ATA/ATAPI controllers / Intel(R) 7 Series/C216 Chipset Family SATA AHCI Controller - 1E03]

Device Properties:

Driver Description	Intel(R) 7 Series/C216 Chipset Family SATA AHCI Controller - 1E03
Driver Date	7/25/2013
Driver Version	9.3.0.1029
Driver Provider	Intel
INF File	oem7.inf
Hardware ID	PCI\VEN_8086&DEV_1E03&SUBSYS_06491025&REV_04
Location Information	PCI bus 0, device 31, function 2
PCI Device	Intel Panther Point-M PCH - SATA AHCI Controller [C-1]

Device Resources:

IRQ	19
Memory	C0606000-C06067FF
Port	2060-207F
Port	2080-2087
Port	2088-208F
Port	2090-2093
Port	2094-2097

Chipset Manufacturer:

Company Name	Intel Corporation
Product Information	http://www.intel.com/products/chipsets
Driver Download	http://support.intel.com/support/chipsets
BIOS Upgrades	http://www.aida64.com/bios-updates

Driver Update	http://www.aida64.com/driver-updates

[Imaging devices / HD Webcam]

Device Properties:

Driver Description	HD Webcam
Driver Date	6/21/2006
Driver Version	6.3.9600.17217
Driver Provider	Microsoft
INF File	usbvideo.inf
Hardware ID	USB\VID_1BCF&PID_2C18&REV_0007&MI_00
Location Information	0000.001a.0000.001.003.000.000.000.000

Device Manufacturer:

Driver Update	http://www.aida64.com/driver-updates

[Keyboards / Standard PS/2 Keyboard]

Device Properties:

Driver Description	Standard PS/2 Keyboard
Driver Date	6/21/2006
Driver Version	6.3.9600.17480
Driver Provider	Microsoft
INF File	keyboard.inf
Hardware ID	ACPI\VEN_1025&DEV_0759

Device Resources:

IRQ	01
Port	0060-0060
Port	0064-0064

Device Manufacturer:

Driver Update	http://www.aida64.com/driver-updates

[Mice and other pointing devices / HID-compliant mouse]

Device Properties:

Driver Description	HID-compliant mouse
Driver Date	6/21/2006
Driver Version	6.3.9600.17480
Driver Provider	Microsoft
INF File	msmouse.inf
Hardware ID	HID\VID_17EF&PID_6020&REV_0100

Device Manufacturer:

Driver Update	http://www.aida64.com/driver-updates

[Mice and other pointing devices / PS/2 Compatible Mouse]

Device Properties:

Driver Description	PS/2 Compatible Mouse
Driver Date	6/21/2006
Driver Version	6.3.9600.17480

Driver Provider	Microsoft
INF File	msmouse.inf
Hardware ID	ACPI\VEN_ETD&DEV_0500

Device Resources:

IRQ	12

Device Manufacturer:

Driver Update	http://www.aida64.com/driver-updates

[Monitors / Generic PnP Monitor]

Device Properties:

Driver Description	Generic PnP Monitor
Driver Date	6/21/2006
Driver Version	6.3.9600.16384
Driver Provider	Microsoft
INF File	monitor.inf
Hardware ID	MONITOR\AUO26EC

Device Manufacturer:

Driver Update	http://www.aida64.com/driver-updates

[Network adapters / Bluetooth Device (Personal Area Network)]

Device Properties:

Driver Description	Bluetooth Device (Personal Area Network)
Driver Date	6/21/2006
Driver Version	6.3.9600.17238
Driver Provider	Microsoft
INF File	bthpan.inf
Hardware ID	BTH\MS_BTHPAN

Device Manufacturer:

Driver Update	http://www.aida64.com/driver-updates

[Network adapters / Bluetooth Device (RFCOMM Protocol TDI)]

Device Properties:

Driver Description	Bluetooth Device (RFCOMM Protocol TDI)
Driver Date	6/21/2006
Driver Version	6.3.9600.17673
Driver Provider	Microsoft
INF File	tdibth.inf
Hardware ID	BTH\MS_RFCOMM

Device Manufacturer:

Driver Update	http://www.aida64.com/driver-updates

[Network adapters / Broadcom NetLink (TM) Gigabit Ethernet]

Device Properties:

Driver Description	Broadcom NetLink (TM) Gigabit Ethernet

Driver Date	10/30/2013
Driver Version	15.6.0.14
Driver Provider	Broadcom
INF File	oem5.inf
Hardware ID	PCI\VEN_14E4&DEV_16B5&SUBSYS_06471025&REV_10
Location Information	PCI bus 2, device 0, function 0
PCI Device	Broadcom NetLink BCM57785 PCI-E Gigabit Ethernet Controller

Device Resources:

IRQ	65536
IRQ	65536
IRQ	65536
IRQ	65536
IRQ	65536
Memory	C0430000-C043FFFF
Memory	C0440000-C044FFFF

Network Adapter Manufacturer:

Company Name	Broadcom Corporation
Product Information	http://www.broadcom.com/products
Driver Download	http://www.broadcom.com/support/ethernet_nic
Driver Update	http://www.aida64.com/driver-updates

[Network adapters / Intel(R) Dual Band Wireless-AC 7260]

Device Properties:

Driver Description	Intel(R) Dual Band Wireless-AC 7260
Driver Date	9/19/2013
Driver Version	16.5.3.6
Driver Provider	Intel
INF File	oem57.inf
Hardware ID	PCI\VEN_8086&DEV_08B1&SUBSYS_40708086&REV_BB
Location Information	PCI bus 3, device 0, function 0
PCI Device	Intel Dual Band Wireless-AC 7260 AC 2x2 HMC WiFi Adapter

Device Resources:

IRQ	65536
Memory	C0500000-C0501FFF

Network Adapter Manufacturer:

Company Name	Intel Corporation
Product Information	http://www.intel.com/embedded
Driver Download	http://www.intel.com/support/network
Driver Update	http://www.aida64.com/driver-updates

[Network adapters / Microsoft Kernel Debug Network Adapter]

Device Properties:

Driver Description	Microsoft Kernel Debug Network Adapter
Driver Date	6/21/2006
Driver Version	6.3.9600.16384
Driver Provider	Microsoft
INF File	kdnic.inf
Hardware ID	root\kdnic

Device Manufacturer:

Driver Update	http://www.aida64.com/driver-updates

[Network adapters / Microsoft Wi-Fi Direct Virtual Adapter #4]

Device Properties:

Driver Description	Microsoft Wi-Fi Direct Virtual Adapter #4
Driver Date	6/21/2006
Driver Version	6.3.9600.16384
Driver Provider	Microsoft
INF File	netvwifimp.inf
Hardware ID	{5d624f94-8850-40c3-a3fa-a4fd2080baf3}\vwifimp_wfd
Location Information	VWiFi Bus 0

Device Manufacturer:

Driver Update	http://www.aida64.com/driver-updates

[Network Infrastructure Devices / Community]

Device Properties:

Driver Description	Community
Driver Date	5/13/2010
Driver Version	1.0.0.2
Driver Provider	Microsoft
INF File	oem14.inf
Hardware ID	UMB\VEN_0BD5&DEV_0002&REV_01
Location Information	http://192.168.1.1:49152/IGDdevicedesc.xml

[Print queues / Fax]

Device Properties:

Driver Description	Fax
Driver Date	6/21/2006
Driver Version	6.3.9600.16384
Driver Provider	Microsoft
INF File	PrintQueue.inf
Hardware ID	PRINTENUM\microsoftmicrosoft_s7d14

[Print queues / Microsoft XPS Document Writer]

Device Properties:

Driver Description	Microsoft XPS Document Writer
Driver Date	6/21/2006
Driver Version	6.3.9600.16384
Driver Provider	Microsoft
INF File	PrintQueue.inf
Hardware ID	PRINTENUM\{0f4130dd-19c7-7ab6-99a1-980f03b2ee4e}

[Print queues / Root Print Queue]

Device Properties:

Driver Description	Root Print Queue
Driver Date	6/21/2006
Driver Version	6.3.9600.16384
Driver Provider	Microsoft
INF File	PrintQueue.inf
Hardware ID	PRINTENUM\LocalPrintQueue

[Print queues / Send To OneNote 2013]

Device Properties:

Driver Description	Send To OneNote 2013
Driver Date	6/21/2006
Driver Version	6.3.9600.16384
Driver Provider	Microsoft
INF File	PrintQueue.inf
Hardware ID	PRINTENUM\{3ee39114-30b4-45a4-a109-19d4a40fcc22}

[Processors / Intel(R) Core(TM) i7-3520M CPU @ 2.90GHz]

Device Properties:

Driver Description	Intel(R) Core(TM) i7-3520M CPU @ 2.90GHz
Driver Date	4/21/2009
Driver Version	6.3.9600.16384
Driver Provider	Microsoft
INF File	cpu.inf
Hardware ID	ACPI\GenuineIntel_-_Intel64_Family_6_Model_58

CPU Manufacturer:

Company Name	Intel Corporation
Product Information	http://ark.intel.com/search.aspx?q=Intel Core i7-3520M
Driver Update	http://www.aida64.com/driver-updates

[Processors / Intel(R) Core(TM) i7-3520M CPU @ 2.90GHz]

Device Properties:

Driver Description	Intel(R) Core(TM) i7-3520M CPU @ 2.90GHz
Driver Date	4/21/2009
Driver Version	6.3.9600.16384
Driver Provider	Microsoft
INF File	cpu.inf
Hardware ID	ACPI\GenuineIntel_-_Intel64_Family_6_Model_58

CPU Manufacturer:

Company Name	Intel Corporation
Product Information	http://ark.intel.com/search.aspx?q=Intel Core i7-3520M
Driver Update	http://www.aida64.com/driver-updates

[Processors / Intel(R) Core(TM) i7-3520M CPU @ 2.90GHz]

Device Properties:

Driver Description	Intel(R) Core(TM) i7-3520M CPU @ 2.90GHz
Driver Date	4/21/2009
Driver Version	6.3.9600.16384

Driver Provider	Microsoft
INF File	cpu.inf
Hardware ID	ACPI\GenuineIntel_-_Intel64_Family_6_Model_58

CPU Manufacturer:

Company Name	Intel Corporation
Product Information	http://ark.intel.com/search.aspx?q=Intel Core i7-3520M
Driver Update	http://www.aida64.com/driver-updates

[Processors / Intel(R) Core(TM) i7-3520M CPU @ 2.90GHz]

Device Properties:

Driver Description	Intel(R) Core(TM) i7-3520M CPU @ 2.90GHz
Driver Date	4/21/2009
Driver Version	6.3.9600.16384
Driver Provider	Microsoft
INF File	cpu.inf
Hardware ID	ACPI\GenuineIntel_-_Intel64_Family_6_Model_58

CPU Manufacturer:

Company Name	Intel Corporation
Product Information	http://ark.intel.com/search.aspx?q=Intel Core i7-3520M
Driver Update	http://www.aida64.com/driver-updates

[Software devices / LANDevice:1]

Device Properties:

Driver Description	LANDevice:1
Driver Date	6/21/2006
Driver Version	6.3.9600.16384
Driver Provider	Microsoft
INF File	c_swdevice.inf
Location Information	http://192.168.1.1:49152/IGDdevicedesc.xml

[Software devices / Microsoft Device Association Root Enumerator]

Device Properties:

Driver Description	Microsoft Device Association Root Enumerator
Driver Date	6/21/2006
Driver Version	6.3.9600.16384
Driver Provider	Microsoft
INF File	c_swdevice.inf

[Software devices / WANConnectionDevice:1]

Device Properties:

Driver Description	WANConnectionDevice:1
Driver Date	6/21/2006
Driver Version	6.3.9600.16384
Driver Provider	Microsoft
INF File	c_swdevice.inf
Location Information	http://192.168.1.1:49152/IGDdevicedesc.xml

[Software devices / WANDevice:1]

Device Properties:

Driver Description	WANDevice:1
Driver Date	6/21/2006
Driver Version	6.3.9600.16384
Driver Provider	Microsoft
INF File	c_swdevice.inf
Location Information	http://192.168.1.1:49152/IGDdevicedesc.xml

[Sound, video and game controllers / High Definition Audio Device]

Device Properties:

Driver Description	High Definition Audio Device
Driver Date	8/22/2013
Driver Version	6.3.9600.16384
Driver Provider	Microsoft
INF File	hdaudio.inf
Hardware ID	HDAUDIO\FUNC_01&VEN_8086&DEV_2806&SUBSYS_80860101&REV_1000
Location Information	Internal High Definition Audio Bus

Device Manufacturer:

Driver Update	http://www.aida64.com/driver-updates

[Sound, video and game controllers / High Definition Audio Device]

Device Properties:

Driver Description	High Definition Audio Device
Driver Date	8/22/2013
Driver Version	6.3.9600.16384
Driver Provider	Microsoft
INF File	hdaudio.inf
Hardware ID	HDAUDIO\FUNC_01&VEN_10EC&DEV_0269&SUBSYS_10250649&REV_1001
Location Information	Internal High Definition Audio Bus

Device Manufacturer:

Driver Update	http://www.aida64.com/driver-updates

[Sound, video and game controllers / HY-525-BT Stereo]

Device Properties:

Driver Description	HY-525-BT Stereo
Driver Date	1/29/2015
Driver Version	6.3.9600.17673
Driver Provider	Microsoft
INF File	wdma_bt.inf
Hardware ID	BTHENUM\{0000110b-0000-1000-8000-00805f9b34fb}_LOCALMFG&000f

Device Manufacturer:

Driver Update	http://www.aida64.com/driver-updates

[Storage controllers / Microsoft Storage Spaces Controller]

Device Properties:

Driver Description	Microsoft Storage Spaces Controller
Driver Date	6/21/2006
Driver Version	6.3.9600.17415
Driver Provider	Microsoft
INF File	spaceport.inf
Hardware ID	Root\Spaceport

Device Manufacturer:

Driver Update	http://www.aida64.com/driver-updates

[Storage volume shadow copies / Generic volume shadow copy]

Device Properties:

Driver Description	Generic volume shadow copy
Driver Date	6/21/2006
Driver Version	6.3.9600.16384
Driver Provider	Microsoft
INF File	volsnap.inf
Hardware ID	STORAGE\VolumeSnapshot

[Storage volume shadow copies / Generic volume shadow copy]

Device Properties:

Driver Description	Generic volume shadow copy
Driver Date	6/21/2006
Driver Version	6.3.9600.16384
Driver Provider	Microsoft
INF File	volsnap.inf
Hardware ID	STORAGE\VolumeSnapshot

[Storage volume shadow copies / Generic volume shadow copy]

Device Properties:

Driver Description	Generic volume shadow copy
Driver Date	6/21/2006
Driver Version	6.3.9600.16384
Driver Provider	Microsoft
INF File	volsnap.inf
Hardware ID	STORAGE\VolumeSnapshot

[Storage volume shadow copies / Generic volume shadow copy]

Device Properties:

Driver Description	Generic volume shadow copy
Driver Date	6/21/2006
Driver Version	6.3.9600.16384
Driver Provider	Microsoft
INF File	volsnap.inf
Hardware ID	STORAGE\VolumeSnapshot

[Storage volumes / Generic volume]

Device Properties:

Driver Description	Generic volume
Driver Date	6/21/2006
Driver Version	6.3.9600.17215
Driver Provider	Microsoft
INF File	volume.inf
Hardware ID	STORAGE\Volume

[Storage volumes / Generic volume]

Device Properties:

Driver Description	Generic volume
Driver Date	6/21/2006
Driver Version	6.3.9600.17215
Driver Provider	Microsoft
INF File	volume.inf
Hardware ID	STORAGE\Volume

[System devices / 3rd Gen Core processor DRAM Controller - 0154]

Device Properties:

Driver Description	3rd Gen Core processor DRAM Controller - 0154
Driver Date	6/21/2006
Driver Version	6.3.9600.17238
Driver Provider	Microsoft
INF File	machine.inf
Hardware ID	PCI\VEN_8086&DEV_0154&SUBSYS_06491025&REV_09
Location Information	PCI bus 0, device 0, function 0
PCI Device	Intel Ivy Bridge-MB - Host Bridge/DRAM Controller

[System devices / ACPI Fixed Feature Button]

Device Properties:

Driver Description	ACPI Fixed Feature Button
Driver Date	6/21/2006
Driver Version	6.3.9600.17238
Driver Provider	Microsoft
INF File	machine.inf
Hardware ID	ACPI\FixedButton

[System devices / ACPI Lid]

Device Properties:

Driver Description	ACPI Lid
Driver Date	6/21/2006
Driver Version	6.3.9600.17238
Driver Provider	Microsoft
INF File	machine.inf
Hardware ID	ACPI\VEN_PNP&DEV_0C0D

[System devices / ACPI Power Button]

Device Properties:

Driver Description	ACPI Power Button
Driver Date	6/21/2006
Driver Version	6.3.9600.17238
Driver Provider	Microsoft
INF File	machine.inf
Hardware ID	ACPI\VEN_PNP&DEV_0C0C

[System devices / ACPI Sleep Button]

Device Properties:

Driver Description	ACPI Sleep Button
Driver Date	6/21/2006
Driver Version	6.3.9600.17238
Driver Provider	Microsoft
INF File	machine.inf
Hardware ID	ACPI\VEN_PNP&DEV_0C0E

[System devices / Broadcom Memory Stick]

Device Properties:

Driver Description	Broadcom Memory Stick
Driver Date	7/23/2013
Driver Version	1.0.8.0
Driver Provider	Broadcom Corporation
INF File	oem11.inf
Hardware ID	PCI\VEN_14E4&DEV_16BE&SUBSYS_06471025&REV_10
Location Information	PCI bus 2, device 0, function 2
PCI Device	Broadcom Memory Stick Card Reader

Device Resources:

IRQ	17
Memory	C0410000-C041FFFF

[System devices / Broadcom SD Host Controller]

Device Properties:

Driver Description	Broadcom SD Host Controller
Driver Date	7/19/2013
Driver Version	1.0.0.254
Driver Provider	Broadcom Corporation
INF File	oem12.inf
Hardware ID	PCI\VEN_14E4&DEV_16BC&SUBSYS_06471025&REV_10
Location Information	PCI bus 2, device 0, function 1
PCI Device	Broadcom SD Card Reader

Device Resources:

IRQ	17
Memory	C0400000-C040FFFF

[System devices / Composite Bus Enumerator]

Device Properties:

Driver Description	Composite Bus Enumerator
Driver Date	6/21/2006
Driver Version	6.3.9600.16384
Driver Provider	Microsoft
INF File	CompositeBus.inf
Hardware ID	ROOT\CompositeBus

[System devices / Direct memory access controller]

Device Properties:

Driver Description	Direct memory access controller
Driver Date	6/21/2006
Driver Version	6.3.9600.17238
Driver Provider	Microsoft
INF File	machine.inf
Hardware ID	ACPI\VEN_PNP&DEV_0200

[System devices / High Definition Audio Controller]

Device Properties:

Driver Description	High Definition Audio Controller
Driver Date	7/23/2014
Driver Version	6.3.9600.17238
Driver Provider	Microsoft
INF File	hdaudbus.inf
Hardware ID	PCI\VEN_8086&DEV_1E20&SUBSYS_06491025&REV_04
Location Information	PCI bus 0, device 27, function 0
PCI Device	Intel Panther Point PCH - High Definition Audio Controller [C-1]

Device Resources:

IRQ	22
Memory	C0600000-C0603FFF

[System devices / High precision event timer]

Device Properties:

Driver Description	High precision event timer
Driver Date	6/21/2006
Driver Version	6.3.9600.17238
Driver Provider	Microsoft
INF File	machine.inf
Hardware ID	ACPI\VEN_PNP&DEV_0103

[System devices / Intel(R) 7 Series/C216 Chipset Family PCI Express Root Port 1 - 1E10]

Device Properties:

Driver Description	Intel(R) 7 Series/C216 Chipset Family PCI Express Root Port 1 - 1E10
Driver Date	7/25/2013
Driver Version	9.3.0.1029
Driver Provider	Intel
INF File	oem8.inf
Hardware ID	PCI\VEN_8086&DEV_1E10&SUBSYS_06491025&REV_C4

Location Information	PCI bus 0, device 28, function 0
PCI Device	Intel Panther Point PCH - PCI Express Port 1

Device Resources:

IRQ	17
Memory	C0400000-C04FFFFF

Chipset Manufacturer:

Company Name	Intel Corporation
Product Information	http://www.intel.com/products/chipsets
Driver Download	http://support.intel.com/support/chipsets
BIOS Upgrades	http://www.aida64.com/bios-updates
Driver Update	http://www.aida64.com/driver-updates

[System devices / Intel(R) 7 Series/C216 Chipset Family PCI Express Root Port 2 - 1E12]

Device Properties:

Driver Description	Intel(R) 7 Series/C216 Chipset Family PCI Express Root Port 2 - 1E12
Driver Date	7/25/2013
Driver Version	9.3.0.1029
Driver Provider	Intel
INF File	oem8.inf
Hardware ID	PCI\VEN_8086&DEV_1E12&SUBSYS_06491025&REV_C4
Location Information	PCI bus 0, device 28, function 1
PCI Device	Intel Panther Point PCH - PCI Express Port 2

Device Resources:

IRQ	16
Memory	C0500000-C05FFFFF

Chipset Manufacturer:

Company Name	Intel Corporation
Product Information	http://www.intel.com/products/chipsets
Driver Download	http://support.intel.com/support/chipsets
BIOS Upgrades	http://www.aida64.com/bios-updates
Driver Update	http://www.aida64.com/driver-updates

[System devices / Intel(R) 7 Series/C216 Chipset Family SMBus Host Controller - 1E22]

Device Properties:

Driver Description	Intel(R) 7 Series/C216 Chipset Family SMBus Host Controller - 1E22
Driver Date	7/25/2013
Driver Version	9.3.0.1029
Driver Provider	Intel
INF File	oem9.inf
Hardware ID	PCI\VEN_8086&DEV_1E22&SUBSYS_06491025&REV_04
Location Information	PCI bus 0, device 31, function 3
PCI Device	Intel Panther Point PCH - SMBus Controller [C-1]

Chipset Manufacturer:

Company Name	Intel Corporation
Product Information	http://www.intel.com/products/chipsets
Driver Download	http://support.intel.com/support/chipsets
BIOS Upgrades	http://www.aida64.com/bios-updates

Driver Update	http://www.aida64.com/driver-updates

[System devices / Intel(R) 82802 Firmware Hub Device]

Device Properties:

Driver Description	Intel(R) 82802 Firmware Hub Device
Driver Date	6/21/2006
Driver Version	6.3.9600.17238
Driver Provider	Microsoft
INF File	machine.inf
Hardware ID	ACPI\VEN_INT&DEV_0800

Chipset Manufacturer:

Company Name	Intel Corporation
Product Information	http://www.intel.com/products/chipsets
Driver Download	http://support.intel.com/support/chipsets
BIOS Upgrades	http://www.aida64.com/bios-updates
Driver Update	http://www.aida64.com/driver-updates

[System devices / Intel(R) HM70 Express Chipset LPC Controller - 1E5E]

Device Properties:

Driver Description	Intel(R) HM70 Express Chipset LPC Controller - 1E5E
Driver Date	7/25/2013
Driver Version	9.3.0.1029
Driver Provider	Intel
INF File	oem8.inf
Hardware ID	PCI\VEN_8086&DEV_1E5E&SUBSYS_06491025&REV_04
Location Information	PCI bus 0, device 31, function 0
PCI Device	Intel HM70 Chipset - LPC Interface Controller [C-1]

Chipset Manufacturer:

Company Name	Intel Corporation
Product Information	http://www.intel.com/products/chipsets
Driver Download	http://support.intel.com/support/chipsets
BIOS Upgrades	http://www.aida64.com/bios-updates
Driver Update	http://www.aida64.com/driver-updates

[System devices / IWD Bus Enumerator]

Device Properties:

Driver Description	IWD Bus Enumerator
Driver Date	3/13/2014
Driver Version	4.5.52.0
Driver Provider	Intel Corporation
INF File	oem60.inf
Hardware ID	root\iwdbus

[System devices / Microsoft ACPI-Compliant Embedded Controller]

Device Properties:

Driver Description	Microsoft ACPI-Compliant Embedded Controller
Driver Date	6/21/2006

Driver Version	6.3.9600.17238
Driver Provider	Microsoft
INF File	machine.inf
Hardware ID	ACPI\VEN_PNP&DEV_0C09

Device Resources:

Port	0062-0062
Port	0066-0066

[System devices / Microsoft ACPI-Compliant System]

Device Properties:

Driver Description	Microsoft ACPI-Compliant System
Driver Date	6/21/2006
Driver Version	6.3.9600.17393
Driver Provider	Microsoft
INF File	acpi.inf
Hardware ID	ACPI_HAL\PNP0C08
PnP Device	ACPI Driver/BIOS

Device Resources:

IRQ	100
IRQ	101
IRQ	102
IRQ	103
IRQ	104
IRQ	105
IRQ	106
IRQ	107
IRQ	108
IRQ	109
IRQ	110
IRQ	111
IRQ	112
IRQ	113
IRQ	114
IRQ	115
IRQ	116
IRQ	117
IRQ	118
IRQ	119
IRQ	120
IRQ	121
IRQ	122
IRQ	123
IRQ	124
IRQ	125
IRQ	126
IRQ	127
IRQ	128
IRQ	129
IRQ	130
IRQ	131
IRQ	132

IRQ	133
IRQ	134
IRQ	135
IRQ	136
IRQ	137
IRQ	138
IRQ	139
IRQ	140
IRQ	141
IRQ	142
IRQ	143
IRQ	144
IRQ	145
IRQ	146
IRQ	147
IRQ	148
IRQ	149
IRQ	150
IRQ	151
IRQ	152
IRQ	153
IRQ	154
IRQ	155
IRQ	156
IRQ	157
IRQ	158
IRQ	159
IRQ	160
IRQ	161
IRQ	162
IRQ	163
IRQ	164
IRQ	165
IRQ	166
IRQ	167
IRQ	168
IRQ	169
IRQ	170
IRQ	171
IRQ	172
IRQ	173
IRQ	174
IRQ	175
IRQ	176
IRQ	177
IRQ	178
IRQ	179
IRQ	180
IRQ	181
IRQ	182
IRQ	183
IRQ	184
IRQ	185
IRQ	186

IRQ	187
IRQ	188
IRQ	189
IRQ	190
IRQ	191
IRQ	256
IRQ	257
IRQ	258
IRQ	259
IRQ	260
IRQ	261
IRQ	262
IRQ	263
IRQ	264
IRQ	265
IRQ	266
IRQ	267
IRQ	268
IRQ	269
IRQ	270
IRQ	271
IRQ	272
IRQ	273
IRQ	274
IRQ	275
IRQ	276
IRQ	277
IRQ	278
IRQ	279
IRQ	280
IRQ	281
IRQ	282
IRQ	283
IRQ	284
IRQ	285
IRQ	286
IRQ	287
IRQ	288
IRQ	289
IRQ	290
IRQ	291
IRQ	292
IRQ	293
IRQ	294
IRQ	295
IRQ	296
IRQ	297
IRQ	298
IRQ	299
IRQ	300
IRQ	301
IRQ	302
IRQ	303
IRQ	304

IRQ	305
IRQ	306
IRQ	307
IRQ	308
IRQ	309
IRQ	310
IRQ	311
IRQ	312
IRQ	313
IRQ	314
IRQ	315
IRQ	316
IRQ	317
IRQ	318
IRQ	319
IRQ	320
IRQ	321
IRQ	322
IRQ	323
IRQ	324
IRQ	325
IRQ	326
IRQ	327
IRQ	328
IRQ	329
IRQ	330
IRQ	331
IRQ	332
IRQ	333
IRQ	334
IRQ	335
IRQ	336
IRQ	337
IRQ	338
IRQ	339
IRQ	340
IRQ	341
IRQ	342
IRQ	343
IRQ	344
IRQ	345
IRQ	346
IRQ	347
IRQ	348
IRQ	349
IRQ	350
IRQ	351
IRQ	352
IRQ	353
IRQ	354
IRQ	355
IRQ	356
IRQ	357
IRQ	358

IRQ	359
IRQ	360
IRQ	361
IRQ	362
IRQ	363
IRQ	364
IRQ	365
IRQ	366
IRQ	367
IRQ	368
IRQ	369
IRQ	370
IRQ	371
IRQ	372
IRQ	373
IRQ	374
IRQ	375
IRQ	376
IRQ	377
IRQ	378
IRQ	379
IRQ	380
IRQ	381
IRQ	382
IRQ	383
IRQ	384
IRQ	385
IRQ	386
IRQ	387
IRQ	388
IRQ	389
IRQ	390
IRQ	391
IRQ	392
IRQ	393
IRQ	394
IRQ	395
IRQ	396
IRQ	397
IRQ	398
IRQ	399
IRQ	400
IRQ	401
IRQ	402
IRQ	403
IRQ	404
IRQ	405
IRQ	406
IRQ	407
IRQ	408
IRQ	409
IRQ	410
IRQ	411
IRQ	412

IRQ	413
IRQ	414
IRQ	415
IRQ	416
IRQ	417
IRQ	418
IRQ	419
IRQ	420
IRQ	421
IRQ	422
IRQ	423
IRQ	424
IRQ	425
IRQ	426
IRQ	427
IRQ	428
IRQ	429
IRQ	430
IRQ	431
IRQ	432
IRQ	433
IRQ	434
IRQ	435
IRQ	436
IRQ	437
IRQ	438
IRQ	439
IRQ	440
IRQ	441
IRQ	442
IRQ	443
IRQ	444
IRQ	445
IRQ	446
IRQ	447
IRQ	448
IRQ	449
IRQ	450
IRQ	451
IRQ	452
IRQ	453
IRQ	454
IRQ	455
IRQ	456
IRQ	457
IRQ	458
IRQ	459
IRQ	460
IRQ	461
IRQ	462
IRQ	463
IRQ	464
IRQ	465
IRQ	466

IRQ	467
IRQ	468
IRQ	469
IRQ	470
IRQ	471
IRQ	472
IRQ	473
IRQ	474
IRQ	475
IRQ	476
IRQ	477
IRQ	478
IRQ	479
IRQ	480
IRQ	481
IRQ	482
IRQ	483
IRQ	484
IRQ	485
IRQ	486
IRQ	487
IRQ	488
IRQ	489
IRQ	490
IRQ	491
IRQ	492
IRQ	493
IRQ	494
IRQ	495
IRQ	496
IRQ	497
IRQ	498
IRQ	499
IRQ	500
IRQ	501
IRQ	502
IRQ	503
IRQ	504
IRQ	505
IRQ	506
IRQ	507
IRQ	508
IRQ	509
IRQ	510
IRQ	511
IRQ	81
IRQ	82
IRQ	83
IRQ	84
IRQ	85
IRQ	86
IRQ	87
IRQ	88
IRQ	89

IRQ	90
IRQ	91
IRQ	92
IRQ	93
IRQ	94
IRQ	95
IRQ	96
IRQ	97
IRQ	98
IRQ	99

[System devices / Microsoft Basic Display Driver]

Device Properties:

Driver Description	Microsoft Basic Display Driver
Driver Date	6/21/2006
Driver Version	6.3.9600.16384
Driver Provider	Microsoft
INF File	basicdisplay.inf
Hardware ID	ROOT\BasicDisplay

[System devices / Microsoft Basic Render Driver]

Device Properties:

Driver Description	Microsoft Basic Render Driver
Driver Date	6/21/2006
Driver Version	6.3.9600.17031
Driver Provider	Microsoft
INF File	basicrender.inf
Hardware ID	ROOT\BasicRender

[System devices / Microsoft System Management BIOS Driver]

Device Properties:

Driver Description	Microsoft System Management BIOS Driver
Driver Date	6/21/2006
Driver Version	6.3.9600.16384
Driver Provider	Microsoft
INF File	mssmbios.inf
Hardware ID	ROOT\mssmbios

[System devices / Microsoft Virtual Drive Enumerator]

Device Properties:

Driver Description	Microsoft Virtual Drive Enumerator
Driver Date	6/21/2006
Driver Version	6.3.9600.16384
Driver Provider	Microsoft
INF File	vdrvroot.inf
Hardware ID	ROOT\vdrvroot

[System devices / Microsoft Windows Management Interface for ACPI]

Device Properties:

Driver Description	Microsoft Windows Management Interface for ACPI
Driver Date	6/21/2006
Driver Version	6.3.9600.16384
Driver Provider	Microsoft
INF File	wmiacpi.inf
Hardware ID	ACPI\VEN_PNP&DEV_0C14

[System devices / Microsoft Windows Management Interface for ACPI]

Device Properties:

Driver Description	Microsoft Windows Management Interface for ACPI
Driver Date	6/21/2006
Driver Version	6.3.9600.16384
Driver Provider	Microsoft
INF File	wmiacpi.inf
Hardware ID	ACPI\VEN_PNP&DEV_0C14

[System devices / Motherboard resources]

Device Properties:

Driver Description	Motherboard resources
Driver Date	6/21/2006
Driver Version	6.3.9600.17238
Driver Provider	Microsoft
INF File	machine.inf
Hardware ID	ACPI\VEN_INT&DEV_340E

[System devices / Motherboard resources]

Device Properties:

Driver Description	Motherboard resources
Driver Date	6/21/2006
Driver Version	6.3.9600.17238
Driver Provider	Microsoft
INF File	machine.inf
Hardware ID	ACPI\VEN_PNP&DEV_0C02

[System devices / Motherboard resources]

Device Properties:

Driver Description	Motherboard resources
Driver Date	6/21/2006
Driver Version	6.3.9600.17238
Driver Provider	Microsoft
INF File	machine.inf
Hardware ID	ACPI\VEN_PNP&DEV_0C02

[System devices / Motherboard resources]

Device Properties:

Driver Description	Motherboard resources
Driver Date	6/21/2006
Driver Version	6.3.9600.17238
Driver Provider	Microsoft
INF File	machine.inf
Hardware ID	ACPI\VEN_INT&DEV_3F0D

[System devices / NDIS Virtual Network Adapter Enumerator]

Device Properties:

Driver Description	NDIS Virtual Network Adapter Enumerator
Driver Date	6/21/2006
Driver Version	6.3.9600.16384
Driver Provider	Microsoft
INF File	ndisvirtualbus.inf
Hardware ID	ROOT\NdisVirtualBus

[System devices / Numeric data processor]

Device Properties:

Driver Description	Numeric data processor
Driver Date	6/21/2006
Driver Version	6.3.9600.17238
Driver Provider	Microsoft
INF File	machine.inf
Hardware ID	ACPI\VEN_PNP&DEV_0C04

[System devices / PCI Express Root Complex]

Device Properties:

Driver Description	PCI Express Root Complex
Driver Date	6/21/2006
Driver Version	6.3.9600.17238
Driver Provider	Microsoft
INF File	machine.inf
Hardware ID	ACPI\VEN_PNP&DEV_0A08

Device Resources:

Memory	000A0000-000BFFFF
Memory	AFA00000-FEAFFFFF
Port	0000-0CF7
Port	0D00-FFFF

[System devices / Plug and Play Software Device Enumerator]

Device Properties:

Driver Description	Plug and Play Software Device Enumerator
Driver Date	6/21/2006
Driver Version	6.3.9600.17415
Driver Provider	Microsoft
INF File	swenum.inf
Hardware ID	ROOT\SWENUM

[System devices / Programmable interrupt controller]

Device Properties:

Driver Description	Programmable interrupt controller
Driver Date	6/21/2006
Driver Version	6.3.9600.17238
Driver Provider	Microsoft
INF File	machine.inf
Hardware ID	ACPI\VEN_PNP&DEV_0000

[System devices / Remote Desktop Device Redirector Bus]

Device Properties:

Driver Description	Remote Desktop Device Redirector Bus
Driver Date	6/21/2006
Driver Version	6.3.9600.16384
Driver Provider	Microsoft
INF File	rdpbus.inf
Hardware ID	ROOT\RDPBUS

[System devices / System board]

Device Properties:

Driver Description	System board
Driver Date	6/21/2006
Driver Version	6.3.9600.17238
Driver Provider	Microsoft
INF File	machine.inf
Hardware ID	ACPI\VEN_PNP&DEV_0C01

[System devices / System CMOS/real time clock]

Device Properties:

Driver Description	System CMOS/real time clock
Driver Date	6/21/2006
Driver Version	6.3.9600.17238
Driver Provider	Microsoft
INF File	machine.inf
Hardware ID	ACPI\VEN_PNP&DEV_0B00

Device Resources:

IRQ	08
Port	0070-0077

[System devices / System timer]

Device Properties:

Driver Description	System timer
Driver Date	6/21/2006
Driver Version	6.3.9600.17238
Driver Provider	Microsoft
INF File	machine.inf
Hardware ID	ACPI\VEN_PNP&DEV_0100

[System devices / UMBus Root Bus Enumerator]

Device Properties:

Driver Description	UMBus Root Bus Enumerator
Driver Date	6/21/2006
Driver Version	6.3.9600.16384
Driver Provider	Microsoft
INF File	umbus.inf
Hardware ID	root\umbus

[System devices / Volume Manager]

Device Properties:

Driver Description	Volume Manager
Driver Date	6/21/2006
Driver Version	6.3.9600.16384
Driver Provider	Microsoft
INF File	volmgr.inf
Hardware ID	ROOT\VOLMGR

[Universal Serial Bus controllers / Generic USB Hub]

Device Properties:

Driver Description	Generic USB Hub
Driver Date	6/21/2006
Driver Version	6.3.9600.17238
Driver Provider	Microsoft
INF File	usb.inf
Hardware ID	USB\VID_8087&PID_0024&REV_0000
Location Information	Port_#0001.Hub_#0001

[Universal Serial Bus controllers / Generic USB Hub]

Device Properties:

Driver Description	Generic USB Hub
Driver Date	6/21/2006
Driver Version	6.3.9600.17238
Driver Provider	Microsoft
INF File	usb.inf
Hardware ID	USB\VID_8087&PID_0024&REV_0000
Location Information	Port_#0001.Hub_#0002

[Universal Serial Bus controllers / Intel(R) 7 Series/C216 Chipset Family USB Enhanced Host Controller - 1E26]

Device Properties:

Driver Description	Intel(R) 7 Series/C216 Chipset Family USB Enhanced Host Controller - 1E26
Driver Date	7/31/2013
Driver Version	9.3.0.1030
Driver Provider	Intel
INF File	oem10.inf
Hardware ID	PCI\VEN_8086&DEV_1E26&SUBSYS_06491025&REV_04

Location Information	PCI bus 0, device 29, function 0
PCI Device	Intel Panther Point PCH - USB 2.0 EHCI Controller #1 [C-1]

Device Resources:

IRQ	23
Memory	C0607000-C06073FF

Chipset Manufacturer:

Company Name	Intel Corporation
Product Information	http://www.intel.com/products/chipsets
Driver Download	http://support.intel.com/support/chipsets
BIOS Upgrades	http://www.aida64.com/bios-updates
Driver Update	http://www.aida64.com/driver-updates

[Universal Serial Bus controllers / Intel(R) 7 Series/C216 Chipset Family USB Enhanced Host Controller - 1E2D]

Device Properties:

Driver Description	Intel(R) 7 Series/C216 Chipset Family USB Enhanced Host Controller - 1E2D
Driver Date	7/31/2013
Driver Version	9.3.0.1030
Driver Provider	Intel
INF File	oem10.inf
Hardware ID	PCI\VEN_8086&DEV_1E2D&SUBSYS_06491025&REV_04
Location Information	PCI bus 0, device 26, function 0
PCI Device	Intel Panther Point PCH - USB 2.0 EHCI Controller #2 [C-1]

Device Resources:

IRQ	16
Memory	C0608000-C06083FF

Chipset Manufacturer:

Company Name	Intel Corporation
Product Information	http://www.intel.com/products/chipsets
Driver Download	http://support.intel.com/support/chipsets
BIOS Upgrades	http://www.aida64.com/bios-updates
Driver Update	http://www.aida64.com/driver-updates

[Universal Serial Bus controllers / USB Composite Device]

Device Properties:

Driver Description	USB Composite Device
Driver Date	6/21/2006
Driver Version	6.3.9600.17238
Driver Provider	Microsoft
INF File	usb.inf
Hardware ID	USB\VID_1BCF&PID_2C18&REV_0007
Location Information	Port_#0003.Hub_#0004

[Universal Serial Bus controllers / USB Root Hub]

Device Properties:

Driver Description	USB Root Hub
Driver Date	6/21/2006

Driver Version	6.3.9600.17238
Driver Provider	Microsoft
INF File	usbport.inf
Hardware ID	USB\ROOT_HUB20&VID8086&PID1E2D&REV0004

[Universal Serial Bus controllers / USB Root Hub]

Device Properties:

Driver Description	USB Root Hub
Driver Date	6/21/2006
Driver Version	6.3.9600.17238
Driver Provider	Microsoft
INF File	usbport.inf
Hardware ID	USB\ROOT_HUB20&VID8086&PID1E26&REV0004

[Unknown / Base System Device]

Device Properties:

Driver Description	Base System Device
Hardware ID	PCI\VEN_14E4&DEV_16BF&SUBSYS_06471025&REV_10
Location Information	PCI bus 2, device 0, function 3
PCI Device	Broadcom xD Card Reader

[Unknown / Bluetooth Peripheral Device]

Device Properties:

Driver Description	Bluetooth Peripheral Device
Hardware ID	BTHENUM\{00001800-0000-1000-8000-00805f9b34fb}_VID&0001001d_PID&1200

[Unknown / Bluetooth Peripheral Device]

Device Properties:

Driver Description	Bluetooth Peripheral Device
Hardware ID	BTHENUM\{00001801-0000-1000-8000-00805f9b34fb}_VID&0001001d_PID&1200

[Unknown / MAP SMS/MMS]

Device Properties:

Driver Description	MAP SMS/MMS
Hardware ID	BTHENUM\{00001132-0000-1000-8000-00805f9b34fb}_VID&0001001d_PID&1200

[Unknown / PandoraLink]

Device Properties:

Driver Description	PandoraLink
Hardware ID	BTHENUM\{453994d5-d58b-96f9-6616-b37f586ba2ec}_VID&0001001d_PID&1200

[Unknown / Unknown]

Device Properties:

Driver Description	Unknown

Physical Devices

PCI Devices:

Bus 2, Device 0, Function 2	Broadcom Memory Stick Card Reader
Bus 2, Device 0, Function 0	Broadcom NetLink BCM57785 PCI-E Gigabit Ethernet Controller
Bus 2, Device 0, Function 1	Broadcom SD Card Reader
Bus 2, Device 0, Function 3	Broadcom xD Card Reader
Bus 3, Device 0, Function 0	Intel Dual Band Wireless-AC 7260 AC 2x2 HMC WiFi Adapter
Bus 0, Device 31, Function 0	Intel HM70 Chipset - LPC Interface Controller [C-1]
Bus 0, Device 0, Function 0	Intel Ivy Bridge-MB - Host Bridge/DRAM Controller
Bus 0, Device 2, Function 0	Intel Ivy Bridge-MB - Integrated Graphics Controller (MB GT2)
Bus 0, Device 27, Function 0	Intel Panther Point PCH - High Definition Audio Controller [C-1]
Bus 0, Device 28, Function 0	Intel Panther Point PCH - PCI Express Port 1
Bus 0, Device 28, Function 1	Intel Panther Point PCH - PCI Express Port 2
Bus 0, Device 31, Function 3	Intel Panther Point PCH - SMBus Controller [C-1]
Bus 0, Device 31, Function 6	Intel Panther Point PCH - Thermal Management Controller [C-1]
Bus 0, Device 29, Function 0	Intel Panther Point PCH - USB 2.0 EHCI Controller #1 [C-1]
Bus 0, Device 26, Function 0	Intel Panther Point PCH - USB 2.0 EHCI Controller #2 [C-1]
Bus 0, Device 31, Function 2	Intel Panther Point-M PCH - SATA AHCI Controller [C-1]

PnP Devices:

PNP0C08	ACPI Driver/BIOS
FIXEDBUTTON	ACPI Fixed Feature Button
PNP0C14	ACPI Management Interface
PNP0C14	ACPI Management Interface
PNP0A08	ACPI Three-wire Device Bus
PNP0C0A	Control Method Battery
PNP0200	DMA Controller
ETD0500	ELAN PS/2 Port Smart-Pad
PNP0C09	Embedded Controller Device
PNP0103	High Precision Event Timer
INT0800	Intel Flash EEPROM
INT340E	Intel System Device
INT3F0D	Intel Watchdog Timer
GENUINEINTEL_-_INTEL64_FAMILY_6_MODEL_58_-________INTEL(R)_CORE(TM)_I7-3520M_CPU_@_2.90GHZ	Intel(R) Core(TM) i7-3520M CPU @ 2.90GHz
GENUINEINTEL_-_INTEL64_FAMILY_6_MODEL_58_-________INTEL(R)_CORE(TM)_I7-3520M_CPU_@_2.90GHZ	Intel(R) Core(TM) i7-3520M CPU @ 2.90GHz
GENUINEINTEL_-_INTEL64_FAMILY_6_MODEL_58_-________INTEL(R)_CORE(TM)_I7-3520M_CPU_@_2.90GHZ	Intel(R) Core(TM) i7-3520M CPU @ 2.90GHz
GENUINEINTEL_-_INTEL64_FAMILY_6_MODEL_58_-________INTEL(R)_CORE(TM)_I7-3520M_CPU_@_2.90GHZ	Intel(R) Core(TM) i7-3520M CPU @ 2.90GHz
PNP0C0D	Lid
ACPI0003	Microsoft AC Adapter
PNP0C04	Numeric Data Processor
PNP0C0C	Power Button
PNP0000	Programmable Interrupt Controller
PNP0B00	Real-Time Clock
PNP0C0E	Sleep Button
10250759	Standard PS/2 Keyboard
PNP0C01	System Board Extension
PNP0100	System Timer
PNP0C02	Thermal Monitoring ACPI Device
PNP0C02	Thermal Monitoring ACPI Device

USB Devices:

0A12 0001	Generic Bluetooth Radio
8087 0024	Generic USB Hub
8087 0024	Generic USB Hub
1BCF 2C18	HD Webcam
1BCF 2C18	USB Composite Device
17EF 6020	USB Input Device

PCI Devices

[Broadcom Memory Stick Card Reader]

Device Properties:

Device Description	Broadcom Memory Stick Card Reader
Bus Type	PCI Express 2.0 x1
Bus / Device / Function	2 / 0 / 2
Device ID	14E4-16BE
Subsystem ID	1025-0647
Device Class	0880 (Base System Peripheral)
Revision	10
Fast Back-to-Back Transactions	Not Supported

Device Features:

66 MHz Operation	Not Supported
Bus Mastering	Enabled

[Broadcom NetLink BCM57785 PCI-E Gigabit Ethernet Controller]

Device Properties:

Device Description	Broadcom NetLink BCM57785 PCI-E Gigabit Ethernet Controller
Bus Type	PCI Express 2.0 x1
Bus / Device / Function	2 / 0 / 0
Device ID	14E4-16B5
Subsystem ID	1025-0647
Device Class	0200 (Ethernet Controller)
Revision	10
Fast Back-to-Back Transactions	Not Supported

Device Features:

66 MHz Operation	Not Supported
Bus Mastering	Enabled

Network Adapter Manufacturer:

Company Name	Broadcom Corporation
Product Information	http://www.broadcom.com/products
Driver Download	http://www.broadcom.com/support/ethernet_nic
Driver Update	http://www.aida64.com/driver-updates

[Broadcom SD Card Reader]

Device Properties:

Device Description	Broadcom SD Card Reader

Bus Type	PCI Express 2.0 x1
Bus / Device / Function	2 / 0 / 1
Device ID	14E4-16BC
Subsystem ID	1025-0647
Device Class	0805 (SD Host Controller)
Revision	10
Fast Back-to-Back Transactions	Not Supported

Device Features:

66 MHz Operation	Not Supported
Bus Mastering	Enabled

[Broadcom xD Card Reader]

Device Properties:

Device Description	Broadcom xD Card Reader
Bus Type	PCI Express 2.0 x1
Bus / Device / Function	2 / 0 / 3
Device ID	14E4-16BF
Subsystem ID	1025-0647
Device Class	0880 (Base System Peripheral)
Revision	10
Fast Back-to-Back Transactions	Not Supported

Device Features:

66 MHz Operation	Not Supported
Bus Mastering	Enabled

[Intel Dual Band Wireless-AC 7260 AC 2x2 HMC WiFi Adapter]

Device Properties:

Device Description	Intel Dual Band Wireless-AC 7260 AC 2x2 HMC WiFi Adapter
Bus Type	PCI Express 2.0 x1
Bus / Device / Function	3 / 0 / 0
Device ID	8086-08B1
Subsystem ID	8086-4070
Device Class	0280 (Network Controller)
Revision	BB
Fast Back-to-Back Transactions	Not Supported

Device Features:

66 MHz Operation	Not Supported
Bus Mastering	Enabled

[Intel HM70 Chipset - LPC Interface Controller [C-1]]

Device Properties:

Device Description	Intel HM70 Chipset - LPC Interface Controller [C-1]
Bus Type	PCI
Bus / Device / Function	0 / 31 / 0
Device ID	8086-1E5E
Subsystem ID	1025-0649
Device Class	0601 (PCI/ISA Bridge)

Revision	04
Fast Back-to-Back Transactions	Not Supported

Device Features:

66 MHz Operation	Not Supported
Bus Mastering	Enabled

[Intel Ivy Bridge-MB - Host Bridge/DRAM Controller]

Device Properties:

Device Description	Intel Ivy Bridge-MB - Host Bridge/DRAM Controller
Bus Type	PCI
Bus / Device / Function	0 / 0 / 0
Device ID	8086-0154
Subsystem ID	1025-0649
Device Class	0600 (Host/PCI Bridge)
Revision	09
Fast Back-to-Back Transactions	Supported, Disabled

Device Features:

66 MHz Operation	Not Supported
Bus Mastering	Enabled

[Intel Ivy Bridge-MB - Integrated Graphics Controller (MB GT2)]

Device Properties:

Device Description	Intel Ivy Bridge-MB - Integrated Graphics Controller (MB GT2)
Bus Type	PCI
Bus / Device / Function	0 / 2 / 0
Device ID	8086-0166
Subsystem ID	1025-0649
Device Class	0300 (VGA Display Controller)
Revision	09
Fast Back-to-Back Transactions	Supported, Disabled

Device Features:

66 MHz Operation	Not Supported
Bus Mastering	Enabled

Video Adapter Manufacturer:

Company Name	Intel Corporation
Product Information	http://www.intel.com/products/chipsets
Driver Download	http://support.intel.com/support/graphics
Driver Update	http://www.aida64.com/driver-updates

[Intel Panther Point PCH - High Definition Audio Controller [C-1]]

Device Properties:

Device Description	Intel Panther Point PCH - High Definition Audio Controller [C-1]
Bus Type	PCI Express 1.0
Bus / Device / Function	0 / 27 / 0
Device ID	8086-1E20
Subsystem ID	1025-0649

Device Class	0403 (High Definition Audio)
Revision	04
Fast Back-to-Back Transactions	Not Supported

Device Features:

66 MHz Operation	Not Supported
Bus Mastering	Enabled

[Intel Panther Point PCH - PCI Express Port 1]

Device Properties:

Device Description	Intel Panther Point PCH - PCI Express Port 1
Bus Type	PCI
Bus / Device / Function	0 / 28 / 0
Device ID	8086-1E10
Subsystem ID	0000-0000
Device Class	0604 (PCI/PCI Bridge)
Revision	C4
Fast Back-to-Back Transactions	Not Supported

Device Features:

66 MHz Operation	Not Supported
Bus Mastering	Enabled

[Intel Panther Point PCH - PCI Express Port 2]

Device Properties:

Device Description	Intel Panther Point PCH - PCI Express Port 2
Bus Type	PCI
Bus / Device / Function	0 / 28 / 1
Device ID	8086-1E12
Subsystem ID	0000-0000
Device Class	0604 (PCI/PCI Bridge)
Revision	C4
Fast Back-to-Back Transactions	Not Supported

Device Features:

66 MHz Operation	Not Supported
Bus Mastering	Enabled

[Intel Panther Point PCH - SMBus Controller [C-1]]

Device Properties:

Device Description	Intel Panther Point PCH - SMBus Controller [C-1]
Bus Type	PCI
Bus / Device / Function	0 / 31 / 3
Device ID	8086-1E22
Subsystem ID	1025-0649
Device Class	0C05 (SMBus Controller)
Revision	04
Fast Back-to-Back Transactions	Supported, Disabled

Device Features:

66 MHz Operation	Not Supported
Bus Mastering	Disabled

[Intel Panther Point PCH - Thermal Management Controller [C-1]]

Device Properties:

Device Description	Intel Panther Point PCH - Thermal Management Controller [C-1]
Bus Type	PCI
Bus / Device / Function	0 / 31 / 6
Device ID	8086-1E24
Subsystem ID	1025-0649
Device Class	1180 (Data Acquisition / Signal Processing Controller)
Revision	04
Fast Back-to-Back Transactions	Not Supported

Device Features:

66 MHz Operation	Not Supported
Bus Mastering	Disabled

[Intel Panther Point PCH - USB 2.0 EHCI Controller #1 [C-1]]

Device Properties:

Device Description	Intel Panther Point PCH - USB 2.0 EHCI Controller #1 [C-1]
Bus Type	PCI
Bus / Device / Function	0 / 29 / 0
Device ID	8086-1E26
Subsystem ID	1025-0649
Device Class	0C03 (USB Controller)
Revision	04
Fast Back-to-Back Transactions	Supported, Disabled

Device Features:

66 MHz Operation	Not Supported
Bus Mastering	Enabled

[Intel Panther Point PCH - USB 2.0 EHCI Controller #2 [C-1]]

Device Properties:

Device Description	Intel Panther Point PCH - USB 2.0 EHCI Controller #2 [C-1]
Bus Type	PCI
Bus / Device / Function	0 / 26 / 0
Device ID	8086-1E2D
Subsystem ID	1025-0649
Device Class	0C03 (USB Controller)
Revision	04
Fast Back-to-Back Transactions	Supported, Disabled

Device Features:

66 MHz Operation	Not Supported
Bus Mastering	Enabled

[Intel Panther Point-M PCH - SATA AHCI Controller [C-1]]

Device Properties:

Device Description	Intel Panther Point-M PCH - SATA AHCI Controller [C-1]
Bus Type	PCI
Bus / Device / Function	0 / 31 / 2
Device ID	8086-1E03
Subsystem ID	1025-0649
Device Class	0106 (SATA Controller)
Revision	04
Fast Back-to-Back Transactions	Supported, Disabled

Device Features:

66 MHz Operation	Supported
Bus Mastering	Enabled

USB Devices

[Generic USB Hub]

Device Properties:

Device Description	Generic USB Hub
Device ID	8087-0024
Device Class	09 / 00 (Hi-Speed Hub with single TT)
Device Protocol	01
Supported USB Version	2.00
Current Speed	High (USB 2.0)

[USB Composite Device]

Device Properties:

Device Description	USB Composite Device
Device ID	1BCF-2C18
Device Class	EF / 02 (Interface Association Descriptor)
Device Protocol	01
Supported USB Version	2.00
Current Speed	High (USB 2.0)

[Generic USB Hub]

Device Properties:

Device Description	Generic USB Hub
Device ID	8087-0024
Device Class	09 / 00 (Hi-Speed Hub with single TT)
Device Protocol	01
Supported USB Version	2.00
Current Speed	High (USB 2.0)

[Generic Bluetooth Radio (Bluetooth V2.0 Dongle)]

Device Properties:

Device Description	Generic Bluetooth Radio

Device ID	0A12-0001
Device Class	E0 / 01 (Bluetooth)
Device Protocol	01
Manufacturer	Bluetooth v2.0
Product	Bluetooth V2.0 Dongle
Supported USB Version	2.00
Current Speed	Full (USB 1.1)

[USB Input Device (Lenovo Wireless Optical Mouse N3903)]

Device Properties:

Device Description	USB Input Device
Device ID	17EF-6020
Device Class	03 / 01 (Human Interface Device)
Device Protocol	02
Manufacturer	Lenovo 2.4G Wireless
Product	Lenovo Wireless Optical Mouse N3903
Supported USB Version	2.00
Current Speed	Full (USB 1.1)

Device Resources

Resource	Share	Device Description
IRQ 01	Exclusive	Standard PS/2 Keyboard
IRQ 08	Exclusive	System CMOS/real time clock
IRQ 100	Exclusive	Microsoft ACPI-Compliant System
IRQ 101	Exclusive	Microsoft ACPI-Compliant System
IRQ 102	Exclusive	Microsoft ACPI-Compliant System
IRQ 103	Exclusive	Microsoft ACPI-Compliant System
IRQ 104	Exclusive	Microsoft ACPI-Compliant System
IRQ 105	Exclusive	Microsoft ACPI-Compliant System
IRQ 106	Exclusive	Microsoft ACPI-Compliant System
IRQ 107	Exclusive	Microsoft ACPI-Compliant System
IRQ 108	Exclusive	Microsoft ACPI-Compliant System
IRQ 109	Exclusive	Microsoft ACPI-Compliant System
IRQ 110	Exclusive	Microsoft ACPI-Compliant System
IRQ 111	Exclusive	Microsoft ACPI-Compliant System
IRQ 112	Exclusive	Microsoft ACPI-Compliant System
IRQ 113	Exclusive	Microsoft ACPI-Compliant System
IRQ 114	Exclusive	Microsoft ACPI-Compliant System
IRQ 115	Exclusive	Microsoft ACPI-Compliant System
IRQ 116	Exclusive	Microsoft ACPI-Compliant System
IRQ 117	Exclusive	Microsoft ACPI-Compliant System
IRQ 118	Exclusive	Microsoft ACPI-Compliant System
IRQ 119	Exclusive	Microsoft ACPI-Compliant System
IRQ 12	Exclusive	PS/2 Compatible Mouse
IRQ 120	Exclusive	Microsoft ACPI-Compliant System
IRQ 121	Exclusive	Microsoft ACPI-Compliant System
IRQ 122	Exclusive	Microsoft ACPI-Compliant System
IRQ 123	Exclusive	Microsoft ACPI-Compliant System
IRQ 124	Exclusive	Microsoft ACPI-Compliant System

IRQ 125	Exclusive	Microsoft ACPI-Compliant System
IRQ 126	Exclusive	Microsoft ACPI-Compliant System
IRQ 127	Exclusive	Microsoft ACPI-Compliant System
IRQ 128	Exclusive	Microsoft ACPI-Compliant System
IRQ 129	Exclusive	Microsoft ACPI-Compliant System
IRQ 130	Exclusive	Microsoft ACPI-Compliant System
IRQ 131	Exclusive	Microsoft ACPI-Compliant System
IRQ 132	Exclusive	Microsoft ACPI-Compliant System
IRQ 133	Exclusive	Microsoft ACPI-Compliant System
IRQ 134	Exclusive	Microsoft ACPI-Compliant System
IRQ 135	Exclusive	Microsoft ACPI-Compliant System
IRQ 136	Exclusive	Microsoft ACPI-Compliant System
IRQ 137	Exclusive	Microsoft ACPI-Compliant System
IRQ 138	Exclusive	Microsoft ACPI-Compliant System
IRQ 139	Exclusive	Microsoft ACPI-Compliant System
IRQ 140	Exclusive	Microsoft ACPI-Compliant System
IRQ 141	Exclusive	Microsoft ACPI-Compliant System
IRQ 142	Exclusive	Microsoft ACPI-Compliant System
IRQ 143	Exclusive	Microsoft ACPI-Compliant System
IRQ 144	Exclusive	Microsoft ACPI-Compliant System
IRQ 145	Exclusive	Microsoft ACPI-Compliant System
IRQ 146	Exclusive	Microsoft ACPI-Compliant System
IRQ 147	Exclusive	Microsoft ACPI-Compliant System
IRQ 148	Exclusive	Microsoft ACPI-Compliant System
IRQ 149	Exclusive	Microsoft ACPI-Compliant System
IRQ 150	Exclusive	Microsoft ACPI-Compliant System
IRQ 151	Exclusive	Microsoft ACPI-Compliant System
IRQ 152	Exclusive	Microsoft ACPI-Compliant System
IRQ 153	Exclusive	Microsoft ACPI-Compliant System
IRQ 154	Exclusive	Microsoft ACPI-Compliant System
IRQ 155	Exclusive	Microsoft ACPI-Compliant System
IRQ 156	Exclusive	Microsoft ACPI-Compliant System
IRQ 157	Exclusive	Microsoft ACPI-Compliant System
IRQ 158	Exclusive	Microsoft ACPI-Compliant System
IRQ 159	Exclusive	Microsoft ACPI-Compliant System
IRQ 16	Shared	Intel(R) 7 Series/C216 Chipset Family USB Enhanced Host Controller - 1E2D
IRQ 16	Shared	Intel(R) 7 Series/C216 Chipset Family PCI Express Root Port 2 - 1E12
IRQ 160	Exclusive	Microsoft ACPI-Compliant System
IRQ 161	Exclusive	Microsoft ACPI-Compliant System
IRQ 162	Exclusive	Microsoft ACPI-Compliant System
IRQ 163	Exclusive	Microsoft ACPI-Compliant System
IRQ 164	Exclusive	Microsoft ACPI-Compliant System
IRQ 165	Exclusive	Microsoft ACPI-Compliant System
IRQ 166	Exclusive	Microsoft ACPI-Compliant System
IRQ 167	Exclusive	Microsoft ACPI-Compliant System
IRQ 168	Exclusive	Microsoft ACPI-Compliant System
IRQ 169	Exclusive	Microsoft ACPI-Compliant System
IRQ 17	Shared	Broadcom Memory Stick
IRQ 17	Shared	Broadcom SD Host Controller
IRQ 17	Shared	Intel(R) 7 Series/C216 Chipset Family PCI Express Root Port 1 - 1E10
IRQ 170	Exclusive	Microsoft ACPI-Compliant System
IRQ 171	Exclusive	Microsoft ACPI-Compliant System
IRQ 172	Exclusive	Microsoft ACPI-Compliant System
IRQ 173	Exclusive	Microsoft ACPI-Compliant System

IRQ 174	Exclusive	Microsoft ACPI-Compliant System
IRQ 175	Exclusive	Microsoft ACPI-Compliant System
IRQ 176	Exclusive	Microsoft ACPI-Compliant System
IRQ 177	Exclusive	Microsoft ACPI-Compliant System
IRQ 178	Exclusive	Microsoft ACPI-Compliant System
IRQ 179	Exclusive	Microsoft ACPI-Compliant System
IRQ 180	Exclusive	Microsoft ACPI-Compliant System
IRQ 181	Exclusive	Microsoft ACPI-Compliant System
IRQ 182	Exclusive	Microsoft ACPI-Compliant System
IRQ 183	Exclusive	Microsoft ACPI-Compliant System
IRQ 184	Exclusive	Microsoft ACPI-Compliant System
IRQ 185	Exclusive	Microsoft ACPI-Compliant System
IRQ 186	Exclusive	Microsoft ACPI-Compliant System
IRQ 187	Exclusive	Microsoft ACPI-Compliant System
IRQ 188	Exclusive	Microsoft ACPI-Compliant System
IRQ 189	Exclusive	Microsoft ACPI-Compliant System
IRQ 19	Shared	Intel(R) 7 Series/C216 Chipset Family SATA AHCI Controller - 1E03
IRQ 190	Exclusive	Microsoft ACPI-Compliant System
IRQ 191	Exclusive	Microsoft ACPI-Compliant System
IRQ 22	Shared	High Definition Audio Controller
IRQ 23	Shared	Intel(R) 7 Series/C216 Chipset Family USB Enhanced Host Controller - 1E26
IRQ 256	Exclusive	Microsoft ACPI-Compliant System
IRQ 257	Exclusive	Microsoft ACPI-Compliant System
IRQ 258	Exclusive	Microsoft ACPI-Compliant System
IRQ 259	Exclusive	Microsoft ACPI-Compliant System
IRQ 260	Exclusive	Microsoft ACPI-Compliant System
IRQ 261	Exclusive	Microsoft ACPI-Compliant System
IRQ 262	Exclusive	Microsoft ACPI-Compliant System
IRQ 263	Exclusive	Microsoft ACPI-Compliant System
IRQ 264	Exclusive	Microsoft ACPI-Compliant System
IRQ 265	Exclusive	Microsoft ACPI-Compliant System
IRQ 266	Exclusive	Microsoft ACPI-Compliant System
IRQ 267	Exclusive	Microsoft ACPI-Compliant System
IRQ 268	Exclusive	Microsoft ACPI-Compliant System
IRQ 269	Exclusive	Microsoft ACPI-Compliant System
IRQ 270	Exclusive	Microsoft ACPI-Compliant System
IRQ 271	Exclusive	Microsoft ACPI-Compliant System
IRQ 272	Exclusive	Microsoft ACPI-Compliant System
IRQ 273	Exclusive	Microsoft ACPI-Compliant System
IRQ 274	Exclusive	Microsoft ACPI-Compliant System
IRQ 275	Exclusive	Microsoft ACPI-Compliant System
IRQ 276	Exclusive	Microsoft ACPI-Compliant System
IRQ 277	Exclusive	Microsoft ACPI-Compliant System
IRQ 278	Exclusive	Microsoft ACPI-Compliant System
IRQ 279	Exclusive	Microsoft ACPI-Compliant System
IRQ 280	Exclusive	Microsoft ACPI-Compliant System
IRQ 281	Exclusive	Microsoft ACPI-Compliant System
IRQ 282	Exclusive	Microsoft ACPI-Compliant System
IRQ 283	Exclusive	Microsoft ACPI-Compliant System
IRQ 284	Exclusive	Microsoft ACPI-Compliant System
IRQ 285	Exclusive	Microsoft ACPI-Compliant System
IRQ 286	Exclusive	Microsoft ACPI-Compliant System
IRQ 287	Exclusive	Microsoft ACPI-Compliant System
IRQ 288	Exclusive	Microsoft ACPI-Compliant System

IRQ 289	Exclusive	Microsoft ACPI-Compliant System
IRQ 290	Exclusive	Microsoft ACPI-Compliant System
IRQ 291	Exclusive	Microsoft ACPI-Compliant System
IRQ 292	Exclusive	Microsoft ACPI-Compliant System
IRQ 293	Exclusive	Microsoft ACPI-Compliant System
IRQ 294	Exclusive	Microsoft ACPI-Compliant System
IRQ 295	Exclusive	Microsoft ACPI-Compliant System
IRQ 296	Exclusive	Microsoft ACPI-Compliant System
IRQ 297	Exclusive	Microsoft ACPI-Compliant System
IRQ 298	Exclusive	Microsoft ACPI-Compliant System
IRQ 299	Exclusive	Microsoft ACPI-Compliant System
IRQ 300	Exclusive	Microsoft ACPI-Compliant System
IRQ 301	Exclusive	Microsoft ACPI-Compliant System
IRQ 302	Exclusive	Microsoft ACPI-Compliant System
IRQ 303	Exclusive	Microsoft ACPI-Compliant System
IRQ 304	Exclusive	Microsoft ACPI-Compliant System
IRQ 305	Exclusive	Microsoft ACPI-Compliant System
IRQ 306	Exclusive	Microsoft ACPI-Compliant System
IRQ 307	Exclusive	Microsoft ACPI-Compliant System
IRQ 308	Exclusive	Microsoft ACPI-Compliant System
IRQ 309	Exclusive	Microsoft ACPI-Compliant System
IRQ 310	Exclusive	Microsoft ACPI-Compliant System
IRQ 311	Exclusive	Microsoft ACPI-Compliant System
IRQ 312	Exclusive	Microsoft ACPI-Compliant System
IRQ 313	Exclusive	Microsoft ACPI-Compliant System
IRQ 314	Exclusive	Microsoft ACPI-Compliant System
IRQ 315	Exclusive	Microsoft ACPI-Compliant System
IRQ 316	Exclusive	Microsoft ACPI-Compliant System
IRQ 317	Exclusive	Microsoft ACPI-Compliant System
IRQ 318	Exclusive	Microsoft ACPI-Compliant System
IRQ 319	Exclusive	Microsoft ACPI-Compliant System
IRQ 320	Exclusive	Microsoft ACPI-Compliant System
IRQ 321	Exclusive	Microsoft ACPI-Compliant System
IRQ 322	Exclusive	Microsoft ACPI-Compliant System
IRQ 323	Exclusive	Microsoft ACPI-Compliant System
IRQ 324	Exclusive	Microsoft ACPI-Compliant System
IRQ 325	Exclusive	Microsoft ACPI-Compliant System
IRQ 326	Exclusive	Microsoft ACPI-Compliant System
IRQ 327	Exclusive	Microsoft ACPI-Compliant System
IRQ 328	Exclusive	Microsoft ACPI-Compliant System
IRQ 329	Exclusive	Microsoft ACPI-Compliant System
IRQ 330	Exclusive	Microsoft ACPI-Compliant System
IRQ 331	Exclusive	Microsoft ACPI-Compliant System
IRQ 332	Exclusive	Microsoft ACPI-Compliant System
IRQ 333	Exclusive	Microsoft ACPI-Compliant System
IRQ 334	Exclusive	Microsoft ACPI-Compliant System
IRQ 335	Exclusive	Microsoft ACPI-Compliant System
IRQ 336	Exclusive	Microsoft ACPI-Compliant System
IRQ 337	Exclusive	Microsoft ACPI-Compliant System
IRQ 338	Exclusive	Microsoft ACPI-Compliant System
IRQ 339	Exclusive	Microsoft ACPI-Compliant System
IRQ 340	Exclusive	Microsoft ACPI-Compliant System
IRQ 341	Exclusive	Microsoft ACPI-Compliant System
IRQ 342	Exclusive	Microsoft ACPI-Compliant System

IRQ 343	Exclusive	Microsoft ACPI-Compliant System
IRQ 344	Exclusive	Microsoft ACPI-Compliant System
IRQ 345	Exclusive	Microsoft ACPI-Compliant System
IRQ 346	Exclusive	Microsoft ACPI-Compliant System
IRQ 347	Exclusive	Microsoft ACPI-Compliant System
IRQ 348	Exclusive	Microsoft ACPI-Compliant System
IRQ 349	Exclusive	Microsoft ACPI-Compliant System
IRQ 350	Exclusive	Microsoft ACPI-Compliant System
IRQ 351	Exclusive	Microsoft ACPI-Compliant System
IRQ 352	Exclusive	Microsoft ACPI-Compliant System
IRQ 353	Exclusive	Microsoft ACPI-Compliant System
IRQ 354	Exclusive	Microsoft ACPI-Compliant System
IRQ 355	Exclusive	Microsoft ACPI-Compliant System
IRQ 356	Exclusive	Microsoft ACPI-Compliant System
IRQ 357	Exclusive	Microsoft ACPI-Compliant System
IRQ 358	Exclusive	Microsoft ACPI-Compliant System
IRQ 359	Exclusive	Microsoft ACPI-Compliant System
IRQ 360	Exclusive	Microsoft ACPI-Compliant System
IRQ 361	Exclusive	Microsoft ACPI-Compliant System
IRQ 362	Exclusive	Microsoft ACPI-Compliant System
IRQ 363	Exclusive	Microsoft ACPI-Compliant System
IRQ 364	Exclusive	Microsoft ACPI-Compliant System
IRQ 365	Exclusive	Microsoft ACPI-Compliant System
IRQ 366	Exclusive	Microsoft ACPI-Compliant System
IRQ 367	Exclusive	Microsoft ACPI-Compliant System
IRQ 368	Exclusive	Microsoft ACPI-Compliant System
IRQ 369	Exclusive	Microsoft ACPI-Compliant System
IRQ 370	Exclusive	Microsoft ACPI-Compliant System
IRQ 371	Exclusive	Microsoft ACPI-Compliant System
IRQ 372	Exclusive	Microsoft ACPI-Compliant System
IRQ 373	Exclusive	Microsoft ACPI-Compliant System
IRQ 374	Exclusive	Microsoft ACPI-Compliant System
IRQ 375	Exclusive	Microsoft ACPI-Compliant System
IRQ 376	Exclusive	Microsoft ACPI-Compliant System
IRQ 377	Exclusive	Microsoft ACPI-Compliant System
IRQ 378	Exclusive	Microsoft ACPI-Compliant System
IRQ 379	Exclusive	Microsoft ACPI-Compliant System
IRQ 380	Exclusive	Microsoft ACPI-Compliant System
IRQ 381	Exclusive	Microsoft ACPI-Compliant System
IRQ 382	Exclusive	Microsoft ACPI-Compliant System
IRQ 383	Exclusive	Microsoft ACPI-Compliant System
IRQ 384	Exclusive	Microsoft ACPI-Compliant System
IRQ 385	Exclusive	Microsoft ACPI-Compliant System
IRQ 386	Exclusive	Microsoft ACPI-Compliant System
IRQ 387	Exclusive	Microsoft ACPI-Compliant System
IRQ 388	Exclusive	Microsoft ACPI-Compliant System
IRQ 389	Exclusive	Microsoft ACPI-Compliant System
IRQ 390	Exclusive	Microsoft ACPI-Compliant System
IRQ 391	Exclusive	Microsoft ACPI-Compliant System
IRQ 392	Exclusive	Microsoft ACPI-Compliant System
IRQ 393	Exclusive	Microsoft ACPI-Compliant System
IRQ 394	Exclusive	Microsoft ACPI-Compliant System
IRQ 395	Exclusive	Microsoft ACPI-Compliant System
IRQ 396	Exclusive	Microsoft ACPI-Compliant System

IRQ 397	Exclusive	Microsoft ACPI-Compliant System
IRQ 398	Exclusive	Microsoft ACPI-Compliant System
IRQ 399	Exclusive	Microsoft ACPI-Compliant System
IRQ 400	Exclusive	Microsoft ACPI-Compliant System
IRQ 401	Exclusive	Microsoft ACPI-Compliant System
IRQ 402	Exclusive	Microsoft ACPI-Compliant System
IRQ 403	Exclusive	Microsoft ACPI-Compliant System
IRQ 404	Exclusive	Microsoft ACPI-Compliant System
IRQ 405	Exclusive	Microsoft ACPI-Compliant System
IRQ 406	Exclusive	Microsoft ACPI-Compliant System
IRQ 407	Exclusive	Microsoft ACPI-Compliant System
IRQ 408	Exclusive	Microsoft ACPI-Compliant System
IRQ 409	Exclusive	Microsoft ACPI-Compliant System
IRQ 410	Exclusive	Microsoft ACPI-Compliant System
IRQ 411	Exclusive	Microsoft ACPI-Compliant System
IRQ 412	Exclusive	Microsoft ACPI-Compliant System
IRQ 413	Exclusive	Microsoft ACPI-Compliant System
IRQ 414	Exclusive	Microsoft ACPI-Compliant System
IRQ 415	Exclusive	Microsoft ACPI-Compliant System
IRQ 416	Exclusive	Microsoft ACPI-Compliant System
IRQ 417	Exclusive	Microsoft ACPI-Compliant System
IRQ 418	Exclusive	Microsoft ACPI-Compliant System
IRQ 419	Exclusive	Microsoft ACPI-Compliant System
IRQ 420	Exclusive	Microsoft ACPI-Compliant System
IRQ 421	Exclusive	Microsoft ACPI-Compliant System
IRQ 422	Exclusive	Microsoft ACPI-Compliant System
IRQ 423	Exclusive	Microsoft ACPI-Compliant System
IRQ 424	Exclusive	Microsoft ACPI-Compliant System
IRQ 425	Exclusive	Microsoft ACPI-Compliant System
IRQ 426	Exclusive	Microsoft ACPI-Compliant System
IRQ 427	Exclusive	Microsoft ACPI-Compliant System
IRQ 428	Exclusive	Microsoft ACPI-Compliant System
IRQ 429	Exclusive	Microsoft ACPI-Compliant System
IRQ 430	Exclusive	Microsoft ACPI-Compliant System
IRQ 431	Exclusive	Microsoft ACPI-Compliant System
IRQ 432	Exclusive	Microsoft ACPI-Compliant System
IRQ 433	Exclusive	Microsoft ACPI-Compliant System
IRQ 434	Exclusive	Microsoft ACPI-Compliant System
IRQ 435	Exclusive	Microsoft ACPI-Compliant System
IRQ 436	Exclusive	Microsoft ACPI-Compliant System
IRQ 437	Exclusive	Microsoft ACPI-Compliant System
IRQ 438	Exclusive	Microsoft ACPI-Compliant System
IRQ 439	Exclusive	Microsoft ACPI-Compliant System
IRQ 440	Exclusive	Microsoft ACPI-Compliant System
IRQ 441	Exclusive	Microsoft ACPI-Compliant System
IRQ 442	Exclusive	Microsoft ACPI-Compliant System
IRQ 443	Exclusive	Microsoft ACPI-Compliant System
IRQ 444	Exclusive	Microsoft ACPI-Compliant System
IRQ 445	Exclusive	Microsoft ACPI-Compliant System
IRQ 446	Exclusive	Microsoft ACPI-Compliant System
IRQ 447	Exclusive	Microsoft ACPI-Compliant System
IRQ 448	Exclusive	Microsoft ACPI-Compliant System
IRQ 449	Exclusive	Microsoft ACPI-Compliant System
IRQ 450	Exclusive	Microsoft ACPI-Compliant System

IRQ 451	Exclusive	Microsoft ACPI-Compliant System
IRQ 452	Exclusive	Microsoft ACPI-Compliant System
IRQ 453	Exclusive	Microsoft ACPI-Compliant System
IRQ 454	Exclusive	Microsoft ACPI-Compliant System
IRQ 455	Exclusive	Microsoft ACPI-Compliant System
IRQ 456	Exclusive	Microsoft ACPI-Compliant System
IRQ 457	Exclusive	Microsoft ACPI-Compliant System
IRQ 458	Exclusive	Microsoft ACPI-Compliant System
IRQ 459	Exclusive	Microsoft ACPI-Compliant System
IRQ 460	Exclusive	Microsoft ACPI-Compliant System
IRQ 461	Exclusive	Microsoft ACPI-Compliant System
IRQ 462	Exclusive	Microsoft ACPI-Compliant System
IRQ 463	Exclusive	Microsoft ACPI-Compliant System
IRQ 464	Exclusive	Microsoft ACPI-Compliant System
IRQ 465	Exclusive	Microsoft ACPI-Compliant System
IRQ 466	Exclusive	Microsoft ACPI-Compliant System
IRQ 467	Exclusive	Microsoft ACPI-Compliant System
IRQ 468	Exclusive	Microsoft ACPI-Compliant System
IRQ 469	Exclusive	Microsoft ACPI-Compliant System
IRQ 470	Exclusive	Microsoft ACPI-Compliant System
IRQ 471	Exclusive	Microsoft ACPI-Compliant System
IRQ 472	Exclusive	Microsoft ACPI-Compliant System
IRQ 473	Exclusive	Microsoft ACPI-Compliant System
IRQ 474	Exclusive	Microsoft ACPI-Compliant System
IRQ 475	Exclusive	Microsoft ACPI-Compliant System
IRQ 476	Exclusive	Microsoft ACPI-Compliant System
IRQ 477	Exclusive	Microsoft ACPI-Compliant System
IRQ 478	Exclusive	Microsoft ACPI-Compliant System
IRQ 479	Exclusive	Microsoft ACPI-Compliant System
IRQ 480	Exclusive	Microsoft ACPI-Compliant System
IRQ 481	Exclusive	Microsoft ACPI-Compliant System
IRQ 482	Exclusive	Microsoft ACPI-Compliant System
IRQ 483	Exclusive	Microsoft ACPI-Compliant System
IRQ 484	Exclusive	Microsoft ACPI-Compliant System
IRQ 485	Exclusive	Microsoft ACPI-Compliant System
IRQ 486	Exclusive	Microsoft ACPI-Compliant System
IRQ 487	Exclusive	Microsoft ACPI-Compliant System
IRQ 488	Exclusive	Microsoft ACPI-Compliant System
IRQ 489	Exclusive	Microsoft ACPI-Compliant System
IRQ 490	Exclusive	Microsoft ACPI-Compliant System
IRQ 491	Exclusive	Microsoft ACPI-Compliant System
IRQ 492	Exclusive	Microsoft ACPI-Compliant System
IRQ 493	Exclusive	Microsoft ACPI-Compliant System
IRQ 494	Exclusive	Microsoft ACPI-Compliant System
IRQ 495	Exclusive	Microsoft ACPI-Compliant System
IRQ 496	Exclusive	Microsoft ACPI-Compliant System
IRQ 497	Exclusive	Microsoft ACPI-Compliant System
IRQ 498	Exclusive	Microsoft ACPI-Compliant System
IRQ 499	Exclusive	Microsoft ACPI-Compliant System
IRQ 500	Exclusive	Microsoft ACPI-Compliant System
IRQ 501	Exclusive	Microsoft ACPI-Compliant System
IRQ 502	Exclusive	Microsoft ACPI-Compliant System
IRQ 503	Exclusive	Microsoft ACPI-Compliant System
IRQ 504	Exclusive	Microsoft ACPI-Compliant System

IRQ 505	Exclusive	Microsoft ACPI-Compliant System
IRQ 506	Exclusive	Microsoft ACPI-Compliant System
IRQ 507	Exclusive	Microsoft ACPI-Compliant System
IRQ 508	Exclusive	Microsoft ACPI-Compliant System
IRQ 509	Exclusive	Microsoft ACPI-Compliant System
IRQ 510	Exclusive	Microsoft ACPI-Compliant System
IRQ 511	Exclusive	Microsoft ACPI-Compliant System
IRQ 65536	Exclusive	Broadcom NetLink (TM) Gigabit Ethernet
IRQ 65536	Exclusive	Broadcom NetLink (TM) Gigabit Ethernet
IRQ 65536	Exclusive	Broadcom NetLink (TM) Gigabit Ethernet
IRQ 65536	Exclusive	Broadcom NetLink (TM) Gigabit Ethernet
IRQ 65536	Exclusive	Broadcom NetLink (TM) Gigabit Ethernet
IRQ 65536	Exclusive	Intel(R) Dual Band Wireless-AC 7260
IRQ 65536	Exclusive	Intel(R) HD Graphics 4000
IRQ 81	Exclusive	Microsoft ACPI-Compliant System
IRQ 82	Exclusive	Microsoft ACPI-Compliant System
IRQ 83	Exclusive	Microsoft ACPI-Compliant System
IRQ 84	Exclusive	Microsoft ACPI-Compliant System
IRQ 85	Exclusive	Microsoft ACPI-Compliant System
IRQ 86	Exclusive	Microsoft ACPI-Compliant System
IRQ 87	Exclusive	Microsoft ACPI-Compliant System
IRQ 88	Exclusive	Microsoft ACPI-Compliant System
IRQ 89	Exclusive	Microsoft ACPI-Compliant System
IRQ 90	Exclusive	Microsoft ACPI-Compliant System
IRQ 91	Exclusive	Microsoft ACPI-Compliant System
IRQ 92	Exclusive	Microsoft ACPI-Compliant System
IRQ 93	Exclusive	Microsoft ACPI-Compliant System
IRQ 94	Exclusive	Microsoft ACPI-Compliant System
IRQ 95	Exclusive	Microsoft ACPI-Compliant System
IRQ 96	Exclusive	Microsoft ACPI-Compliant System
IRQ 97	Exclusive	Microsoft ACPI-Compliant System
IRQ 98	Exclusive	Microsoft ACPI-Compliant System
IRQ 99	Exclusive	Microsoft ACPI-Compliant System
Memory 000A0000-000BFFFF	Shared	Intel(R) HD Graphics 4000
Memory 000A0000-000BFFFF	Shared	PCI Express Root Complex
Memory AFA00000-FEAFFFFF	Shared	PCI Express Root Complex
Memory B0000000-BFFFFFFF	Exclusive	Intel(R) HD Graphics 4000
Memory C0000000-C03FFFFF	Exclusive	Intel(R) HD Graphics 4000
Memory C0400000-C040FFFF	Exclusive	Broadcom SD Host Controller
Memory C0400000-C04FFFFF	Exclusive	Intel(R) 7 Series/C216 Chipset Family PCI Express Root Port 1 - 1E10
Memory C0410000-C041FFFF	Exclusive	Broadcom Memory Stick
Memory C0430000-C043FFFF	Exclusive	Broadcom NetLink (TM) Gigabit Ethernet
Memory C0440000-C044FFFF	Exclusive	Broadcom NetLink (TM) Gigabit Ethernet
Memory C0500000-C0501FFF	Exclusive	Intel(R) Dual Band Wireless-AC 7260
Memory C0500000-C05FFFFF	Exclusive	Intel(R) 7 Series/C216 Chipset Family PCI Express Root Port 2 - 1E12
Memory C0600000-C0603FFF	Exclusive	High Definition Audio Controller
Memory C0606000-C06067FF	Exclusive	Intel(R) 7 Series/C216 Chipset Family SATA AHCI Controller - 1E03
Memory C0607000-C06073FF	Exclusive	Intel(R) 7 Series/C216 Chipset Family USB Enhanced Host Controller - 1E26
Memory C0608000-C06083FF	Exclusive	Intel(R) 7 Series/C216 Chipset Family USB Enhanced Host Controller - 1E2D
Port 0000-0CF7	Shared	PCI Express Root Complex
Port 0060-0060	Exclusive	Standard PS/2 Keyboard
Port 0062-0062	Exclusive	Microsoft ACPI-Compliant Embedded Controller
Port 0064-0064	Exclusive	Standard PS/2 Keyboard
Port 0066-0066	Exclusive	Microsoft ACPI-Compliant Embedded Controller

Port 0070-0077	Exclusive	System CMOS/real time clock
Port 03B0-03BB	Shared	Intel(R) HD Graphics 4000
Port 03C0-03DF	Shared	Intel(R) HD Graphics 4000
Port 0D00-FFFF	Shared	PCI Express Root Complex
Port 2000-203F	Exclusive	Intel(R) HD Graphics 4000
Port 2060-207F	Exclusive	Intel(R) 7 Series/C216 Chipset Family SATA AHCI Controller - 1E03
Port 2080-2087	Exclusive	Intel(R) 7 Series/C216 Chipset Family SATA AHCI Controller - 1E03
Port 2088-208F	Exclusive	Intel(R) 7 Series/C216 Chipset Family SATA AHCI Controller - 1E03
Port 2090-2093	Exclusive	Intel(R) 7 Series/C216 Chipset Family SATA AHCI Controller - 1E03
Port 2094-2097	Exclusive	Intel(R) 7 Series/C216 Chipset Family SATA AHCI Controller - 1E03

Input

[Standard PS/2 Keyboard]

Keyboard Properties:

Keyboard Name	Standard PS/2 Keyboard
Keyboard Type	Japanese keyboard
Keyboard Layout	US
ANSI Code Page	1252 - Western European (Windows)
OEM Code Page	437
Repeat Delay	1
Repeat Rate	31

[HID-compliant mouse]

Mouse Properties:

Mouse Name	HID-compliant mouse
Mouse Buttons	8
Mouse Hand	Right
Pointer Speed	1
Double-Click Time	550 msec
X/Y Threshold	6 / 10
Wheel Scroll Lines	3

Mouse Features:

Active Window Tracking	Disabled
ClickLock	Disabled
Hide Pointer While Typing	Enabled
Mouse Wheel	Present
Move Pointer To Default Button	Disabled
Pointer Trails	Disabled
Sonar	Disabled

Printers

[Fax]

Printer Properties:

Printer Name	Fax
Default Printer	No
Share Point	Not shared
Printer Port	SHRFAX:
Printer Driver	Microsoft Shared Fax Driver (v4.00)
Device Name	Fax
Print Processor	winprint
Separator Page	None
Availability	Always
Priority	1
Print Jobs Queued	0
Status	Unknown

Paper Properties:

Paper Size	Letter, 8.5 x 11 in
Orientation	Portrait
Print Quality	200 x 200 dpi Mono

[Microsoft XPS Document Writer]

Printer Properties:

Printer Name	Microsoft XPS Document Writer
Default Printer	No
Share Point	Not shared
Printer Port	PORTPROMPT:
Printer Driver	Microsoft XPS Document Writer v4 (v6.03)
Device Name	Microsoft XPS Document Writer
Print Processor	winprint
Separator Page	None
Availability	Always
Priority	1
Print Jobs Queued	0
Status	Unknown

Paper Properties:

Paper Size	Letter, 8.5 x 11 in
Orientation	Portrait
Print Quality	600 x 600 dpi Color

[Send To OneNote 2013 (Default)]

Printer Properties:

Printer Name	Send To OneNote 2013
Default Printer	Yes
Share Point	Not shared
Printer Port	nul:
Printer Driver	Send to Microsoft OneNote 15 Driver (v6.03)
Device Name	Send To OneNote 2013
Print Processor	winprint
Separator Page	None
Availability	Always
Priority	1
Print Jobs Queued	0

Status	Unknown

Paper Properties:

Paper Size	Letter, 8.5 x 11 in
Orientation	Portrait
Print Quality	600 x 600 dpi Color

Auto Start

Application Description	Start From	Application Command
BTMTrayAgent	Registry\Common\Run	rundll32.exe C:\Program Files (x86)\Intel\Bluetooth\btmshellex.dll",TrayApp
Send to OneNote	StartMenu\User	C:\Program Files (x86)\Microsoft Office\Office15\ONENOTEM.EXE /tsr

Scheduled

[Microsoft Office 15 Sync Maintenance for LTRANPHD-Liem LTranPHD]

Task Properties:

Task Name	Microsoft Office 15 Sync Maintenance for LTRANPHD-Liem LTranPHD
Status	Enabled
Application Name	C:\Program Files\Microsoft Office\Office15\MsoSync.exe
Application Parameters	
Working Folder	
Comment	Lightweight task keeps Microsoft Office Document Cache in good shape. Disabling this task may lead to unexpected issues when working with documents from online sources as well as higher disk usage.
Account Name	LTRANPHD\Liem
Creator	Microsoft Office
Last Run	3/22/2015 3:29:18 PM
Next Run	Unknown

Task Triggers:

At log on	At log on of LTRANPHD\Liem
On idle	When computer is idle
One time	At 02:16:24Z on 4/23/2015

[Optimize Start Menu Cache Files-S-1-5-21-1888849264-3803429180-4108621888-1001]

Task Properties:

Task Name	Optimize Start Menu Cache Files-S-1-5-21-1888849264-3803429180-4108621888-1001
Status	Disabled
Application Name	
Application Parameters	
Working Folder	
Comment	This idle task reorganizes the cache files used to display the start menu. It is enabled only when the cache files are not optimally organized.
Account Name	Liem
Creator	Microsoft Corporation
Last Run	4/27/2015 6:02:00 PM

Next Run	Unknown

Task Triggers:

On idle	When computer is idle

Installed Programs

Program	Version	Inst. Size	GUID	Publisher	Inst. Date
Advanced SystemCare 8	8.2.0	Unknown	Advanced SystemCare 8_is1	IObit	2015-04-10
CCleaner	5.04	Unknown	CCleaner	Piriform	
Definition Update for Microsoft Office 2013 (KB2965273) 64-Bit Edition		Unknown	{90150000-0011-0000-1000-0000000FF1CE}_Office15.PROPLUS_{3D7BF4DB-4BB0-4559-9E7D-9BFFEBD36234}	Microsoft	
Glary Utilities 5.22	5.22.0.41	Unknown	Glary Utilities 5	Glarysoft Ltd	
Google Chrome	41.0.2272.118	Unknown	Google Chrome	Google Inc.	2015-04-10
Google Update Helper	1.3.26.9	Unknown	{60EC980A-BDA2-4CB6-A427-B07A5498B4CA}	Google Inc.	2015-04-10
HHD Software Free Hex Editor Neo 6.11	6.11.0.5363	Unknown	{8EB85C0E-DE7D-4A53-BD66-708B8F2C80B0}	HHD Software, Ltd.	
HWiNFO64 Version 4.60	4.60	Unknown	HWiNFO64_is1	Martin Malík - REALiX	2015-04-22
Intel(R) Processor Graphics	10.18.10.3958	Unknown	{F0E3AD40-2BBD-4360-9C76-B9AC9A5886EA}	Intel Corporation	
Intel(R) Wireless Bluetooth(R)(patch version 17.1.1512.771)	17.1.1501.0514	Unknown	{302600C1-6BDF-4FD1-1501-148929CC1385}	Intel Corporation	2015-04-22
Microsoft Access MUI (English) 2013	15.0.4569.1506	Unknown	{90150000-0015-0409-1000-0000000FF1CE}	Microsoft Corporation	2015-04-15
Microsoft Access Setup Metadata MUI (English) 2013	15.0.4569.1506	Unknown	{90150000-0117-0409-1000-0000000FF1CE}	Microsoft Corporation	2015-04-11
Microsoft DCF MUI (English) 2013	15.0.4569.1506	Unknown	{90150000-0090-0409-1000-0000000FF1CE}	Microsoft Corporation	2015-04-11
Microsoft Excel MUI (English) 2013	15.0.4569.1506	Unknown	{90150000-0016-0409-1000-0000000FF1CE}	Microsoft Corporation	2015-04-15
Microsoft Groove MUI (English) 2013	15.0.4569.1506	Unknown	{90150000-00BA-0409-1000-0000000FF1CE}	Microsoft Corporation	2015-04-15
Microsoft InfoPath MUI (English) 2013	15.0.4569.1506	Unknown	{90150000-0044-0409-1000-0000000FF1CE}	Microsoft Corporation	2015-04-11
Microsoft Lync MUI (English) 2013	15.0.4569.1506	Unknown	{90150000-012B-0409-1000-0000000FF1CE}	Microsoft Corporation	2015-04-20
Microsoft Office 32-bit Components 2013	15.0.4569.1506	Unknown	{90150000-00C1-0000-1000-0000000FF1CE}	Microsoft Corporation	2015-04-20
Microsoft Office OSM MUI (English) 2013	15.0.4569.1506	Unknown	{90150000-00E1-0409-1000-0000000FF1CE}	Microsoft Corporation	2015-04-11
Microsoft Office OSM UX MUI (English) 2013	15.0.4569.1506	Unknown	{90150000-00E2-0409-1000-0000000FF1CE}	Microsoft Corporation	2015-04-11
Microsoft Office Professional Plus 2013	15.0.4569.1506	Unknown	{90150000-0011-0000-1000-0000000FF1CE}	Microsoft Corporation	2015-04-20
Microsoft Office Proofing (English) 2013	15.0.4569.1506	Unknown	{90150000-002C-0409-1000-0000000FF1CE}	Microsoft Corporation	2015-04-11
Microsoft Office Proofing Tools 2013 - English	15.0.4569.1506	Unknown	{90150000-001F-0409-1000-0000000FF1CE}	Microsoft Corporation	2015-04-15
Microsoft Office Proofing Tools 2013 - Español [spanish (spain, international sort)]	15.0.4569.1506	Unknown	{90150000-001F-0C0A-1000-0000000FF1CE}	Microsoft Corporation	2015-04-15
Microsoft Office Shared 32-bit MUI (English) 2013	15.0.4569.1506	Unknown	{90150000-00C1-0409-1000-0000000FF1CE}	Microsoft Corporation	2015-04-15

Microsoft Office Shared MUI (English) 2013	15.0.4569.1506	Unknown	{90150000-006E-0409-1000-0000000FF1CE}	Microsoft Corporation	2015-04-19
Microsoft Office Shared Setup Metadata MUI (English) 2013	15.0.4569.1506	Unknown	{90150000-0115-0409-1000-0000000FF1CE}	Microsoft Corporation	2015-04-11
Microsoft OneNote MUI (English) 2013	15.0.4569.1506	Unknown	{90150000-00A1-0409-1000-0000000FF1CE}	Microsoft Corporation	2015-04-19
Microsoft Outlook MUI (English) 2013	15.0.4569.1506	Unknown	{90150000-001A-0409-1000-0000000FF1CE}	Microsoft Corporation	2015-04-15
Microsoft PowerPoint MUI (English) 2013	15.0.4569.1506	Unknown	{90150000-0018-0409-1000-0000000FF1CE}	Microsoft Corporation	2015-04-15
Microsoft Publisher MUI (English) 2013	15.0.4569.1506	Unknown	{90150000-0019-0409-1000-0000000FF1CE}	Microsoft Corporation	2015-04-11
Microsoft Visual C++ 2010 x64 Redistributable - 10.0.40219	10.0.40219	Unknown	{1D8E6291-B0D5-35EC-8441-6616F567A0F7}	Microsoft Corporation	2015-04-11
Microsoft Visual C++ 2010 x86 Redistributable - 10.0.40219	10.0.40219	Unknown	{F0C3E5D1-1ADE-321E-8167-68EF0DE699A5}	Microsoft Corporation	2015-04-11
Microsoft Visual Studio 2010 Tools for Office Runtime (x64)	10.0.50903	Unknown	Microsoft Visual Studio 2010 Tools for Office Runtime (x64)	Microsoft Corporation	
Microsoft Visual Studio 2010 Tools for Office Runtime (x64)	10.0.50908	Unknown	{9495AEB4-AB97-39DE-8C42-806EEF75ECA7}	Microsoft Corporation	2015-04-11
Microsoft Word MUI (English) 2013	15.0.4569.1506	Unknown	{90150000-001B-0409-1000-0000000FF1CE}	Microsoft Corporation	2015-04-15
Outils de vérification linguistique 2013 de Microsoft Office - Français [french (france)]	15.0.4569.1506	Unknown	{90150000-001F-040C-1000-0000000FF1CE}	Microsoft Corporation	2015-04-15
PerformanceTest v8.0	8.0.1046.0	Unknown	PerformanceTest 8_is1	Passmark Software	2015-04-24
SAMSUNG USB Driver for Mobile Phones	1.5.45.0	Unknown	{D0795B21-0CDA-4a92-AB9E-6E92D8111E44}	SAMSUNG Electronics Co., Ltd.	
Security Update for Microsoft Office 2013 (KB2910941) 64-Bit Edition		Unknown	{90150000-0011-0000-1000-0000000FF1CE}_Office15.PROPLUS_{43ECCB82-45DF-4800-8930-0689BF91F765}	Microsoft	
Security Update for Microsoft Word 2013 (KB2965224) 64-Bit Edition		Unknown	{90150000-012B-0409-1000-0000000FF1CE}_Office15.PROPLUS_{CAFFE1BB-5EB9-413A-B84A-65F01EAF7C15}	Microsoft	
Service Pack 1 for Microsoft Office 2013 (KB2850036) 64-Bit Edition		Unknown	{90150000-012B-0409-1000-0000000FF1CE}_Office15.PROPLUS_{6227D1A8-9E29-463F-8DE6-1CFA1FFF8ECE}	Microsoft	
Start Menu 8	2.1.0	Unknown	IObit_StartMenu8_is1	IObit	2015-04-11
Universal Extractor 1.6.1	1.6.1	Unknown	Universal Extractor_is1	Jared Breland	2015-04-27
Update for Microsoft Access 2013 (KB2965276) 64-Bit Edition		Unknown	{90150000-0015-0409-1000-0000000FF1CE}_Office15.PROPLUS_{62C59657-4920-48B6-B802-7FD75FFA6A48}	Microsoft	
Update for Microsoft Excel 2013 (KB2965275) 64-Bit Edition		Unknown	{90150000-00C1-0409-1000-0000000FF1CE}_Office15.PROPLUS_{F1E55CDA-F069-414A-9257-C59E4DBFA091}	Microsoft	
Update for Microsoft Lync 2013 (KB2889923) 64-Bit Edition		Unknown	{90150000-012B-0409-1000-0000000FF1CE}_Office15.PROPLUS_{DCCD390F-B9A0-4EC0-B903-942608CF4093}	Microsoft	
Update for Microsoft Office 2013 (KB2760249) 64-Bit Edition		Unknown	{90150000-0011-0000-1000-0000000FF1CE}_Office15.PROPLUS_{7A4AB8E1-C091-4BD3-B308-844BA6EE752A}	Microsoft	
Update for Microsoft Office 2013 (KB2760344) 64-Bit Edition		Unknown	{90150000-0011-0000-1000-0000000FF1CE}_Office15.PROPLUS_{EF77B4A6-DFEC-4010-A87D-9B6BF87FABEC}	Microsoft	
Update for Microsoft Office 2013 (KB2760371) 64-Bit Edition		Unknown	{90150000-0011-0000-1000-0000000FF1CE}_Office15.PROPLUS_{25DEA344-FF6F-41BD-B88F-5242BB8E80E1}	Microsoft	
Update for Microsoft Office 2013 (KB2760544) 64-Bit			{90150000-0011-0000-1000-		

Edition	Unknown	0000000FF1CE}_Office15.PROPLUS_{62857CDD-2985-4939-91BA-19ED0B0031A5}
Update for Microsoft Office 2013 (KB2768012) 64-Bit Edition	Unknown	{90150000-0011-0000-1000-0000000FF1CE}_Office15.PROPLUS_{0814662C-FD28-4DE0-ACE5-EE50D1D6C8FB}
Update for Microsoft Office 2013 (KB2825678) 64-Bit Edition	Unknown	{90150000-0011-0000-1000-0000000FF1CE}_Office15.PROPLUS_{978D704B-AF50-405A-BBDA-B2E480CC5D3E}
Update for Microsoft Office 2013 (KB2837654) 64-Bit Edition	Unknown	{90150000-0011-0000-1000-0000000FF1CE}_Office15.PROPLUS_{2147FFF7-71C4-4306-AFE2-1AA7A6025BB1}
Update for Microsoft Office 2013 (KB2880478) 64-Bit Edition	Unknown	{90150000-0011-0000-1000-0000000FF1CE}_Office15.PROPLUS_{8116ED50-F1E7-49E1-9D8D-421497D34B0F}
Update for Microsoft Office 2013 (KB2880487) 64-Bit Edition	Unknown	{90150000-0011-0000-1000-0000000FF1CE}_Office15.PROPLUS_{76379D52-B506-4634-8404-8E1718DF1430}
Update for Microsoft Office 2013 (KB2880977) 64-Bit Edition	Unknown	{90150000-0011-0000-1000-0000000FF1CE}_Office15.PROPLUS_{3FF26B00-AC61-487F-B03B-5D83415C5408}
Update for Microsoft Office 2013 (KB2881001) 64-Bit Edition	Unknown	{90150000-0011-0000-1000-0000000FF1CE}_Office15.PROPLUS_{DF1B7B95-4A86-4605-A628-556394B5580A}
Update for Microsoft Office 2013 (KB2881035) 64-Bit Edition	Unknown	{90150000-0090-0409-1000-0000000FF1CE}_Office15.PROPLUS_{885C981B-F1E3-430A-A099-31CA9D28C251}
Update for Microsoft Office 2013 (KB2883036) 64-Bit Edition	Unknown	{90150000-0011-0000-1000-0000000FF1CE}_Office15.PROPLUS_{E919ACF4-A1D7-4CAA-A103-5EB115563721}
Update for Microsoft Office 2013 (KB2883095) 64-Bit Edition	Unknown	{90150000-0011-0000-1000-0000000FF1CE}_Office15.PROPLUS_{EADBF225-163E-406B-B11A-26ECCCAB5A0E}
Update for Microsoft Office 2013 (KB2899498) 64-Bit Edition	Unknown	{90150000-0016-0409-1000-0000000FF1CE}_Office15.PROPLUS_{D7FAA622-6BCF-4EDF-8C34-A48E1838D57B}
Update for Microsoft Office 2013 (KB2899522) 64-Bit Edition	Unknown	{90150000-0011-0000-1000-0000000FF1CE}_Office15.PROPLUS_{A4E88D96-814F-4183-8DB2-BA3EC2B7E434}
Update for Microsoft Office 2013 (KB2920754) 64-Bit Edition	Unknown	{90150000-0011-0000-1000-0000000FF1CE}_Office15.PROPLUS_{2513C305-E7E9-46F9-BECA-C6AC02D769B3}
Update for Microsoft Office 2013 (KB2920769) 64-Bit Edition	Unknown	{90150000-0011-0000-1000-0000000FF1CE}_Office15.PROPLUS_{C906EC6B-8610-487F-8528-658FE2575C86}
Update for Microsoft Office 2013 (KB2956154) 64-Bit Edition	Unknown	{90150000-0011-0000-1000-0000000FF1CE}_Office15.PROPLUS_{8AB3858C-5246-4C78-937F-86A38A494CAA}
Update for Microsoft Office 2013 (KB2956169) 64-Bit Edition	Unknown	{90150000-0011-0000-1000-0000000FF1CE}_Office15.PROPLUS_{B5A6B49E-30F3-4D1D-8F9C-E53712D30996}
Update for Microsoft Office 2013 (KB2956171) 64-Bit Edition	Unknown	{90150000-0011-0000-1000-0000000FF1CE}_Office15.PROPLUS_{A3DC29E8-0E97-448A-B9C0-9086CB8B3E86}
Update for Microsoft Office 2013 (KB2956177) 64-Bit Edition	Unknown	{90150000-00C1-0000-1000-0000000FF1CE}_Office15.PROPLUS_{3F8EF29A-A7F8-48B0-BA19-01D0B88AB1B7}
Update for Microsoft Office 2013 (KB2965218) 64-Bit Edition	Unknown	{90150000-00C1-0000-1000-0000000FF1CE}_Office15.PROPLUS_{C326AAF2-6DE4-4ABC-9C3D-7E4B31E772C2}
Update for Microsoft Office 2013 (KB2965255) 64-Bit Edition	Unknown	{90150000-0011-0000-1000-0000000FF1CE}_Office15.PROPLUS_{6091607B-2689-4A09-B14A-65907BBAE202}

Update for Microsoft Office 2013 (KB2965262) 64-Bit Edition		Unknown	{90150000-006E-0409-1000-0000000FF1CE}_Office15.PROPLUS_{D99CCEA8-CBD6-4800-8805-535A99AFC8BC}	Microsoft
Update for Microsoft Office 2013 (KB2965267) 64-Bit Edition		Unknown	{90150000-00C1-0000-1000-0000000FF1CE}_Office15.PROPLUS_{A64A29C8-BB35-4FC5-84D6-6D1C6B2BB59F}	Microsoft
Update for Microsoft Office 2013 (KB2965268) 64-Bit Edition		Unknown	{90150000-001F-0C0A-1000-0000000FF1CE}_Office15.PROPLUS_{7DD1A269-36B9-4C80-AD80-11C4E42A0B96}	Microsoft
Update for Microsoft OneDrive for Business (KB2956185) 64-Bit Edition		Unknown	{90150000-00C1-0409-1000-0000000FF1CE}_Office15.PROPLUS_{171E6E09-C2A5-432E-85A4-C19136E59BCE}	Microsoft
Update for Microsoft OneNote 2013 (KB2965264) 64-Bit Edition		Unknown	{90150000-00C1-0000-1000-0000000FF1CE}_Office15.PROPLUS_{537DB67E-C616-45F0-BC92-C8E3AC7D16EF}	Microsoft
Update for Microsoft Outlook 2013 (KB2965270) 64-Bit Edition		Unknown	{90150000-001A-0409-1000-0000000FF1CE}_Office15.PROPLUS_{B4FE3F01-A94B-44F5-8142-C9522B537443}	Microsoft
Update for Microsoft Outlook Social Connector 2013 (KB2965257) 64-Bit Edition		Unknown	{90150000-001A-0409-1000-0000000FF1CE}_Office15.PROPLUS_{292F3133-E3A4-40EB-9044-D63C09FB9F2D}	Microsoft
Update for Microsoft PowerPoint 2013 (KB2965256) 64-Bit Edition		Unknown	{90150000-0018-0409-1000-0000000FF1CE}_Office15.PROPLUS_{F6542279-5D7F-42DA-B213-E7FD11597B03}	Microsoft
Update for Microsoft Project 2013 (KB2965279) 64-Bit Edition		Unknown	{90150000-00C1-0000-1000-0000000FF1CE}_Office15.PROPLUS_{0CDCFFFE-0E55-4C46-9B09-8CB5D0F38566}	Microsoft
Update for Microsoft Publisher 2013 (KB2883048) 64-Bit Edition		Unknown	{90150000-0019-0409-1000-0000000FF1CE}_Office15.PROPLUS_{F24DFA32-C8EE-4AFB-89AB-07EE7A52E414}	Microsoft
Update for Microsoft Visio Viewer 2013 (KB2817301) 64-Bit Edition		Unknown	{90150000-006E-0409-1000-0000000FF1CE}_Office15.PROPLUS_{8E5CD68A-CDF8-4930-88DF-B7778B1871A9}	Microsoft
Update for Microsoft Word 2013 (KB2878319) 64-Bit Edition		Unknown	{90150000-0011-0000-1000-0000000FF1CE}_Office15.PROPLUS_{BC51FE30-3A56-4802-8D9E-E9BC05B56B49}	Microsoft
Update for Skype for Business 2015 (KB2889853) 64-Bit Edition		Unknown	{90150000-012B-0409-1000-0000000FF1CE}_Office15.PROPLUS_{40930C8E-A677-414C-A72F-DFDEB10738FB}	Microsoft
VLC media player	2.2.0	Unknown	VLC media player	VideoLAN
WinRAR 5.21 (64-bit)	5.21.0	Unknown	WinRAR archiver	win.rar GmbH

Licenses

Software	Product Key
Microsoft Internet Explorer 9.11.9600.17728	
Microsoft Office Professional Plus 2013	YC7DK-G2NP3-2QQC3-J6H88-GVGXT
Microsoft Windows 8.1 Professional	

File Types

Extension	File Type Description	Content Type
001	Universal Extractor Archive	
386	Virtual Device Driver	
3G2	3GPP2 Audio/Video	video/3gpp2

3GA	VLC media file (.3ga)	
3GP	3GPP Audio/Video	video/3gpp
3GP2	VLC media file (.3gp2)	video/3gpp2
3GPP	3GPP Audio/Video	video/3gpp
669	VLC media file (.669)	
7Z	WinRAR archive	
A52	VLC media file (.a52)	
AAC	ADTS Audio	audio/vnd.dlna.adts
AC3	VLC media file (.ac3)	audio/vnd.dolby.dd-raw
ACCDA	Microsoft Access Add-in	application/msaccess.addin
ACCDB	Microsoft Access Database	application/msaccess
ACCDC	Microsoft Access Signed Package	application/msaccess.cab
ACCDE	Microsoft Access ACCDE Database	application/msaccess.exec
ACCDR	Microsoft Access Runtime Application	application/msaccess.runtime
ACCDT	Microsoft Access Template	application/msaccess.template
ACCDU	Microsoft Access Add-in Data	
ACCDW	Microsoft Access Web Application	application/msaccess.webapplication
ACCFT	Microsoft Access Template	application/msaccess.ftemplate
ACCOUNTPICTURE-MS	Account Picture File	application/windows-accountpicture
ACE	WinRAR archive	
ACL	AutoCorrect List File	
ADE	Microsoft Access Project Extension	application/msaccess
ADN	Microsoft Access Blank Project Template	
ADP	Microsoft Access Project	application/msaccess
ADT	ADTS Audio	audio/vnd.dlna.adts
ADTS	ADTS Audio	audio/vnd.dlna.adts
AIF	VLC media file (.aif)	audio/aiff
AIFC	VLC media file (.aifc)	audio/aiff
AIFF	VLC media file (.aiff)	audio/aiff
AMR	VLC media file (.amr)	
AMV	VLC media file (.amv)	
ANI	Animated Cursor	
AOB	VLC media file (.aob)	
APE	VLC media file (.ape)	
APPCONTENT-MS	Application Content	application/windows-appcontent+xml
APPLICATION	Application Manifest	application/x-ms-application
APPREF-MS	Application Reference	
ARC	Universal Extractor Archive	
ARJ	WinRAR archive	
ASA	ASA File	
ASF	VLC media file (.asf)	video/x-ms-asf
ASP	ASP File	
ASX	VLC media file (.asx)	video/x-ms-asf
AU	VLC media file (.au)	audio/basic
AVI	Video Clip	video/avi
AW	Answer Wizard File	
B4S	VLC media file (.b4s)	
BAT	Windows Batch File	
BIK	VLC media file (.bik)	
BLG	Performance Monitor File	
BMP	Bitmap Image	image/bmp
BZ	WinRAR archive	
BZ2	WinRAR archive	
CAB	WinRAR archive	

CAF	VLC media file (.caf)	
CAMP	WCS Viewing Condition Profile	
CAT	Security Catalog	application/vnd.ms-pki.seccat
CDA	VLC media file (.cda)	
CDMP	WCS Device Profile	
CDX	CDX File	
CDXML	CDXML File	
CER	Security Certificate	application/x-x509-ca-cert
CHK	Recovered File Fragments	
CHM	Compiled HTML Help file	
CMD	Windows Command Script	
COM	MS-DOS Application	
COMPOSITEFONT	Composite Font File	
CONTACT	Contact File	text/x-ms-contact
CPIO	Universal Extractor Archive	
CPL	Control Panel Item	
CRL	Certificate Revocation List	application/pkix-crl
CRT	Security Certificate	application/x-x509-ca-cert
CRTX	Microsoft Office Chart Template	
CSS	Cascading Style Sheet Document	text/css
CSV	Microsoft Excel Comma Separated Values File	application/vnd.ms-excel
CUE	VLC media file (.cue)	
CUR	Cursor	
DB	Data Base File	
DBX	Universal Extractor Archive	
DCTX	Open Extended Dictionary	
DCTXC	Open Extended Dictionary	
DDS	DDS Image	image/vnd.ms-dds
DEB	Universal Extractor Archive	
DER	Security Certificate	application/x-x509-ca-cert
DESKLINK	Desktop Shortcut	
DESKTHEMEPACK	Windows Desktop Theme Pack	
DET	Office Data File	
DIAGCAB	Diagnostic Cabinet	
DIAGCFG	Diagnostic Configuration	
DIAGPKG	Diagnostic Document	
DIB	Bitmap Image	image/bmp
DIC	Text Document	
DLL	Application Extension	application/x-msdownload
DOC	Microsoft Word 97 - 2003 Document	application/msword
DOCHTML	Microsoft Word HTML Document	
DOCM	Microsoft Word Macro-Enabled Document	application/vnd.ms-word.document.macroEnabled.12
DOCMHTML	DOCMHTML File	
DOCX	Microsoft Word Document	application/vnd.openxmlformats-officedocument.wordprocessingml.document
DOCXML	Microsoft Word XML Document	
DOT	Microsoft Word 97 - 2003 Template	application/msword
DOTHTML	Microsoft Word HTML Template	
DOTM	Microsoft Word Macro-Enabled Template	application/vnd.ms-word.template.macroEnabled.12
DOTX	Microsoft Word Template	application/vnd.openxmlformats-officedocument.wordprocessingml.template
DQY	Microsoft Excel ODBC Query File	
DRC	VLC media file (.drc)	
DRV	Device Driver	
DSN	Microsoft OLE DB Provider for ODBC Drivers	
DTS	VLC media file (.dts)	

DV	VLC media file (.dv)	
DWFX	XPS Document	model/vnd.dwfx+xps
EASMX	XPS Document	model/vnd.easmx+xps
EDRWX	XPS Document	model/vnd.edrwx+xps
ELM	Microsoft Office Themes File	
EMF	EMF File	image/x-emf
EML	E-mail Message	
EPRTX	XPS Document	model/vnd.eprtx+xps
EVT	EVT File	
EVTX	EVTX File	
EXC	Text Document	
EXE	Application	application/x-msdownload
F4V	VLC media file (.f4v)	
FDM	Outlook Form Definition	
FLAC	VLC media file (.flac)	
FLV	VLC media file (.flv)	
FON	Font file	
GCSX	Microsoft Office SmartArt Graphic Color Variation	
GFE	Glary Utilities Encrypted File	
GFS	Glary Utilities Splitted File	
GIF	GIF Image	image/gif
GLOX	Microsoft Office SmartArt Graphic Layout	
GMMP	WCS Gamut Mapping Profile	
GQSX	Microsoft Office SmartArt Graphic Quick Style	
GRA	Microsoft Graph Chart	
GROUP	Contact Group File	text/x-ms-group
GRP	Microsoft Program Group	
GVI	VLC media file (.gvi)	
GXF	VLC media file (.gxf)	
GZ	WinRAR archive	
HLP	Help File	
HOL	Outlook Holidays	
HTA	HTML Application	application/hta
HTM	HTML Document	text/html
HTML	HTML Document	text/html
HXA	Microsoft Help Attribute Definition File	application/xml
HXC	Microsoft Help Collection Definition File	application/xml
HXD	Microsoft Help Validator File	application/octet-stream
HXE	Microsoft Help Samples Definition File	application/xml
HXF	Microsoft Help Include File	application/xml
HXH	Microsoft Help Merged Hierarchy File	application/octet-stream
HXI	Microsoft Help Compiled Index File	application/octet-stream
HXK	Microsoft Help Index File	application/xml
HXQ	Microsoft Help Merged Query Index File	application/octet-stream
HXR	Microsoft Help Merged Attribute Index File	application/octet-stream
HXS	Microsoft Help Compiled Storage File	application/octet-stream
HXT	Microsoft Help Table of Contents File	application/xml
HXV	Microsoft Help Virtual Topic Definition File	application/xml
HXW	Microsoft Help Attribute Definition File	application/octet-stream
ICC	ICC Profile	
ICL	Icon Library	
ICM	ICC Profile	
ICO	Icon	image/x-icon
ICS	iCalendar File	text/calendar

IFO	VLC media file (.ifo)	
IGP	Intel Graphics Profiles	
IMESX	IME Search provider definition	
IMG	Disc Image File	
INF	Setup Information	
INFOPATHXML	Microsoft InfoPath Form	application/ms-infopath.xml
INI	Configuration Settings	
IQY	Microsoft Excel Web Query File	text/x-ms-iqy
ISO	Disc Image File	
IT	VLC media file (.it)	
JAR	Universal Extractor Archive	
JFIF	JPEG Image	image/jpeg
JNT	Journal Document	
JOB	Task Scheduler Task Object	
JOD	Microsoft.Jet.OLEDB.4.0	
JPE	JPEG Image	image/jpeg
JPEG	JPEG Image	image/jpeg
JPG	JPEG Image	image/jpeg
JS	JavaScript File	
JSE	JScript Encoded File	
JTP	Journal Template	
JTX	XPS Document	application/x-jtx+xps
JXR	Windows Media Photo	image/vnd.ms-photo
KGB	Universal Extractor Archive	
KGE	Universal Extractor Archive	
LABEL	Property List	
LACCDB	Microsoft Access Record-Locking Information	
LDB	Microsoft Access Record-Locking Information	
LEX	Dictionary File	
LHA	WinRAR archive	
LIBRARY-MS	Library Folder	application/windows-library+xml
LIT	Universal Extractor Archive	
LNK	Shortcut	
LOG	Text Document	
LZH	WinRAR archive	
LZO	Universal Extractor Archive	
M1V	VLC media file (.m1v)	video/mpeg
M2T	AVCHD Video	video/vnd.dlna.mpeg-tts
M2TS	AVCHD Video	video/vnd.dlna.mpeg-tts
M2V	VLC media file (.m2v)	video/mpeg
M3U	M3U file	audio/x-mpegurl
M3U8	VLC media file (.m3u8)	
M4A	MPEG-4 Audio	audio/mp4
M4P	VLC media file (.m4p)	
M4V	MP4 Video	video/mp4
MAD	Microsoft Access Module Shortcut	
MAF	Microsoft Access Form Shortcut	
MAG	Microsoft Access Diagram Shortcut	
MAM	Microsoft Access Macro Shortcut	
MAPIMAIL	Mail Service	
MAQ	Microsoft Access Query Shortcut	
MAR	Microsoft Access Report Shortcut	
MAS	Microsoft Access Stored Procedure Shortcut	
MAT	Microsoft Access Table Shortcut	

MAU	MAU File	
MAV	Microsoft Access View Shortcut	
MAW	Microsoft Access Data Access Page Shortcut	
MDA	Microsoft Access Add-in	application/msaccess
MDB	Microsoft Access Database	application/msaccess
MDBHTML	Microsoft Access HTML Document	
MDE	Microsoft Access MDE Database	application/msaccess
MDN	Microsoft Access Blank Database Template	
MDT	Microsoft Access Add-in Data	
MDW	Microsoft Access Workgroup Information	
MFP	Macromedia Flash Paper	application/x-shockwave-flash
MHT	MHTML Document	message/rfc822
MHTML	MHTML Document	message/rfc822
MID	VLC media file (.mid)	audio/mid
MIDI	MIDI Sequence	audio/mid
MIG	Migration Store	
MKA	VLC media file (.mka)	
MLC	Language Pack File_	
MLP	VLC media file (.mlp)	
MOD	Movie Clip	video/mpeg
MOV	QuickTime Movie	video/quicktime
MP1	VLC media file (.mp1)	
MP2	MP3 Format Sound	audio/mpeg
MP2V	VLC media file (.mp2v)	video/mpeg
MP3	MP3 Format Sound	audio/mpeg
MP4	MP4 Video	video/mp4
MP4V	MP4 Video	video/mp4
MPA	Movie Clip	audio/mpeg
MPC	VLC media file (.mpc)	
MPE	Movie Clip	video/mpeg
MPEG	Movie Clip	video/mpeg
MPEG1	VLC media file (.mpeg1)	
MPEG2	VLC media file (.mpeg2)	
MPEG4	VLC media file (.mpeg4)	
MPG	Movie Clip	video/mpeg
MPGA	VLC media file (.mpga)	
MPV2	Movie Clip	video/mpeg
MSC	Microsoft Common Console Document	
MSG	Outlook Item	
MSI	Windows Installer Package	
MS-ONE-STUB	Microsoft OneNote Stub	
MSP	Windows Installer Patch	
MSRCINCIDENT	Windows Remote Assistance Invitation	
MSSTYLES	Windows Visual Style File	
MSU	Microsoft Update Standalone Package	
MTS	AVCHD Video	video/vnd.dlna.mpeg-tts
MTV	VLC media file (.mtv)	
MXF	VLC media file (.mxf)	
MYDOCS	MyDocs Drop Target	
NFO	MSInfo Configuration File	
NK2	Outlook Nickname File	
NSV	VLC media file (.nsv)	
NUV	VLC media file (.nuv)	
OCX	ActiveX control	

ODC	Microsoft Office Data Connection	text/x-ms-odc
ODCCUBEFILE	ODCCUBEFILE File	
ODCDATABASEFILE	ODCDATABASEFILE File	
ODCNEWFILE	ODCNEWFILE File	
ODCTABLECOLLECTIONFILE	ODCTABLECOLLECTIONFILE File	
ODCTABLEFILE	ODCTABLEFILE File	
ODP	OpenDocument Presentation	application/vnd.oasis.opendocument.presentation
ODS	OpenDocument Spreadsheet	application/vnd.oasis.opendocument.spreadsheet
ODT	OpenDocument Text	application/vnd.oasis.opendocument.text
OFS	Outlook Form Regions	
OFT	Outlook Item Template	
OGA	VLC media file (.oga)	
OGG	VLC media file (.ogg)	
OGM	VLC media file (.ogm)	
OGV	VLC media file (.ogv)	
OGX	VLC media file (.ogx)	
OLS	Office List Shortcut	application/vnd.ms-publisher
OMA	VLC media file (.oma)	
ONE	Microsoft OneNote Section	application/msonenote
ONEPKG	Microsoft OneNote Single File Package	application/msonenote
ONETOC	Microsoft OneNote 2003 Table Of Contents	
ONETOC2	Microsoft OneNote Table Of Contents	
OPC	Microsoft Clean-up Wizard File	
OPUS	VLC media file (.opus)	
OQY	Microsoft Excel OLAP Query File	
OSDX	OpenSearch Description File	application/opensearchdescription+xml
OST	Outlook Data File	
OTF	OpenType Font file	
OTM	Outlook VBA Project File	
OXPS	XPS Document	
P10	Certificate Request	application/pkcs10
P12	Personal Information Exchange	application/x-pkcs12
P7B	PKCS #7 Certificates	application/x-pkcs7-certificates
P7C	Digital ID File	application/pkcs7-mime
P7M	PKCS #7 MIME Message	application/pkcs7-mime
P7R	Certificate Request Response	application/x-pkcs7-certreqresp
P7S	PKCS #7 Signature	application/pkcs7-signature
PAB	Outlook Personal Address Book	
PANO	PANO File	application/vnd.ms-pano
PBK	Dial-Up Phonebook	
PCB	PCB File	
PEA	Universal Extractor Archive	
PERFMONCFG	Performance Monitor Configuration	
PFM	Type 1 Font file	
PFX	Personal Information Exchange	application/x-pkcs12
PIF	Shortcut to MS-DOS Program	
PKO	Public Key Security Object	application/vnd.ms-pki.pko
PLS	VLC media file (.pls)	
PNF	Precompiled Setup Information	
PNG	PNG Image	image/png
POT	Microsoft PowerPoint 97-2003 Template	application/vnd.ms-powerpoint
POTHTML	Microsoft PowerPoint HTML Template	
POTM	Microsoft PowerPoint Macro-Enabled Design Template	application/vnd.ms-powerpoint.template.macroEnabled.12
POTX	Microsoft PowerPoint Template	application/vnd.openxmlformats-officedocument.presentationml.template

PPA	Microsoft PowerPoint 97-2003 Addin	application/vnd.ms-powerpoint
PPAM	Microsoft PowerPoint Addin	application/vnd.ms-powerpoint.addin.macroEnabled.12
PPS	Microsoft PowerPoint 97-2003 Slide Show	application/vnd.ms-powerpoint
PPSM	Microsoft PowerPoint Macro-Enabled Slide Show	application/vnd.ms-powerpoint.slideshow.macroEnabled.12
PPSX	Microsoft PowerPoint Slide Show	application/vnd.openxmlformats-officedocument.presentationml.slideshow
PPT	Microsoft PowerPoint 97-2003 Presentation	application/vnd.ms-powerpoint
PPTHTML	Microsoft PowerPoint HTML Document	
PPTM	Microsoft PowerPoint Macro-Enabled Presentation	application/vnd.ms-powerpoint.presentation.macroEnabled.12
PPTMHTML	PPTMHTML File	
PPTX	Microsoft PowerPoint Presentation	application/vnd.openxmlformats-officedocument.presentationml.presentation
PPTXML	Microsoft PowerPoint XML Presentation	
PRF	PICS Rules File	application/pics-rules
PRINTEREXPORT	Printer Migration File	
PS1	PS1 File	
PS1XML	PS1XML File	
PSC1	PSC1 File	application/PowerShell
PSD1	PSD1 File	
PSM1	PSM1 File	
PSSC	PSSC File	
PST	Outlook Data File	
PT	PerformanceTest Baseline	
PTX	PerformanceTest Baseline	
PUB	Microsoft Publisher Document	application/vnd.ms-publisher
PUBHTML	PUBHTML File	
PUBMHTML	PUBMHTML File	
PWZ	Microsoft PowerPoint Wizard	application/vnd.ms-powerpoint
QCP	VLC media file (.qcp)	
QDS	Directory Query	
R00	WinRAR archive	
R01	WinRAR archive	
R02	WinRAR archive	
R03	WinRAR archive	
R04	WinRAR archive	
R05	WinRAR archive	
R06	WinRAR archive	
R07	WinRAR archive	
R08	WinRAR archive	
R09	WinRAR archive	
R10	WinRAR archive	
R11	WinRAR archive	
R12	WinRAR archive	
R13	WinRAR archive	
R14	WinRAR archive	
R15	WinRAR archive	
R16	WinRAR archive	
R17	WinRAR archive	
R18	WinRAR archive	
R19	WinRAR archive	
R20	WinRAR archive	
R21	WinRAR archive	
R22	WinRAR archive	
R23	WinRAR archive	
R24	WinRAR archive	
R25	WinRAR archive	

R26	WinRAR archive	
R27	WinRAR archive	
R28	WinRAR archive	
R29	WinRAR archive	
RA	VLC media file (.ra)	
RAM	VLC media file (.ram)	
RAR	WinRAR archive	
RAT	Rating System File	application/rat-file
RDP	Remote Desktop Connection	
REC	VLC media file (.rec)	
REG	Registration Entries	
RELS	XML Document	
RESMONCFG	Resource Monitor Configuration	
REV	RAR recovery volume	
RLE	RLE File	
RLL	Application Extension	
RM	VLC media file (.rm)	
RMI	VLC media file (.rmi)	audio/mid
RMVB	VLC media file (.rmvb)	
RPL	VLC media file (.rpl)	
RPM	Universal Extractor Archive	
RQY	Microsoft Excel OLE DB Query File	text/x-ms-rqy
RTF	Rich Text Format	application/msword
S3M	VLC media file (.s3m)	
SCF	File Explorer Command	
SCP	Text Document	
SCR	Screen saver	
SCT	Windows Script Component	text/scriptlet
SDP	VLC media file (.sdp)	
SEARCHCONNECTOR-MS	Search Connector Folder	application/windows-search-connector+xml
SEARCH-MS	Saved Search	
SENDTOBLUETOOTH	Send To Bluetooth	
SETTINGCONTENT-MS	Setting Content	
SFCACHE	ReadyBoost Cache File	
SIT	Universal Extractor Archive	application/x-stuffit
SLDM	Microsoft PowerPoint Macro-Enabled Slide	application/vnd.ms-powerpoint.slide.macroEnabled.12
SLDX	Microsoft PowerPoint Slide	application/vnd.openxmlformats-officedocument.presentationml.slide
SLK	Microsoft Excel SLK Data Import Format	application/vnd.ms-excel
SND	VLC media file (.snd)	audio/basic
SPC	PKCS #7 Certificates	application/x-pkcs7-certificates
SPL	Shockwave Flash Object	application/futuresplash
SPX	VLC media file (.spx)	
SST	Microsoft Serialized Certificate Store	application/vnd.ms-pki.certstore
SVG	SVG Document	image/svg+xml
SWF	Shockwave Flash Object	application/x-shockwave-flash
SYMLINK	.symlink	
SYS	System file	
TAR	WinRAR archive	
TAZ	WinRAR archive	
TBZ	WinRAR archive	
TBZ2	WinRAR archive	
TGZ	WinRAR archive	
THEME	Windows Theme File	
THEMEPACK	Windows Theme Pack	

THMX	Microsoft Office Theme	application/vnd.ms-officetheme
THP	VLC media file (.thp)	
TIF	TIF File	image/tiff
TIFF	TIFF File	image/tiff
TS	MPEG-2 TS Video	video/vnd.dlna.mpeg-tts
TTA	VLC media file (.tta)	
TTC	TrueType Collection Font file	
TTF	TrueType Font file	
TTS	MPEG-2 TS Video	video/vnd.dlna.mpeg-tts
TXT	Text Document	text/plain
TXZ	WinRAR archive	
TZ	Universal Extractor Archive	
UDL	Microsoft Data Link	
UHA	Universal Extractor Archive	
URL	URL File	
UU	WinRAR archive	
UUE	WinRAR archive	
UXDC	UXDC File	
VBE	VBScript Encoded File	
VBS	VBScript Script File	
VCF	vCard File	text/x-vcard
VCS	vCalendar File	
VDW	Microsoft Visio Document	application/vnd.ms-visio.viewer
VDX	Microsoft Visio Document	application/vnd.ms-visio.viewer
VHD	Disc Image File	
VHDX	Disc Image File	
VLC	VLC media file (.vlc)	
VLT	VLC skin file (.vlt)	
VOB	VLC media file (.vob)	
VOC	VLC media file (.voc)	
VQF	VLC media file (.vqf)	
VRO	VLC media file (.vro)	
VSD	Microsoft Visio Document	application/vnd.ms-visio.viewer
VSDM	Microsoft Visio Document	application/vnd.ms-visio.viewer
VSDX	Microsoft Visio Document	application/vnd.ms-visio.viewer
VSS	Microsoft Visio Document	application/vnd.ms-visio.viewer
VSSM	Microsoft Visio Document	application/vnd.ms-visio.viewer
VSSX	Microsoft Visio Document	application/vnd.ms-visio.viewer
VST	Microsoft Visio Document	application/vnd.ms-visio.viewer
VSTM	Microsoft Visio Document	application/vnd.ms-visio.viewer
VSTO	VSTO Deployment Manifest	application/x-ms-vsto
VSTX	Microsoft Visio Document	application/vnd.ms-visio.viewer
VSX	Microsoft Visio Document	application/vnd.ms-visio.viewer
VTX	Microsoft Visio Document	application/vnd.ms-visio.viewer
VXD	Virtual Device Driver	
W64	VLC media file (.w64)	
WAB	Address Book File	
WAV	Wave Sound	audio/wav
WAX	Windows Media Audio shortcut	audio/x-ms-wax
WBK	Microsoft Word Backup Document	application/msword
WCX	Workspace Configuration File	
WDP	Windows Media Photo	image/vnd.ms-photo
WEBM	VLC media file (.webm)	
WEBPNP	Web Point And Print File	

WEBSITE	Pinned Site Shortcut	application/x-mswebsite
WIZ	Microsoft Word Wizard	application/msword
WIZHTML	Microsoft Access HTML Template	
WLL	WLL File	
WM	Windows Media Audio/Video file	video/x-ms-wm
WMA	Windows Media Audio file	audio/x-ms-wma
WMD	Windows Media Player Download Package	application/x-ms-wmd
WMDB	Windows Media Library	
WMF	WMF File	image/x-wmf
WMS	Windows Media Player Skin File	
WMV	Windows Media Audio/Video file	video/x-ms-wmv
WMX	Windows Media Audio/Video playlist	video/x-ms-wmx
WMZ	Windows Media Player Skin Package	application/x-ms-wmz
WPL	Windows Media playlist	application/vnd.ms-wpl
WSC	Windows Script Component	text/scriptlet
WSF	Windows Script File	
WSH	Windows Script Host Settings File	
WSZ	VLC skin file (.wsz)	
WTX	Text Document	
WV	VLC media file (.wv)	
WVX	VLC media file (.wvx)	video/x-ms-wvx
XA	VLC media file (.xa)	
XAML	Windows Markup File	application/xaml+xml
XBAP	XAML Browser Application	application/x-ms-xbap
XESC	VLC media file (.xesc)	
XEVGENXML	XEVGENXML File	
XHT	XHTML Document	application/xhtml+xml
XHTML	XHTML Document	application/xhtml+xml
XLA	Microsoft Excel Add-In	application/vnd.ms-excel
XLAM	Microsoft Excel Add-In	application/vnd.ms-excel.addin.macroEnabled.12
XLD	Microsoft Excel 5.0 DialogSheet	application/vnd.ms-excel
XLK	Microsoft Excel Backup File	application/vnd.ms-excel
XLL	Microsoft Excel XLL Add-In	application/vnd.ms-excel
XLM	Microsoft Excel 4.0 Macro	application/vnd.ms-excel
XLS	Microsoft Excel 97-2003 Worksheet	application/vnd.ms-excel
XLSB	Microsoft Excel Binary Worksheet	application/vnd.ms-excel.sheet.binary.macroEnabled.12
XLSHTML	Microsoft Excel HTML Document	
XLSM	Microsoft Excel Macro-Enabled Worksheet	application/vnd.ms-excel.sheet.macroEnabled.12
XLSMHTML	XLSMHTML File	
XLSX	Microsoft Excel Worksheet	application/vnd.openxmlformats-officedocument.spreadsheetml.sheet
XLT	Microsoft Excel Template	application/vnd.ms-excel
XLTHTML	Microsoft Excel HTML Template	
XLTM	Microsoft Excel Macro-Enabled Template	application/vnd.ms-excel.template.macroEnabled.12
XLTX	Microsoft Excel Template	application/vnd.openxmlformats-officedocument.spreadsheetml.template
XLW	Microsoft Excel Workspace	application/vnd.ms-excel
XLXML	Microsoft Excel XML Worksheet	
XM	VLC media file (.xm)	
XML	XML Document	text/xml
XPI	Universal Extractor Archive	
XPS	XPS Document	application/vnd.ms-xpsdocument
XRM-MS	XrML Digital License	text/xml
XSF	Microsoft InfoPath Form Definition File	
XSL	XSL Stylesheet	text/xml
XSN	Microsoft InfoPath Form Template	

XSPF	VLC media file (.xspf)
XTP	Microsoft InfoPath Template Part File
XTP2	Microsoft InfoPath Template Part File
XXE	WinRAR archive
XZ	WinRAR archive
Z	WinRAR archive
ZFSENDTOTARGET	Compressed (zipped) Folder SendTo Target
ZIP	WinRAR ZIP archive

Windows Security

Operating System Properties:

OS Name	Microsoft Windows 8.1 Professional
OS Service Pack	-
Winlogon Shell	explorer.exe
User Account Control (UAC)	Enabled
System Restore	Enabled

Data Execution Prevention (DEP, NX, EDB):

Supported by Operating System	Yes
Supported by CPU	Yes
Active (To Protect Applications)	Yes
Active (To Protect Drivers)	Yes

Windows Update

Update Description	Update Type	Inst. Date
(Automatic Update)	Download:Automatic, Install:Scheduled	Every Day 0:00
Cumulative Security Update for Internet Explorer 11 for Windows 8.1 for x64-based Systems (KB3032359)	Update	4/10/2015
Cumulative Security Update for Internet Explorer 11 for Windows 8.1 for x64-based Systems (KB3038314)	Update	4/15/2015
Definition Update for Microsoft Office 2013 (KB2760587) 64-Bit Edition	Update	4/11/2015
Definition Update for Microsoft Office 2013 (KB2956172) 64-Bit Edition	Update	4/11/2015
Definition Update for Microsoft Office 2013 (KB2965273) 64-Bit Edition	Update	4/15/2015
Definition Update for Windows Defender - KB2267602 (Definition 1.195.2640.0)	Update	4/10/2015
Definition Update for Windows Defender - KB2267602 (Definition 1.195.2815.0)	Update	4/11/2015
Definition Update for Windows Defender - KB2267602 (Definition 1.195.2894.0)	Update	4/11/2015
Definition Update for Windows Defender - KB2267602 (Definition 1.195.3018.0)	Update	4/12/2015
Definition Update for Windows Defender - KB2267602 (Definition 1.195.3163.0)	Update	4/13/2015
Definition Update for Windows Defender - KB2267602 (Definition 1.195.3225.0)	Update	4/14/2015
Definition Update for Windows Defender - KB2267602 (Definition 1.195.3437.0)	Update	4/15/2015
Definition Update for Windows Defender - KB2267602 (Definition 1.195.3761.0)	Update	4/19/2015
Definition Update for Windows Defender - KB2267602 (Definition 1.195.3814.0)	Update	4/20/2015
Definition Update for Windows Defender - KB2267602 (Definition 1.197.155.0)	Update	4/21/2015
Definition Update for Windows Defender - KB2267602 (Definition 1.197.280.0)	Update	4/22/2015
Definition Update for Windows Defender - KB2267602 (Definition 1.197.566.0)	Update	4/24/2015
Definition Update for Windows Defender - KB2267602 (Definition 1.197.652.0)	Update	4/25/2015
Definition Update for Windows Defender - KB2267602 (Definition 1.197.652.0)	Update	4/25/2015
Definition Update for Windows Defender - KB2267602 (Definition 1.197.775.0)	Update	4/27/2015
Definition Update for Windows Defender - KB2267602 (Definition 1.197.775.0)	Update	4/27/2015

Definition Update for Windows Defender - KB2267602 (Definition 1.197.874.0)	Update	4/28/2015
Razer - Input - Razer Copperhead USB Mouse	Update	4/10/2015
Security Update for Internet Explorer Flash Player for Windows 8.1 for x64-based Systems (KB3044132)	Update	4/10/2015
Security Update for Internet Explorer Flash Player for Windows 8.1 for x64-based Systems (KB3049508)	Update	4/15/2015
Security Update for Microsoft .NET Framework 3.5 on Windows 8.1 and Windows Server 2012 R2 for x64-based Systems (KB2894852)	Update	4/12/2015
Security Update for Microsoft .NET Framework 3.5 on Windows 8.1 and Windows Server 2012 R2 for x64-based Systems (KB2966826)	Update	4/12/2015
Security Update for Microsoft .NET Framework 3.5 on Windows 8.1 and Windows Server 2012 R2 for x64-based Systems (KB2966828)	Update	4/12/2015
Security Update for Microsoft .NET Framework 3.5 on Windows 8.1 and Windows Server 2012 R2 for x64-based Systems (KB2968296)	Update	4/12/2015
Security Update for Microsoft .NET Framework 3.5 on Windows 8.1 and Windows Server 2012 R2 for x64-based Systems (KB2972103)	Update	4/12/2015
Security Update for Microsoft .NET Framework 3.5 on Windows 8.1 and Windows Server 2012 R2 for x64-based Systems (KB2972213)	Update	4/12/2015
Security Update for Microsoft .NET Framework 3.5 on Windows 8.1 and Windows Server 2012 R2 for x64-based Systems (KB2973114)	Update	4/12/2015
Security Update for Microsoft .NET Framework 3.5 on Windows 8.1 and Windows Server 2012 R2 for x64-based Systems (KB2978122)	Update	4/12/2015
Security Update for Microsoft .NET Framework 3.5 on Windows 8.1 and Windows Server 2012 R2 for x64-based Systems (KB2979573)	Update	4/12/2015
Security Update for Microsoft .NET Framework 3.5 on Windows 8.1 and Windows Server 2012 R2 for x64-based Systems (KB3037576)	Update	4/15/2015
Security Update for Microsoft .NET Framework 4.5.1 and 4.5.2 on Windows 8.1 and Windows Server 2012 R2 x64-based Systems (KB2977765)	Update	4/10/2015
Security Update for Microsoft .NET Framework 4.5.1 and 4.5.2 on Windows 8.1 and Windows Server 2012 R2 x64-based Systems (KB2978041)	Update	4/11/2015
Security Update for Microsoft .NET Framework 4.5.1 and 4.5.2 on Windows 8.1 and Windows Server 2012 R2 x64-based Systems (KB2978126)	Update	4/11/2015
Security Update for Microsoft .NET Framework 4.5.1 and 4.5.2 on Windows 8.1 and Windows Server 2012 R2 x64-based Systems (KB2979576)	Update	4/11/2015
Security Update for Microsoft .NET Framework 4.5.1 and 4.5.2 on Windows 8.1 and Windows Server 2012 R2 x64-based Systems (KB3037579)	Update	4/15/2015
Security Update for Microsoft .NET Framework 4.5.1 on Windows 8.1 and Windows Server 2012 R2 for x64-based Systems (KB2894856)	Update	4/10/2015
Security Update for Microsoft Excel 2013 (KB2920753) 64-Bit Edition	Update	4/11/2015
Security Update for Microsoft Lync 2013 (KB2881013) 64-Bit Edition	Update	4/11/2015
Security Update for Microsoft Office 2013 (KB2768005) 64-Bit Edition	Update	4/11/2015
Security Update for Microsoft Office 2013 (KB2880463) 64-Bit Edition	Update	4/11/2015
Security Update for Microsoft Office 2013 (KB2910941) 64-Bit Edition	Update	4/11/2015
Security Update for Microsoft Office 2013 (KB2956151) 64-Bit Edition	Update	4/11/2015
Security Update for Microsoft Word 2013 (KB2956163) 64-Bit Edition	Update	4/11/2015
Security Update for Microsoft Word 2013 (KB2965224) 64-Bit Edition	Update	4/15/2015
Security Update for Windows 8.1 for x64-based Systems (KB2918614)	Update	4/10/2015
Security Update for Windows 8.1 for x64-based Systems (KB2920189)	Update	4/11/2015
Security Update for Windows 8.1 for x64-based Systems (KB2961072)	Update	4/11/2015
Security Update for Windows 8.1 for x64-based Systems (KB2962140)	Update	4/10/2015
Security Update for Windows 8.1 for x64-based Systems (KB2964718)	Update	4/10/2015
Security Update for Windows 8.1 for x64-based Systems (KB2971850)	Update	4/10/2015
Security Update for Windows 8.1 for x64-based Systems (KB2972280)	Update	4/10/2015
Security Update for Windows 8.1 for x64-based Systems (KB2973351)	Update	4/11/2015
Security Update for Windows 8.1 for x64-based Systems (KB2977292)	Update	4/10/2015
Security Update for Windows 8.1 for x64-based Systems (KB2988948)	Update	4/10/2015
Security Update for Windows 8.1 for x64-based Systems (KB2993958)	Update	4/10/2015
Security Update for Windows 8.1 for x64-based Systems (KB3004361)	Update	4/11/2015
Security Update for Windows 8.1 for x64-based Systems (KB3004365)	Update	4/10/2015
Security Update for Windows 8.1 for x64-based Systems (KB3006226)	Update	4/10/2015
Security Update for Windows 8.1 for x64-based Systems (KB3010788)	Update	4/10/2015
Security Update for Windows 8.1 for x64-based Systems (KB3011780)	Update	4/10/2015
Security Update for Windows 8.1 for x64-based Systems (KB3019215)	Update	4/10/2015
Security Update for Windows 8.1 for x64-based Systems (KB3019978)	Update	4/11/2015
Security Update for Windows 8.1 for x64-based Systems (KB3021674)	Update	4/11/2015
Security Update for Windows 8.1 for x64-based Systems (KB3022777)	Update	4/10/2015
Security Update for Windows 8.1 for x64-based Systems (KB3023266)	Update	4/10/2015
Security Update for Windows 8.1 for x64-based Systems (KB3023562)	Update	4/11/2015

Security Update for Windows 8.1 for x64-based Systems (KB3030377)	Update	4/10/2015
Security Update for Windows 8.1 for x64-based Systems (KB3032323)	Update	4/11/2015
Security Update for Windows 8.1 for x64-based Systems (KB3033889)	Update	4/10/2015
Security Update for Windows 8.1 for x64-based Systems (KB3034344)	Update	4/11/2015
Security Update for Windows 8.1 for x64-based Systems (KB3035017)	Update	4/10/2015
Security Update for Windows 8.1 for x64-based Systems (KB3035126)	Update	4/10/2015
Security Update for Windows 8.1 for x64-based Systems (KB3035131)	Update	4/10/2015
Security Update for Windows 8.1 for x64-based Systems (KB3035132)	Update	4/10/2015
Security Update for Windows 8.1 for x64-based Systems (KB3039066)	Update	4/10/2015
Security Update for Windows 8.1 for x64-based Systems (KB3042553)	Update	4/15/2015
Security Update for Windows 8.1 for x64-based Systems (KB3045685)	Update	4/15/2015
Security Update for Windows 8.1 for x64-based Systems (KB3045755)	Update	4/15/2015
Security Update for Windows 8.1 for x64-based Systems (KB3045999)	Update	4/15/2015
Security Update for Windows 8.1 for x64-based Systems (KB3046049)	Update	4/11/2015
Service Pack 1 for Microsoft Office 2013 (KB2850036) 64-Bit Edition	Update	4/11/2015
Update for .NET Native on Windows 8.1 and Windows Server 2012 R2 for x64-based Systems (KB2954879)	Update	4/10/2015
Update for Microsoft Access 2013 (KB2956176) 64-Bit Edition	Update	4/11/2015
Update for Microsoft Access 2013 (KB2965276) 64-Bit Edition	Update	4/15/2015
Update for Microsoft Camera Codec Pack for Windows 8.1 for x64-based Systems (KB2899189)	Update	4/10/2015
Update for Microsoft Excel 2013 (KB2956145) 64-Bit Edition	Update	4/11/2015
Update for Microsoft Excel 2013 (KB2965275) 64-Bit Edition	Update	4/15/2015
Update for Microsoft Lync 2013 (KB2881083) 64-Bit Edition	Update	4/11/2015
Update for Microsoft Lync 2013 (KB2889923) 64-Bit Edition	Update	4/20/2015
Update for Microsoft Lync 2013 (KB2956174) 64-Bit Edition	Update	4/11/2015
Update for Microsoft Office 2013 (KB2726996) 64-Bit Edition	Update	4/11/2015
Update for Microsoft Office 2013 (KB2760249) 64-Bit Edition	Update	4/11/2015
Update for Microsoft Office 2013 (KB2760344) 64-Bit Edition	Update	4/11/2015
Update for Microsoft Office 2013 (KB2760371) 64-Bit Edition	Update	4/11/2015
Update for Microsoft Office 2013 (KB2760544) 64-Bit Edition	Update	4/11/2015
Update for Microsoft Office 2013 (KB2760610) 64-Bit Edition	Update	4/11/2015
Update for Microsoft Office 2013 (KB2768012) 64-Bit Edition	Update	4/11/2015
Update for Microsoft Office 2013 (KB2817316) 64-Bit Edition	Update	4/11/2015
Update for Microsoft Office 2013 (KB2825678) 64-Bit Edition	Update	4/15/2015
Update for Microsoft Office 2013 (KB2837654) 64-Bit Edition	Update	4/11/2015
Update for Microsoft Office 2013 (KB2863843) 64-Bit Edition	Update	4/11/2015
Update for Microsoft Office 2013 (KB2880478) 64-Bit Edition	Update	4/11/2015
Update for Microsoft Office 2013 (KB2880487) 64-Bit Edition	Update	4/15/2015
Update for Microsoft Office 2013 (KB2880977) 64-Bit Edition	Update	4/11/2015
Update for Microsoft Office 2013 (KB2881001) 64-Bit Edition	Update	4/11/2015
Update for Microsoft Office 2013 (KB2881035) 64-Bit Edition	Update	4/11/2015
Update for Microsoft Office 2013 (KB2883036) 64-Bit Edition	Update	4/11/2015
Update for Microsoft Office 2013 (KB2883095) 64-Bit Edition	Update	4/11/2015
Update for Microsoft Office 2013 (KB2899498) 64-Bit Edition	Update	4/11/2015
Update for Microsoft Office 2013 (KB2899522) 64-Bit Edition	Update	4/11/2015
Update for Microsoft Office 2013 (KB2920754) 64-Bit Edition	Update	4/11/2015
Update for Microsoft Office 2013 (KB2920769) 64-Bit Edition	Update	4/11/2015
Update for Microsoft Office 2013 (KB2956148) 64-Bit Edition	Update	4/11/2015
Update for Microsoft Office 2013 (KB2956154) 64-Bit Edition	Update	4/11/2015
Update for Microsoft Office 2013 (KB2956160) 64-Bit Edition	Update	4/11/2015
Update for Microsoft Office 2013 (KB2956167) 64-Bit Edition	Update	4/11/2015
Update for Microsoft Office 2013 (KB2956168) 64-Bit Edition	Update	4/11/2015
Update for Microsoft Office 2013 (KB2956169) 64-Bit Edition	Update	4/11/2015
Update for Microsoft Office 2013 (KB2956171) 64-Bit Edition	Update	4/11/2015
Update for Microsoft Office 2013 (KB2956177) 64-Bit Edition	Update	4/11/2015

Update for Microsoft Office 2013 (KB2965218) 64-Bit Edition	Update	4/19/2015
Update for Microsoft Office 2013 (KB2965255) 64-Bit Edition	Update	4/15/2015
Update for Microsoft Office 2013 (KB2965262) 64-Bit Edition	Update	4/15/2015
Update for Microsoft Office 2013 (KB2965267) 64-Bit Edition	Update	4/15/2015
Update for Microsoft Office 2013 (KB2965268) 64-Bit Edition	Update	4/15/2015
Update for Microsoft OneDrive for Business (KB2920746) 64-Bit Edition	Update	4/11/2015
Update for Microsoft OneDrive for Business (KB2956185) 64-Bit Edition	Update	4/15/2015
Update for Microsoft OneNote 2013 (KB2956165) 64-Bit Edition	Update	4/11/2015
Update for Microsoft OneNote 2013 (KB2965264) 64-Bit Edition	Update	4/19/2015
Update for Microsoft Outlook 2013 (KB2956170) 64-Bit Edition	Update	4/11/2015
Update for Microsoft Outlook 2013 (KB2965270) 64-Bit Edition	Update	4/15/2015
Update for Microsoft Outlook Social Connector 2013 (KB2737996) 64-Bit Edition	Update	4/11/2015
Update for Microsoft Outlook Social Connector 2013 (KB2965257) 64-Bit Edition	Update	4/15/2015
Update for Microsoft PowerPoint 2013 (KB2965206) 64-Bit Edition	Update	4/11/2015
Update for Microsoft PowerPoint 2013 (KB2965256) 64-Bit Edition	Update	4/15/2015
Update for Microsoft Project 2013 (KB2956187) 64-Bit Edition	Update	4/11/2015
Update for Microsoft Project 2013 (KB2965279) 64-Bit Edition	Update	4/15/2015
Update for Microsoft Publisher 2013 (KB2883048) 64-Bit Edition	Update	4/11/2015
Update for Microsoft SkyDrive Pro (KB2837652) 64-Bit Edition	Update	4/11/2015
Update for Microsoft Visio 2013 (KB2817306) 64-Bit Edition	Update	4/11/2015
Update for Microsoft Visio Viewer 2013 (KB2817301) 64-Bit Edition	Update	4/11/2015
Update for Microsoft Word 2013 (KB2878319) 64-Bit Edition	Update	4/11/2015
Update for Skype for Business 2015 (KB2889853) 64-Bit Edition	Update	4/15/2015
Update for Windows 8.1 for x64-based Systems (KB2939087)	Update	4/11/2015
Update for Windows 8.1 for x64-based Systems (KB2955164)	Update	4/10/2015
Update for Windows 8.1 for x64-based Systems (KB2958262)	Update	4/10/2015
Update for Windows 8.1 for x64-based Systems (KB2959626)	Update	4/10/2015
Update for Windows 8.1 for x64-based Systems (KB2962409)	Update	4/10/2015
Update for Windows 8.1 for x64-based Systems (KB2965142)	Update	4/10/2015
Update for Windows 8.1 for x64-based Systems (KB2967917)	Update	4/10/2015
Update for Windows 8.1 for x64-based Systems (KB2969817)	Update	4/10/2015
Update for Windows 8.1 for x64-based Systems (KB2971203)	Update	4/10/2015
Update for Windows 8.1 for x64-based Systems (KB2971239)	Update	4/10/2015
Update for Windows 8.1 for x64-based Systems (KB2975719)	Update	4/11/2015
Update for Windows 8.1 for x64-based Systems (KB2984006)	Update	4/10/2015
Update for Windows 8.1 for x64-based Systems (KB2989930)	Update	4/11/2015
Update for Windows 8.1 for x64-based Systems (KB2990967)	Update	4/10/2015
Update for Windows 8.1 for x64-based Systems (KB2994290)	Update	4/11/2015
Update for Windows 8.1 for x64-based Systems (KB2995388)	Update	4/10/2015
Update for Windows 8.1 for x64-based Systems (KB2998174)	Update	4/11/2015
Update for Windows 8.1 for x64-based Systems (KB3000850)	Update	4/15/2015
Update for Windows 8.1 for x64-based Systems (KB3003667)	Update	4/11/2015
Update for Windows 8.1 for x64-based Systems (KB3004394)	Update	4/11/2015
Update for Windows 8.1 for x64-based Systems (KB3006137)	Update	4/11/2015
Update for Windows 8.1 for x64-based Systems (KB3008242)	Update	4/10/2015
Update for Windows 8.1 for x64-based Systems (KB3012199)	Update	4/10/2015
Update for Windows 8.1 for x64-based Systems (KB3012235)	Update	4/11/2015
Update for Windows 8.1 for x64-based Systems (KB3012702)	Update	4/11/2015
Update for Windows 8.1 for x64-based Systems (KB3013172)	Update	4/10/2015
Update for Windows 8.1 for x64-based Systems (KB3013410)	Update	4/10/2015
Update for Windows 8.1 for x64-based Systems (KB3013531)	Update	4/22/2015
Update for Windows 8.1 for x64-based Systems (KB3013538)	Update	4/22/2015
Update for Windows 8.1 for x64-based Systems (KB3013769)	Update	4/22/2015
Update for Windows 8.1 for x64-based Systems (KB3015696)	Update	4/22/2015

Update for Windows 8.1 for x64-based Systems (KB3016074)	Update	4/10/2015
Update for Windows 8.1 for x64-based Systems (KB3018133)	Update	4/10/2015
Update for Windows 8.1 for x64-based Systems (KB3020338)	Update	4/11/2015
Update for Windows 8.1 for x64-based Systems (KB3020370)	Update	4/22/2015
Update for Windows 8.1 for x64-based Systems (KB3022345)	Update	4/22/2015
Update for Windows 8.1 for x64-based Systems (KB3022796)	Update	4/11/2015
Update for Windows 8.1 for x64-based Systems (KB3024751)	Update	4/10/2015
Update for Windows 8.1 for x64-based Systems (KB3024755)	Update	4/11/2015
Update for Windows 8.1 for x64-based Systems (KB3025417)	Update	4/11/2015
Update for Windows 8.1 for x64-based Systems (KB3027209)	Update	4/10/2015
Update for Windows 8.1 for x64-based Systems (KB3029606)	Update	4/10/2015
Update for Windows 8.1 for x64-based Systems (KB3029803)	Update	4/11/2015
Update for Windows 8.1 for x64-based Systems (KB3030947)	Update	4/10/2015
Update for Windows 8.1 for x64-based Systems (KB3033446)	Update	4/22/2015
Update for Windows 8.1 for x64-based Systems (KB3034348)	Update	4/11/2015
Update for Windows 8.1 for x64-based Systems (KB3035527)	Update	4/10/2015
Update for Windows 8.1 for x64-based Systems (KB3035553)	Update	4/10/2015
Update for Windows 8.1 for x64-based Systems (KB3035583)	Update	4/11/2015
Update for Windows 8.1 for x64-based Systems (KB3036228)	Update	4/10/2015
Update for Windows 8.1 for x64-based Systems (KB3036562)	Update	4/11/2015
Update for Windows 8.1 for x64-based Systems (KB3036612)	Update	4/10/2015
Update for Windows 8.1 for x64-based Systems (KB3037924)	Update	4/22/2015
Update for Windows 8.1 for x64-based Systems (KB3038002)	Update	4/22/2015
Update for Windows 8.1 for x64-based Systems (KB3038562)	Update	4/22/2015
Update for Windows 8.1 for x64-based Systems (KB3038701)	Update	4/22/2015
Update for Windows 8.1 for x64-based Systems (KB3042216)	Update	4/22/2015
Update for Windows 8.1 for x64-based Systems (KB3043812)	Update	4/22/2015
Update for Windows 8.1 for x64-based Systems (KB3044673)	Update	4/22/2015
Update for Windows 8.1 for x64-based Systems (KB3045717)	Update	4/22/2015
Update for Windows 8.1 for x64-based Systems (KB3045719)	Update	4/22/2015
Update for Windows 8.1 for x64-based Systems (KB3045992)	Update	4/22/2015
Update for Windows 8.1 for x64-based Systems (KB3046737)	Update	4/22/2015
Update for Windows 8.1 for x64-based Systems (KB3047254)	Update	4/22/2015
Update for Windows 8.1 for x64-based Systems (KB3047255)	Update	4/22/2015
Update for Windows 8.1 for x64-based Systems (KB3047641)	Update	4/22/2015
Windows 8.1 Update for x64-based Systems (KB2919355)	Update	4/11/2015
Windows Malicious Software Removal Tool for Windows 8, 8.1 and Windows Server 2012, 2012 R2 x64 Edition - April 2015 (KB890830)	Update	4/20/2015
Windows Malicious Software Removal Tool for Windows 8, 8.1 and Windows Server 2012, 2012 R2 x64 Edition - March 2015 (KB890830)	Update	4/10/2015

Anti-Virus

Software Description	Software Version	Virus Database Date	Known Viruses
Windows Defender	4.7.0205.0	4/28/2015	?

Firewall

Software Description	Software Version	Status
Windows Firewall	6.3.9600.17415	Enabled

Regional

Time Zone:

Current Time Zone	Pacific Daylight Time
Current Time Zone Description	(UTC-08:00) Pacific Time (US & Canada)
Change To Standard Time	First Sunday of November 2:00:00 AM
Change To Daylight Saving Time	2nd Sunday of March 2:00:00 AM

Language:

Language Name (Native)	English
Language Name (English)	English
Language Name (ISO 639)	en

Country/Region:

Country Name (Native)	United States
Country Name (English)	United States
Country Name (ISO 3166)	US
Country Code	1

Currency:

Currency Name (Native)	US Dollar
Currency Name (English)	US Dollar
Currency Symbol (Native)	$
Currency Symbol (ISO 4217)	USD
Currency Format	$123,456,789.00
Negative Currency Format	($123,456,789.00)

Formatting:

Time Format	h:mm:ss tt
Short Date Format	M/d/yyyy
Long Date Format	dddd, MMMM d, yyyy
Number Format	123,456,789.00
Negative Number Format	-123,456,789.00
List Format	first, second, third
Native Digits	0123456789

Days of Week:

Native Name for Monday	Monday / Mon
Native Name for Tuesday	Tuesday / Tue
Native Name for Wednesday	Wednesday / Wed
Native Name for Thursday	Thursday / Thu
Native Name for Friday	Friday / Fri
Native Name for Saturday	Saturday / Sat
Native Name for Sunday	Sunday / Sun

Months:

Native Name for January	January / Jan
Native Name for February	February / Feb
Native Name for March	March / Mar
Native Name for April	April / Apr
Native Name for May	May / May
Native Name for June	June / Jun

Native Name for July	July / Jul
Native Name for August	August / Aug
Native Name for September	September / Sep
Native Name for October	October / Oct
Native Name for November	November / Nov
Native Name for December	December / Dec

Miscellaneous:

Calendar Type	Gregorian (localized)
Default Paper Size	US Letter
Measurement System	U.S.

Display Languages:

LCID 0409h (Active)	English (United States)

Environment

Variable	Value
__COMPAT_LAYER	Installer
ALLUSERSPROFILE	C:\ProgramData
APPDATA	C:\Users\Liem\AppData\Roaming
CommonProgramFiles(x86)	C:\Program Files (x86)\Common Files
CommonProgramFiles	C:\Program Files (x86)\Common Files
CommonProgramW6432	C:\Program Files\Common Files
COMPUTERNAME	LTRANPHD
ComSpec	C:\Windows\system32\cmd.exe
FP_NO_HOST_CHECK	NO
HOMEDRIVE	C:
HOMEPATH	\Users\Liem
LOCALAPPDATA	C:\Users\Liem\AppData\Local
LOGONSERVER	\\LTRANPHD
NUMBER_OF_PROCESSORS	4
OS	Windows_NT
Path	C:\Windows\system32;C:\Windows;C:\Windows\System32\Wbem;C:\Windows\System32\WindowsPowerShell\v1.0\;C:\Program Files (x86)\Universal Extractor;C:\Program Files (x86)\Universal Extractor\bin
PATHEXT	.COM;.EXE;.BAT;.CMD;.VBS;.VBE;.JS;.JSE;.WSF;.WSH;.MSC
PROCESSOR_ARCHITECTURE	x86
PROCESSOR_ARCHITEW6432	AMD64
PROCESSOR_IDENTIFIER	Intel64 Family 6 Model 58 Stepping 9, GenuineIntel
PROCESSOR_LEVEL	6
PROCESSOR_REVISION	3a09
ProgramData	C:\ProgramData
ProgramFiles(x86)	C:\Program Files (x86)
ProgramFiles	C:\Program Files (x86)
ProgramW6432	C:\Program Files
PSModulePath	C:\Windows\system32\WindowsPowerShell\v1.0\Modules\
PUBLIC	C:\Users\Public
SystemDrive	C:
SystemRoot	C:\Windows
TEMP	C:\Users\Liem\AppData\Local\Temp
TMP	C:\Users\Liem\AppData\Local\Temp
USERDOMAIN_ROAMINGPROFILE	LTRANPHD

USERDOMAIN	LTRANPHD
USERNAME	Liem
USERPROFILE	C:\Users\Liem
windir	C:\Windows

Control Panel

Name	Comment
Flash Player	Manage Flash Player Settings

Recycle Bin

Drive	Items Size	Items Count	Space %	Recycle Bin
B:	0	1	?	?
C:	95 KB	2	?	?

System Files

[system.ini]

```
; for 16-bit app support
[386Enh]
woafont=dosapp.fon
EGA80WOA.FON=EGA80WOA.FON
EGA40WOA.FON=EGA40WOA.FON
CGA80WOA.FON=CGA80WOA.FON
CGA40WOA.FON=CGA40WOA.FON
[drivers]
wave=mmdrv.dll
timer=timer.drv
[mci]
```

[win.ini]

```
; for 16-bit app support
[fonts]
[extensions]
[mci extensions]
[files]
[Mail]
MAPI=1
CMCDLLNAME32=mapi32.dll
CMC=1
MAPIX=1
MAPIXVER=1.0.0.1
OLEMessaging=1
```

[hosts]

[lmhosts.sam]

System Folders

System Folder	Path
Administrative Tools	C:\Users\Liem\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Administrative Tools
AppData	C:\Users\Liem\AppData\Roaming
Cache	B:\Downloads\Temporary\Temporary Internet Files
CD Burning	C:\Users\Liem\AppData\Local\Microsoft\Windows\Burn\Burn
Common Administrative Tools	C:\ProgramData\Microsoft\Windows\Start Menu\Programs\Administrative Tools
Common AppData	C:\ProgramData
Common Desktop	C:\Users\Public\Desktop
Common Documents	C:\Users\Public\Documents
Common Favorites	B:\Favorites
Common Files (x86)	C:\Program Files (x86)\Common Files
Common Files	C:\Program Files (x86)\Common Files
Common Music	C:\Users\Public\Music
Common Pictures	C:\Users\Public\Pictures
Common Programs	C:\ProgramData\Microsoft\Windows\Start Menu\Programs
Common Start Menu	C:\ProgramData\Microsoft\Windows\Start Menu
Common Startup	C:\ProgramData\Microsoft\Windows\Start Menu\Programs\Startup
Common Templates	C:\ProgramData\Microsoft\Windows\Templates
Common Video	C:\Users\Public\Videos
Cookies	C:\Users\Liem\AppData\Local\Microsoft\Windows\INetCookies
Desktop	B:\Desktop
Device	C:\Windows\inf;C:\Program Files\SAMSUNG\USB Drivers\01_Simmental;C:\Program Files\SAMSUNG\USB Drivers\02_Siberian;C:\Program Files\SAMSUNG\USB Drivers\03_Swallowtail;C:\Program Files\SAMSUNG\USB Drivers\04_semseyite;C:\Program Files\SAMSUNG\USB Drivers\07_SchorI;C:\Program Files\SAMSUNG\USB Drivers\09_Hsp;C:\Program Files\SAMSUNG\USB Drivers\11_HSP_Plus_Default;C:\Program Files\SAMSUNG\USB Drivers\16_Shrewsbury;C:\Program Files\SAMSUNG\USB Drivers\20_NXP_Driver;C:\Program Files\SAMSUNG\USB Drivers\24_flashusbdriver;C:\Program Files\SAMSUNG\USB Drivers\25_escape
Favorites	B:\Favorites
Fonts	C:\Windows\Fonts
History	C:\Users\Liem\AppData\Local\Microsoft\Windows\History

Local AppData	C:\Users\Liem\AppData\Local
My Documents	B:\Documents
My Music	B:\Music
My Pictures	B:\Pictures
My Video	B:\Videos
NetHood	C:\Users\Liem\AppData\Roaming\Microsoft\Windows\Network Shortcuts
PrintHood	C:\Users\Liem\AppData\Roaming\Microsoft\Windows\Printer Shortcuts
Profile	C:\Users\Liem
Program Files (x86)	C:\Program Files (x86)
Program Files	C:\Program Files (x86)
Programs	C:\Users\Liem\AppData\Roaming\Microsoft\Windows\Start Menu\Programs
Recent	C:\Users\Liem\AppData\Roaming\Microsoft\Windows\Recent
Resources	C:\Windows\resources
SendTo	C:\Users\Liem\AppData\Roaming\Microsoft\Windows\SendTo
Start Menu	C:\Users\Liem\AppData\Roaming\Microsoft\Windows\Start Menu
Startup	C:\Users\Liem\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup
System (x86)	C:\Windows\SysWOW64
System	C:\Windows\system32
Temp	C:\Users\Liem\AppData\Local\Temp\
Templates	C:\Users\Liem\AppData\Roaming\Microsoft\Windows\Templates
Windows	C:\Windows

Event Logs

Log Name	Event Type	Category	Generated On	User	Source	Description
Application	Warning	None	2015-04-22 16:22:41		Software Protection Platform Service	8233: The rules engine reported a failed VL activation attempt. Reason:0x8007232B AppId = 0ff1ce15-a989-479d-af46-f275c6370663, SkuId = b322da9c-a2e2-4058-9e4e-f59a6970bd69 Trigger=NetworkAvailable
Application	Warning	None	2015-04-22 16:22:44		Software Protection Platform Service	8233: The rules engine reported a failed VL activation attempt. Reason:0x8007232B AppId = 0ff1ce15-a989-479d-af46-f275c6370663, SkuId = b322da9c-a2e2-4058-9e4e-f59a6970bd69 Trigger=NetworkAvailable
Application	Warning	None	2015-04-22 16:23:04		Software Protection Platform Service	8233: The rules engine reported a failed VL activation attempt. Reason:0x8007232B AppId = 0ff1ce15-a989-479d-af46-f275c6370663, SkuId = b322da9c-a2e2-4058-9e4e-f59a6970bd69 Trigger=UserLogon(1)
Application	Error	3	2015-04-22 16:26:20		Windows Search Service	3079: Notifications for the volume C:\ are not active. Context: Windows Application Details: The parameter is incorrect. (HRESULT : 0x80070057) (0x80070057)
Application	Error	None	2015-04-22 16:26:37	SYSTEM	Microsoft-Windows-LoadPerf	3012: The performance strings in the Performance registry value is corrupted when process Performance extension counter provider. The BaseIndex value from the Performance registry is the first DWORD in the Data section, LastCounter value is the second DWORD in the Data section, and LastHelp value is the third DWORD in the Data section.
Application	Error	None	2015-04-22 16:26:37	SYSTEM	Microsoft-Windows-LoadPerf	3011: Unloading the performance counter strings for service WmiApRpl (WmiApRpl) failed. The first DWORD in the Data section contains the error code.
Application	Warning	None	2015-04-22 18:07:26		Software Protection Platform Service	8233: The rules engine reported a failed VL activation attempt. Reason:0x8007267C AppId = 0ff1ce15-a989-479d-af46-f275c6370663, SkuId = b322da9c-a2e2-4058-9e4e-f59a6970bd69 Trigger=UserLogon(1)
Application	Warning	None	2015-04-22 18:07:39		Software Protection Platform Service	8233: The rules engine reported a failed VL activation attempt. Reason:0x8007007B AppId = 0ff1ce15-a989-479d-af46-f275c6370663, SkuId = b322da9c-a2e2-4058-9e4e-f59a6970bd69 Trigger=NetworkAvailable

	Application	Warning	None	2015-04-22 18:07:51		Software Protection Platform Service	8233: The rules engine reported a failed VL activation attempt. Reason:0x8007232B AppId = 0ff1ce15-a989-479d-af46-f275c6370663, SkuId = b322da9c-a2e2-4058-9e4e-f59a6970bd69 Trigger=NetworkAvailable
	Application	Warning	None	2015-04-22 18:10:01		Software Protection Platform Service	8233: The rules engine reported a failed VL activation attempt. Reason:0x8007232B AppId = 0ff1ce15-a989-479d-af46-f275c6370663, SkuId = b322da9c-a2e2-4058-9e4e-f59a6970bd69 Trigger=NetworkAvailable
	Application	Warning	None	2015-04-22 18:10:03		Software Protection Platform Service	8233: The rules engine reported a failed VL activation attempt. Reason:0x8007232B AppId = 0ff1ce15-a989-479d-af46-f275c6370663, SkuId = b322da9c-a2e2-4058-9e4e-f59a6970bd69 Trigger=NetworkAvailable
	Application	Error	None	2015-04-22 18:11:37	SYSTEM	Microsoft-Windows-LoadPerf	3012: The performance strings in the Performance registry value is corrupted when process Performance extension counter provider. The BaseIndex value from the Performance registry is the first DWORD in the Data section, LastCounter value is the second DWORD in the Data section, and LastHelp value is the third DWORD in the Data section.
	Application	Error	None	2015-04-22 18:11:37	SYSTEM	Microsoft-Windows-LoadPerf	3011: Unloading the performance counter strings for service WmiApRpl (WmiApRpl) failed. The first DWORD in the Data section contains the error code.
	Application	Warning	None	2015-04-22 18:53:07		Software Protection Platform Service	8233: The rules engine reported a failed VL activation attempt. Reason:0x8007232B AppId = 0ff1ce15-a989-479d-af46-f275c6370663, SkuId = b322da9c-a2e2-4058-9e4e-f59a6970bd69 Trigger=UserLogon(1)
	Application	Warning	None	2015-04-22 18:53:10		Software Protection Platform Service	8233: The rules engine reported a failed VL activation attempt. Reason:0x8007232B AppId = 0ff1ce15-a989-479d-af46-f275c6370663, SkuId = b322da9c-a2e2-4058-9e4e-f59a6970bd69 Trigger=NetworkAvailable
	Application	Warning	3	2015-04-22 18:55:08		Windows Search Service	3036: Crawl could not be completed on content source <StickyNotes://{S-1-5-21-1888849264-3803429180-4108621888-1001}/notes/>. Context: Application, SystemIndex Catalog Details: The filtering process has been terminated (HRESULT : 0x80040db4) (0x80040db4)
	Application	Error	None	2015-04-22 18:57:12	SYSTEM	Microsoft-Windows-LoadPerf	3012: The performance strings in the Performance registry value is corrupted when process Performance extension counter provider. The BaseIndex value from the Performance registry is the first DWORD in the Data section, LastCounter value is the second DWORD in the Data section, and LastHelp value is the third DWORD in the Data section.
	Application	Error	None	2015-04-22 18:57:12	SYSTEM	Microsoft-Windows-LoadPerf	3011: Unloading the performance counter strings for service WmiApRpl (WmiApRpl) failed. The first DWORD in the Data section contains the error code.
	Application	Warning	None	2015-04-22 19:03:58	SYSTEM	Microsoft-Windows-RestartManager	10010: Application 'C:\Windows\explorer.exe' (pid 2016) cannot be restarted - 1.
	Application	Warning	None	2015-04-22 19:05:29		Software Protection Platform Service	8233: The rules engine reported a failed VL activation attempt. Reason:0x8007232B AppId = 0ff1ce15-a989-479d-af46-f275c6370663, SkuId = b322da9c-a2e2-4058-9e4e-f59a6970bd69 Trigger=NetworkAvailable
	Application	Warning	None	2015-04-22 19:05:31		Software Protection Platform Service	8233: The rules engine reported a failed VL activation attempt. Reason:0x8007232B AppId = 0ff1ce15-a989-479d-af46-f275c6370663, SkuId = b322da9c-a2e2-4058-9e4e-f59a6970bd69 Trigger=NetworkAvailable
	Application	Warning	None	2015-04-22 19:07:25		Software Protection Platform Service	8233: The rules engine reported a failed VL activation attempt. Reason:0x8007232B AppId = 0ff1ce15-a989-479d-af46-f275c6370663, SkuId = b322da9c-a2e2-4058-9e4e-f59a6970bd69 Trigger=UserLogon(1)
	Application	Error	None	2015-04-22 19:09:36	SYSTEM	Microsoft-Windows-LoadPerf	3012: The performance strings in the Performance registry value is corrupted when process Performance extension counter provider. The BaseIndex value from the Performance registry is the first DWORD in the Data section, LastCounter value is the second DWORD in the Data section, and LastHelp value is the third DWORD in the Data section.
	Application	Error	None	2015-04-22 19:09:36	SYSTEM	Microsoft-Windows-LoadPerf	3011: Unloading the performance counter strings for service WmiApRpl (WmiApRpl) failed. The first DWORD in the Data section contains the error code.
	Application	Error	None	2015-04-22 19:21:03	SYSTEM	Microsoft-Windows-LoadPerf	3012: The performance strings in the Performance registry value is corrupted when process Performance extension counter provider. The BaseIndex value from the Performance registry is the first DWORD in the Data section, LastCounter value is the second DWORD in the Data section, and LastHelp value is the third DWORD in the Data section.
	Application	Error	None	2015-04-22 19:21:03	SYSTEM	Microsoft-Windows-LoadPerf	3011: Unloading the performance counter strings for service WmiApRpl (WmiApRpl) failed. The first DWORD in the Data section contains the error code.
	Application	Error	None	2015-04-22 19:30:54		AdvancedSystemCareService8	0:
	Application	Error	None	2015-04-22		AdvancedSystemCareService8	0:

			19:30:54			
Application	Warning	None	2015-04-22 19:47:49		Software Protection Platform Service	8233: The rules engine reported a failed VL activation attempt. Reason:0x8007232B AppId = 0ff1ce15-a989-479d-af46-f275c6370663, SkuId = b322da9c-a2e2-4058-9e4e-f59a6970bd69 Trigger=UserLogon(1)
Application	Warning	None	2015-04-22 19:47:52		Software Protection Platform Service	8233: The rules engine reported a failed VL activation attempt. Reason:0x8007232B AppId = 0ff1ce15-a989-479d-af46-f275c6370663, SkuId = b322da9c-a2e2-4058-9e4e-f59a6970bd69 Trigger=NetworkAvailable
Application	Warning	None	2015-04-22 19:49:38		Software Protection Platform Service	8233: The rules engine reported a failed VL activation attempt. Reason:0x8007267C AppId = 0ff1ce15-a989-479d-af46-f275c6370663, SkuId = b322da9c-a2e2-4058-9e4e-f59a6970bd69 Trigger=UserLogon(1)
Application	Warning	None	2015-04-22 19:49:44		Software Protection Platform Service	8233: The rules engine reported a failed VL activation attempt. Reason:0x8007232B AppId = 0ff1ce15-a989-479d-af46-f275c6370663, SkuId = b322da9c-a2e2-4058-9e4e-f59a6970bd69 Trigger=NetworkAvailable
Application	Warning	None	2015-04-22 19:49:47		Software Protection Platform Service	8233: The rules engine reported a failed VL activation attempt. Reason:0x8007232B AppId = 0ff1ce15-a989-479d-af46-f275c6370663, SkuId = b322da9c-a2e2-4058-9e4e-f59a6970bd69 Trigger=NetworkAvailable
Application	Warning	None	2015-04-22 19:53:08		Software Protection Platform Service	8233: The rules engine reported a failed VL activation attempt. Reason:0x8007232B AppId = 0ff1ce15-a989-479d-af46-f275c6370663, SkuId = b322da9c-a2e2-4058-9e4e-f59a6970bd69 Trigger=UserLogon(1)
Application	Warning	None	2015-04-22 19:53:11		Software Protection Platform Service	8233: The rules engine reported a failed VL activation attempt. Reason:0x8007232B AppId = 0ff1ce15-a989-479d-af46-f275c6370663, SkuId = b322da9c-a2e2-4058-9e4e-f59a6970bd69 Trigger=NetworkAvailable
Application	Warning	None	2015-04-22 19:54:26		Software Protection Platform Service	8233: The rules engine reported a failed VL activation attempt. Reason:0x8007267C AppId = 0ff1ce15-a989-479d-af46-f275c6370663, SkuId = b322da9c-a2e2-4058-9e4e-f59a6970bd69 Trigger=UserLogon(1)
Application	Warning	None	2015-04-22 19:54:34		Software Protection Platform Service	8233: The rules engine reported a failed VL activation attempt. Reason:0x8007232B AppId = 0ff1ce15-a989-479d-af46-f275c6370663, SkuId = b322da9c-a2e2-4058-9e4e-f59a6970bd69 Trigger=NetworkAvailable
Application	Warning	None	2015-04-22 19:54:36		Software Protection Platform Service	8233: The rules engine reported a failed VL activation attempt. Reason:0x8007232B AppId = 0ff1ce15-a989-479d-af46-f275c6370663, SkuId = b322da9c-a2e2-4058-9e4e-f59a6970bd69 Trigger=NetworkAvailable
Application	Error	None	2015-04-22 19:56:20	SYSTEM	Microsoft-Windows-LoadPerf	3012: The performance strings in the Performance registry value is corrupted when process Performance extension counter provider. The BaseIndex value from the Performance registry is the first DWORD in the Data section, LastCounter value is the second DWORD in the Data section, and LastHelp value is the third DWORD in the Data section.
Application	Error	None	2015-04-22 19:56:20	SYSTEM	Microsoft-Windows-LoadPerf	3011: Unloading the performance counter strings for service WmiApRpl (WmiApRpl) failed. The first DWORD in the Data section contains the error code.
Application	Error	None	2015-04-22 19:57:39	Liem	MsiInstaller	1013: Product: Intel(R) Wireless Bluetooth(R) -- A newer version of Intel(R) Wireless Bluetooth(R) is already installed. Setup will now exit.
Application	Error	None	2015-04-22 19:59:13	SYSTEM	Microsoft-Windows-LoadPerf	3012: The performance strings in the Performance registry value is corrupted when process Performance extension counter provider. The BaseIndex value from the Performance registry is the first DWORD in the Data section, LastCounter value is the second DWORD in the Data section, and LastHelp value is the third DWORD in the Data section.
Application	Error	None	2015-04-22 19:59:13	SYSTEM	Microsoft-Windows-LoadPerf	3011: Unloading the performance counter strings for service WmiApRpl (WmiApRpl) failed. The first DWORD in the Data section contains the error code.
Application	Warning	3	2015-04-22 20:06:29		Windows Search Service	3036: Crawl could not be completed on content source <winrt://{S-1-5-21-1888849264-3803429180-4108621888-1001}/>. Context: Application, SystemIndex Catalog Details: The parameter is incorrect. (HRESULT : 0x80070057) (0x80070057)
Application	Warning	3	2015-04-22 20:07:23		Windows Search Service	3036: Crawl could not be completed on content source <StickyNotes://{S-1-5-21-1888849264-3803429180-4108621888-1001}/notes/>. Context: Application, SystemIndex Catalog Details: The filtering process has been terminated (HRESULT : 0x80040db4) (0x80040db4)
Application	Warning	None	2015-04-22 20:24:50		Software Protection Platform Service	8233: The rules engine reported a failed VL activation attempt. Reason:0x8007232B AppId = 0ff1ce15-a989-479d-af46-f275c6370663, SkuId = b322da9c-a2e2-4058-9e4e-f59a6970bd69 Trigger=UserLogon(1)
Application	Warning	None	2015-04-22 20:24:52		Software Protection Platform Service	8233: The rules engine reported a failed VL activation attempt. Reason:0x8007232B AppId = 0ff1ce15-a989-479d-af46-f275c6370663, SkuId = b322da9c-a2e2-4058-9e4e-f59a6970bd69 Trigger=NetworkAvailable
Application	Error	None	2015-04-22	SYSTEM	Microsoft-Windows-LoadPerf	3012: The performance strings in the Performance registry value is corrupted when process Performance extension counter provider. The BaseIndex value from the Performance registry is the first DWORD in the Data section, LastCounter value is the second DWORD in the Data section, and LastHelp value is the third DWORD in

			20:31:25			the Data section.
Application	Error	None	2015-04-22 20:31:25	SYSTEM	Microsoft-Windows-LoadPerf	3011: Unloading the performance counter strings for service WmiApRpl (WmiApRpl) failed. The first DWORD in the Data section contains the error code.
Application	Warning	None	2015-04-22 20:51:57		Software Protection Platform Service	8233: The rules engine reported a failed VL activation attempt. Reason:0x8007007B AppId = 0ff1ce15-a989-479d-af46-f275c6370663, SkuId = b322da9c-a2e2-4058-9e4e-f59a6970bd69 Trigger=NetworkAvailable
Application	Warning	None	2015-04-22 20:52:05		Software Protection Platform Service	8233: The rules engine reported a failed VL activation attempt. Reason:0x8007007B AppId = 0ff1ce15-a989-479d-af46-f275c6370663, SkuId = b322da9c-a2e2-4058-9e4e-f59a6970bd69 Trigger=NetworkAvailable
Application	Warning	None	2015-04-22 20:56:25		Software Protection Platform Service	8233: The rules engine reported a failed VL activation attempt. Reason:0x8007267C AppId = 0ff1ce15-a989-479d-af46-f275c6370663, SkuId = b322da9c-a2e2-4058-9e4e-f59a6970bd69 Trigger=UserLogon(1)
Application	Warning	None	2015-04-22 20:56:27		Software Protection Platform Service	8233: The rules engine reported a failed VL activation attempt. Reason:0x8007007B AppId = 0ff1ce15-a989-479d-af46-f275c6370663, SkuId = b322da9c-a2e2-4058-9e4e-f59a6970bd69 Trigger=NetworkAvailable
Application	Warning	None	2015-04-22 20:56:39		Software Protection Platform Service	8233: The rules engine reported a failed VL activation attempt. Reason:0x8007232B AppId = 0ff1ce15-a989-479d-af46-f275c6370663, SkuId = b322da9c-a2e2-4058-9e4e-f59a6970bd69 Trigger=NetworkAvailable
Application	Warning	None	2015-04-22 20:56:47		Software Protection Platform Service	8233: The rules engine reported a failed VL activation attempt. Reason:0x8007232B AppId = 0ff1ce15-a989-479d-af46-f275c6370663, SkuId = b322da9c-a2e2-4058-9e4e-f59a6970bd69 Trigger=NetworkAvailable
Application	Error	None	2015-04-22 21:03:05	SYSTEM	Microsoft-Windows-LoadPerf	3012: The performance strings in the Performance registry value is corrupted when process Performance extension counter provider. The BaseIndex value from the Performance registry is the first DWORD in the Data section, LastCounter value is the second DWORD in the Data section, and LastHelp value is the third DWORD in the Data section.
Application	Error	None	2015-04-22 21:03:05	SYSTEM	Microsoft-Windows-LoadPerf	3011: Unloading the performance counter strings for service WmiApRpl (WmiApRpl) failed. The first DWORD in the Data section contains the error code.
Application	Warning	None	2015-04-22 21:18:13		Software Protection Platform Service	8233: The rules engine reported a failed VL activation attempt. Reason:0x8007267C AppId = 0ff1ce15-a989-479d-af46-f275c6370663, SkuId = b322da9c-a2e2-4058-9e4e-f59a6970bd69 Trigger=UserLogon(1)
Application	Warning	None	2015-04-22 21:18:19		Software Protection Platform Service	8233: The rules engine reported a failed VL activation attempt. Reason:0x8007232B AppId = 0ff1ce15-a989-479d-af46-f275c6370663, SkuId = b322da9c-a2e2-4058-9e4e-f59a6970bd69 Trigger=NetworkAvailable
Application	Warning	None	2015-04-22 21:18:22		Software Protection Platform Service	8233: The rules engine reported a failed VL activation attempt. Reason:0x8007232B AppId = 0ff1ce15-a989-479d-af46-f275c6370663, SkuId = b322da9c-a2e2-4058-9e4e-f59a6970bd69 Trigger=NetworkAvailable
Application	Error	None	2015-04-22 21:22:20	SYSTEM	Microsoft-Windows-LoadPerf	3012: The performance strings in the Performance registry value is corrupted when process Performance extension counter provider. The BaseIndex value from the Performance registry is the first DWORD in the Data section, LastCounter value is the second DWORD in the Data section, and LastHelp value is the third DWORD in the Data section.
Application	Error	None	2015-04-22 21:22:20	SYSTEM	Microsoft-Windows-LoadPerf	3011: Unloading the performance counter strings for service WmiApRpl (WmiApRpl) failed. The first DWORD in the Data section contains the error code.
Application	Warning	None	2015-04-22 21:33:36		Software Protection Platform Service	8233: The rules engine reported a failed VL activation attempt. Reason:0x8007232B AppId = 0ff1ce15-a989-479d-af46-f275c6370663, SkuId = b322da9c-a2e2-4058-9e4e-f59a6970bd69 Trigger=NetworkAvailable
Application	Warning	None	2015-04-23 07:23:50		Software Protection Platform Service	8233: The rules engine reported a failed VL activation attempt. Reason:0x8007007B AppId = 0ff1ce15-a989-479d-af46-f275c6370663, SkuId = b322da9c-a2e2-4058-9e4e-f59a6970bd69 Trigger=UserLogon(1)
Application	Warning	None	2015-04-23 07:23:51		Software Protection Platform Service	8233: The rules engine reported a failed VL activation attempt. Reason:0x8007007B AppId = 0ff1ce15-a989-479d-af46-f275c6370663, SkuId = b322da9c-a2e2-4058-9e4e-f59a6970bd69 Trigger=NetworkAvailable
Application	Warning	None	2015-04-23 07:23:58		Software Protection Platform Service	8233: The rules engine reported a failed VL activation attempt. Reason:0x8007007B AppId = 0ff1ce15-a989-479d-af46-f275c6370663, SkuId = b322da9c-a2e2-4058-9e4e-f59a6970bd69 Trigger=NetworkAvailable
Application	Error	3	2015-04-23 07:27:44		Windows Search Service	3079: Notifications for the volume C:\ are not active. Context: Windows Application Details: The parameter is incorrect. (HRESULT : 0x80070057) (0x80070057)
Application	Error	None	2015-04-23	SYSTEM	Microsoft-Windows-LoadPerf	3012: The performance strings in the Performance registry value is corrupted when process Performance extension counter provider. The BaseIndex value from the Performance registry is the first DWORD in the Data

			07:28:03			section, LastCounter value is the second DWORD in the Data section, and LastHelp value is the third DWORD in the Data section.
Application	Error	None	2015-04-23 07:28:03	SYSTEM	Microsoft-Windows-LoadPerf	3011: Unloading the performance counter strings for service WmiApRpl (WmiApRpl) failed. The first DWORD in the Data section contains the error code.
Application	Warning	3	2015-04-23 07:35:12		Windows Search Service	3036: Crawl could not be completed on content source <StickyNotes://{S-1-5-21-1888849264-3803429180-4108621888-1001}/notes/>. Context: Application, SystemIndex Catalog Details: The filtering process has been terminated (HRESULT : 0x80040db4) (0x80040db4)
Application	Warning	None	2015-04-23 08:30:28		Software Protection Platform Service	8233: The rules engine reported a failed VL activation attempt. Reason:0x8007007B AppId = 0ff1ce15-a989-479d-af46-f275c6370663, SkuId = b322da9c-a2e2-4058-9e4e-f59a6970bd69 Trigger=NetworkAvailable
Application	Error	1	2015-04-23 08:53:24		Windows Search Service	7040: The search service has detected corrupted data files in the index {id=4810 - enduser\mssearch2\search\ytrip\common\util\jetutil.cpp (167)}. The service will attempt to automatically correct this problem by rebuilding the index. Details: 0x8e5e0210 (0x8e5e0210)
Application	Error	1	2015-04-23 08:53:24		Windows Search Service	7042: The Windows Search Service is being stopped because there is a problem with the indexer: The catalog is corrupt. Details: The content index catalog is corrupt. 0xc0041801 (0xc0041801)
Application	Error	3	2015-04-23 08:53:24		ESENT	455: taskhostex (2432) WebCacheLocal: Error -1811 (0xfffff8ed) occurred while opening logfile C:\Users\Liem\AppData\Local\Microsoft\Windows\WebCache\V010000B.log.
Application	Error	3	2015-04-23 08:53:24		ESENT	455: SearchIndexer (2796) Windows: Error -1811 (0xfffff8ed) occurred while opening logfile C:\ProgramData\Microsoft\Search\Data\Applications\Windows\edb0000C.log.
Application	Error	3	2015-04-23 08:53:24		Windows Search Service	3057: The plug-in manager <Search.TripoliIndexer> cannot be initialized. Context: Windows Application Details: (HRESULT : 0x8e5e0210) (0x8e5e0210)
Application	Error	3	2015-04-23 08:53:24		Windows Search Service	3029: The plug-in in <Search.TripoliIndexer> cannot be initialized. Context: Windows Application, SystemIndex Catalog Details: The specified object cannot be found. Specify the name of an existing object. (HRESULT : 0x80040d06) (0x80040d06)
Application	Error	3	2015-04-23 08:53:24		Windows Search Service	3028: The gatherer object cannot be initialized. Context: Windows Application, SystemIndex Catalog Details: The specified object cannot be found. Specify the name of an existing object. (HRESULT : 0x80040d06) (0x80040d06)
Application	Error	3	2015-04-23 08:53:24		Windows Search Service	3058: The application cannot be initialized. Context: Windows Application Details: The specified object cannot be found. Specify the name of an existing object. (HRESULT : 0x80040d06) (0x80040d06)
Application	Error	3	2015-04-23 08:53:24		Windows Search Service	7010: The index cannot be initialized. Details: The specified object cannot be found. Specify the name of an existing object. (HRESULT : 0x80040d06) (0x80040d06)
Application	Warning	None	2015-04-23 08:53:25		Software Protection Platform Service	8233: The rules engine reported a failed VL activation attempt. Reason:0x8007007B AppId = 0ff1ce15-a989-479d-af46-f275c6370663, SkuId = b322da9c-a2e2-4058-9e4e-f59a6970bd69 Trigger=NetworkAvailable
Application	Warning	1	2015-04-23 08:53:25		Windows Search Service	1008: The Windows Search Service is starting up and attempting to remove the old search index {Reason: Index Corruption}.
Application	Error	3	2015-04-23 08:53:26		Windows Search Service	1019: Windows Search Service failed to process the list of included and excluded locations with the error <30, 0x80040d07, "file:///B:\[2be3cb0f-27a0-48bc-b2b7-f1525ce1859d]\Contacts\">.
Application	Error	3	2015-04-23 08:53:26		Windows Search Service	1019: Windows Search Service failed to process the list of included and excluded locations with the error <30, 0x80040d07, "file:///B:\[2be3cb0f-27a0-48bc-b2b7-f1525ce1859d]\Desktop\">.
Application	Error	3	2015-04-23 08:53:26		Windows Search Service	1019: Windows Search Service failed to process the list of included and excluded locations with the error <30, 0x80040d07, "file:///B:\[2be3cb0f-27a0-48bc-b2b7-f1525ce1859d]\Documents\">.
Application	Error	3	2015-04-23 08:53:26		Windows Search Service	1019: Windows Search Service failed to process the list of included and excluded locations with the error <30, 0x80040d07, "file:///B:\[2be3cb0f-27a0-48bc-b2b7-f1525ce1859d]\Downloads\">.
Application	Error	3	2015-04-23 08:53:26		Windows Search Service	1019: Windows Search Service failed to process the list of included and excluded locations with the error <30, 0x80040d07, "file:///B:\[2be3cb0f-27a0-48bc-b2b7-f1525ce1859d]\Favorites\">.
Application	Error	3	2015-04-23 08:53:26		Windows Search Service	1019: Windows Search Service failed to process the list of included and excluded locations with the error <30, 0x80040d07, "file:///B:\[2be3cb0f-27a0-48bc-b2b7-f1525ce1859d]\Links\">.

Application	Error	3	2015-04-23 08:53:26	Windows Search Service	1019: Windows Search Service failed to process the list of included and excluded locations with the error <30, 0x80040d07, "file:///B:\[2be3cb0f-27a0-48bc-b2b7-f1525ce1859d]\Music\">.
Application	Error	3	2015-04-23 08:53:26	Windows Search Service	1019: Windows Search Service failed to process the list of included and excluded locations with the error <30, 0x80040d07, "file:///B:\[2be3cb0f-27a0-48bc-b2b7-f1525ce1859d]\Pictures\">.
Application	Error	3	2015-04-23 08:53:26	Windows Search Service	1019: Windows Search Service failed to process the list of included and excluded locations with the error <30, 0x80040d07, "file:///B:\[2be3cb0f-27a0-48bc-b2b7-f1525ce1859d]\Saved Games\">.
Application	Error	3	2015-04-23 08:53:26	Windows Search Service	1019: Windows Search Service failed to process the list of included and excluded locations with the error <30, 0x80040d07, "file:///B:\[2be3cb0f-27a0-48bc-b2b7-f1525ce1859d]\Searches\">.
Application	Error	3	2015-04-23 08:53:26	Windows Search Service	1019: Windows Search Service failed to process the list of included and excluded locations with the error <30, 0x80040d07, "file:///B:\[2be3cb0f-27a0-48bc-b2b7-f1525ce1859d]\Videos\">.
Application	Warning	3	2015-04-23 08:53:26	Windows Search Service	3037: Crawl could not be started on content source <B:\[2be3cb0f-27a0-48bc-b2b7-f1525ce1859d]\Contacts\>. Context: Windows Application, SystemIndex Catalog Details: The specified address was excluded from the index. The site path rules may have to be modified to include this address. (HRESULT : 0x80040d07) (0x80040d07)
Application	Warning	3	2015-04-23 08:53:26	Windows Search Service	3023: The update cannot be started because all of the content sources were excluded by site path rules, or removed from the index configuration. Context: Windows Application, SystemIndex Catalog Details: (HRESULT : 0x1) (0x00000001)
Application	Warning	3	2015-04-23 08:53:26	Windows Search Service	3037: Crawl could not be started on content source <B:\[2be3cb0f-27a0-48bc-b2b7-f1525ce1859d]\Desktop\>. Context: Windows Application, SystemIndex Catalog Details: The specified address was excluded from the index. The site path rules may have to be modified to include this address. (HRESULT : 0x80040d07) (0x80040d07)
Application	Warning	3	2015-04-23 08:53:26	Windows Search Service	3023: The update cannot be started because all of the content sources were excluded by site path rules, or removed from the index configuration. Context: Windows Application, SystemIndex Catalog Details: (HRESULT : 0x1) (0x00000001)
Application	Warning	3	2015-04-23 08:53:26	Windows Search Service	3037: Crawl could not be started on content source <B:\[2be3cb0f-27a0-48bc-b2b7-f1525ce1859d]\Documents\>. Context: Windows Application, SystemIndex Catalog Details: The specified address was excluded from the index. The site path rules may have to be modified to include this address. (HRESULT : 0x80040d07) (0x80040d07)
Application	Warning	3	2015-04-23 08:53:26	Windows Search Service	3023: The update cannot be started because all of the content sources were excluded by site path rules, or removed from the index configuration. Context: Windows Application, SystemIndex Catalog Details: (HRESULT : 0x1) (0x00000001)
Application	Warning	3	2015-04-23 08:53:26	Windows Search Service	3037: Crawl could not be started on content source <B:\[2be3cb0f-27a0-48bc-b2b7-f1525ce1859d]\Downloads\>. Context: Windows Application, SystemIndex Catalog Details: The specified address was excluded from the index. The site path rules may have to be modified to include this address. (HRESULT : 0x80040d07) (0x80040d07)
Application	Warning	3	2015-04-23 08:53:26	Windows Search Service	3023: The update cannot be started because all of the content sources were excluded by site path rules, or removed from the index configuration. Context: Windows Application, SystemIndex Catalog Details: (HRESULT : 0x1) (0x00000001)
Application	Warning	3	2015-04-23 08:53:26	Windows Search Service	3037: Crawl could not be started on content source <B:\[2be3cb0f-27a0-48bc-b2b7-f1525ce1859d]\Favorites\>. Context: Windows Application, SystemIndex Catalog Details: The specified address was excluded from the index. The site path rules may have to be modified to include this address. (HRESULT : 0x80040d07) (0x80040d07)
Application	Warning	3	2015-04-23 08:53:26	Windows Search Service	3023: The update cannot be started because all of the content sources were excluded by site path rules, or removed from the index configuration. Context: Windows Application, SystemIndex Catalog Details: (HRESULT : 0x1) (0x00000001)
Application	Warning	3	2015-04-23 08:53:26	Windows Search Service	3037: Crawl could not be started on content source <B:\[2be3cb0f-27a0-48bc-b2b7-f1525ce1859d]\Links\>. Context: Windows Application, SystemIndex Catalog Details: The specified address was excluded from the index. The site path rules may have to be modified to include this address. (HRESULT : 0x80040d07) (0x80040d07)
Application	Warning	3	2015-04-23 08:53:26	Windows Search Service	3023: The update cannot be started because all of the content sources were excluded by site path rules, or removed from the index configuration. Context: Windows Application, SystemIndex Catalog Details: (HRESULT : 0x1) (0x00000001)
Application	Warning	3	2015-04-23 08:53:26	Windows Search Service	3037: Crawl could not be started on content source <B:\[2be3cb0f-27a0-48bc-b2b7-f1525ce1859d]\Music\>. Context: Windows Application, SystemIndex Catalog Details: The specified address was excluded from the index. The site path rules may have to be modified to include this address. (HRESULT : 0x80040d07) (0x80040d07)
Application	Warning	3	2015-04-23	Windows Search Service	3023: The update cannot be started because all of the content sources were excluded by site path rules, or removed from the index configuration. Context: Windows Application, SystemIndex Catalog Details: (HRESULT :

			08:53:26			0x1) (0x00000001)
Application	Warning	3	2015-04-23 08:53:26		Windows Search Service	3037: Crawl could not be started on content source <B:\[2be3cb0f-27a0-48bc-b2b7-f1525ce1859d]\Pictures\>. Context: Windows Application, SystemIndex Catalog Details: The specified address was excluded from the index. The site path rules may have to be modified to include this address. (HRESULT : 0x80040d07) (0x80040d07)
Application	Warning	3	2015-04-23 08:53:26		Windows Search Service	3023: The update cannot be started because all of the content sources were excluded by site path rules, or removed from the index configuration. Context: Windows Application, SystemIndex Catalog Details: (HRESULT : 0x1) (0x00000001)
Application	Warning	3	2015-04-23 08:53:26		Windows Search Service	3037: Crawl could not be started on content source <B:\[2be3cb0f-27a0-48bc-b2b7-f1525ce1859d]\Saved Games\>. Context: Windows Application, SystemIndex Catalog Details: The specified address was excluded from the index. The site path rules may have to be modified to include this address. (HRESULT : 0x80040d07) (0x80040d07)
Application	Warning	3	2015-04-23 08:53:26		Windows Search Service	3023: The update cannot be started because all of the content sources were excluded by site path rules, or removed from the index configuration. Context: Windows Application, SystemIndex Catalog Details: (HRESULT : 0x1) (0x00000001)
Application	Warning	3	2015-04-23 08:53:26		Windows Search Service	3037: Crawl could not be started on content source <B:\[2be3cb0f-27a0-48bc-b2b7-f1525ce1859d]\Searches\>. Context: Windows Application, SystemIndex Catalog Details: The specified address was excluded from the index. The site path rules may have to be modified to include this address. (HRESULT : 0x80040d07) (0x80040d07)
Application	Warning	3	2015-04-23 08:53:26		Windows Search Service	3023: The update cannot be started because all of the content sources were excluded by site path rules, or removed from the index configuration. Context: Windows Application, SystemIndex Catalog Details: (HRESULT : 0x1) (0x00000001)
Application	Warning	3	2015-04-23 08:53:26		Windows Search Service	3037: Crawl could not be started on content source <B:\[2be3cb0f-27a0-48bc-b2b7-f1525ce1859d]\Videos\>. Context: Windows Application, SystemIndex Catalog Details: The specified address was excluded from the index. The site path rules may have to be modified to include this address. (HRESULT : 0x80040d07) (0x80040d07)
Application	Warning	3	2015-04-23 08:53:26		Windows Search Service	3023: The update cannot be started because all of the content sources were excluded by site path rules, or removed from the index configuration. Context: Windows Application, SystemIndex Catalog Details: (HRESULT : 0x1) (0x00000001)
Application	Warning	3	2015-04-23 08:53:27		Windows Search Service	3036: Crawl could not be completed on content source <winrt://{S-1-5-21-1888849264-3803429180-4108621888-1001}/>. Context: Windows Application, SystemIndex Catalog Details: The parameter is incorrect. (HRESULT : 0x80070057) (0x80070057)
Application	Warning	None	2015-04-23 08:53:29		Software Protection Platform Service	8233: The rules engine reported a failed VL activation attempt. Reason:0x8007007B AppId = 0ff1ce15-a989-479d-af46-f275c6370663, SkuId = b322da9c-a2e2-4058-9e4e-f59a6970bd69 Trigger=UserLogon(1)
Application	Error	None	2015-04-23 08:57:26	SYSTEM	Microsoft-Windows-LoadPerf	3012: The performance strings in the Performance registry value is corrupted when process Performance extension counter provider. The BaseIndex value from the Performance registry is the first DWORD in the Data section, LastCounter value is the second DWORD in the Data section, and LastHelp value is the third DWORD in the Data section.
Application	Error	None	2015-04-23 08:57:26	SYSTEM	Microsoft-Windows-LoadPerf	3011: Unloading the performance counter strings for service WmiApRpl (WmiApRpl) failed. The first DWORD in the Data section contains the error code.
Application	Warning	None	2015-04-23 12:33:06		Software Protection Platform Service	8233: The rules engine reported a failed VL activation attempt. Reason:0x8007267C AppId = 0ff1ce15-a989-479d-af46-f275c6370663, SkuId = b322da9c-a2e2-4058-9e4e-f59a6970bd69 Trigger=UserLogon(1)
Application	Error	None	2015-04-23 12:40:15	SYSTEM	Microsoft-Windows-LoadPerf	3012: The performance strings in the Performance registry value is corrupted when process Performance extension counter provider. The BaseIndex value from the Performance registry is the first DWORD in the Data section, LastCounter value is the second DWORD in the Data section, and LastHelp value is the third DWORD in the Data section.
Application	Error	None	2015-04-23 12:40:15	SYSTEM	Microsoft-Windows-LoadPerf	3011: Unloading the performance counter strings for service WmiApRpl (WmiApRpl) failed. The first DWORD in the Data section contains the error code.
Application	Warning	None	2015-04-24 17:31:55		Software Protection Platform Service	8233: The rules engine reported a failed VL activation attempt. Reason:0x8007232B AppId = 0ff1ce15-a989-479d-af46-f275c6370663, SkuId = b322da9c-a2e2-4058-9e4e-f59a6970bd69 Trigger=TimerEvent
Application	Error	3	2015-04-24 17:32:08		Windows Search Service	3079: Notifications for the volume C:\ are not active. Context: Windows Application Details: The parameter is incorrect. (HRESULT : 0x80070057) (0x80070057)
Application	Error	None	2015-04-24 17:33:13	SYSTEM	Microsoft-Windows-LoadPerf	3012: The performance strings in the Performance registry value is corrupted when process Performance extension counter provider. The BaseIndex value from the Performance registry is the first DWORD in the Data section, LastCounter value is the second DWORD in the Data section, and LastHelp value is the third DWORD in the Data section.
			2015-04-			

Application	Error	None	24 17:33:13	SYSTEM	Microsoft-Windows-LoadPerf	3011: Unloading the performance counter strings for service WmiApRpl (WmiApRpl) failed. The first DWORD in the Data section contains the error code.
Application	Error	None	2015-04-24 17:36:38	SYSTEM	Microsoft-Windows-LoadPerf	3012: The performance strings in the Performance registry value is corrupted when process Performance extension counter provider. The BaseIndex value from the Performance registry is the first DWORD in the Data section, LastCounter value is the second DWORD in the Data section, and LastHelp value is the third DWORD in the Data section.
Application	Error	None	2015-04-24 17:36:38	SYSTEM	Microsoft-Windows-LoadPerf	3011: Unloading the performance counter strings for service WmiApRpl (WmiApRpl) failed. The first DWORD in the Data section contains the error code.
Application	Warning	None	2015-04-24 17:58:40		Software Protection Platform Service	8233: The rules engine reported a failed VL activation attempt. Reason:0x8007007B AppId = 0ff1ce15-a989-479d-af46-f275c6370663, SkuId = b322da9c-a2e2-4058-9e4e-f59a6970bd69 Trigger=UserLogon(1)
Application	Warning	None	2015-04-24 17:58:47		Software Protection Platform Service	8233: The rules engine reported a failed VL activation attempt. Reason:0x8007232B AppId = 0ff1ce15-a989-479d-af46-f275c6370663, SkuId = b322da9c-a2e2-4058-9e4e-f59a6970bd69 Trigger=NetworkAvailable
Application	Warning	None	2015-04-24 17:58:49		Software Protection Platform Service	8233: The rules engine reported a failed VL activation attempt. Reason:0x8007232B AppId = 0ff1ce15-a989-479d-af46-f275c6370663, SkuId = b322da9c-a2e2-4058-9e4e-f59a6970bd69 Trigger=NetworkAvailable
Application	Warning	None	2015-04-24 18:00:52		Software Protection Platform Service	8233: The rules engine reported a failed VL activation attempt. Reason:0x8007232B AppId = 0ff1ce15-a989-479d-af46-f275c6370663, SkuId = b322da9c-a2e2-4058-9e4e-f59a6970bd69 Trigger=UserLogon(1)
Application	Warning	None	2015-04-24 18:00:54		Software Protection Platform Service	8233: The rules engine reported a failed VL activation attempt. Reason:0x8007232B AppId = 0ff1ce15-a989-479d-af46-f275c6370663, SkuId = b322da9c-a2e2-4058-9e4e-f59a6970bd69 Trigger=NetworkAvailable
Application	Error	None	2015-04-24 18:04:49	SYSTEM	Microsoft-Windows-LoadPerf	3012: The performance strings in the Performance registry value is corrupted when process Performance extension counter provider. The BaseIndex value from the Performance registry is the first DWORD in the Data section, LastCounter value is the second DWORD in the Data section, and LastHelp value is the third DWORD in the Data section.
Application	Error	None	2015-04-24 18:04:49	SYSTEM	Microsoft-Windows-LoadPerf	3011: Unloading the performance counter strings for service WmiApRpl (WmiApRpl) failed. The first DWORD in the Data section contains the error code.
Application	Warning	None	2015-04-24 18:10:48		Software Protection Platform Service	8233: The rules engine reported a failed VL activation attempt. Reason:0x8007232B AppId = 0ff1ce15-a989-479d-af46-f275c6370663, SkuId = b322da9c-a2e2-4058-9e4e-f59a6970bd69 Trigger=NetworkAvailable
Application	Warning	None	2015-04-24 18:10:51		Software Protection Platform Service	8233: The rules engine reported a failed VL activation attempt. Reason:0x8007232B AppId = 0ff1ce15-a989-479d-af46-f275c6370663, SkuId = b322da9c-a2e2-4058-9e4e-f59a6970bd69 Trigger=UserLogon(1)
Application	Error	None	2015-04-24 18:11:42	SYSTEM	Microsoft-Windows-LoadPerf	3012: The performance strings in the Performance registry value is corrupted when process Performance extension counter provider. The BaseIndex value from the Performance registry is the first DWORD in the Data section, LastCounter value is the second DWORD in the Data section, and LastHelp value is the third DWORD in the Data section.
Application	Error	None	2015-04-24 18:11:42	SYSTEM	Microsoft-Windows-LoadPerf	3011: Unloading the performance counter strings for service WmiApRpl (WmiApRpl) failed. The first DWORD in the Data section contains the error code.
Application	Error	None	2015-04-24 18:14:41	SYSTEM	Microsoft-Windows-LoadPerf	3012: The performance strings in the Performance registry value is corrupted when process Performance extension counter provider. The BaseIndex value from the Performance registry is the first DWORD in the Data section, LastCounter value is the second DWORD in the Data section, and LastHelp value is the third DWORD in the Data section.
Application	Error	None	2015-04-24 18:14:41	SYSTEM	Microsoft-Windows-LoadPerf	3011: Unloading the performance counter strings for service WmiApRpl (WmiApRpl) failed. The first DWORD in the Data section contains the error code.
Application	Error	None	2015-04-24 18:22:10		SideBySide	33: Activation context generation failed for "c:\program files (x86)\IObit\advanced systemcare 8\kb3000850.cab_temp\5666fc85-066a-466c-b765-feb1c72f64a4\amd64_microsoft-windows-narrator_31bf3856ad364e35_6.3.9600.17415_none_af28d3d777766b35\narrator.exe". Dependent Assembly SRH,type="win32",version="1.0.0.0" could not be found. Please use sxstrace.exe for detailed diagnosis.
Application	Error	None	2015-04-24 18:23:13		SideBySide	33: Activation context generation failed for "c:\program files (x86)\IObit\advanced systemcare 8\kb3000850.cab_temp\5666fc85-066a-466c-b765-feb1c72f64a4\wow64_microsoft-windows-narrator_31bf3856ad364e35_6.3.9600.17415_none_b97d7e29abd72d30\narrator.exe". Dependent Assembly SRH,type="win32",version="1.0.0.0" could not be found. Please use sxstrace.exe for detailed diagnosis.
Application	Warning	None	2015-04-24 19:01:36		Software Protection Platform Service	8233: The rules engine reported a failed VL activation attempt. Reason:0x8007232B AppId = 0ff1ce15-a989-479d-af46-f275c6370663, SkuId = b322da9c-a2e2-4058-9e4e-f59a6970bd69 Trigger=NetworkAvailable

Application	Error	None	2015-04-24 19:05:29	SYSTEM	Microsoft-Windows-LoadPerf	3012: The performance strings in the Performance registry value is corrupted when process Performance extension counter provider. The BaseIndex value from the Performance registry is the first DWORD in the Data section, LastCounter value is the second DWORD in the Data section, and LastHelp value is the third DWORD in the Data section.
Application	Error	None	2015-04-24 19:05:29	SYSTEM	Microsoft-Windows-LoadPerf	3011: Unloading the performance counter strings for service WmiApRpl (WmiApRpl) failed. The first DWORD in the Data section contains the error code.
Application	Warning	None	2015-04-24 19:06:52		Software Protection Platform Service	8233: The rules engine reported a failed VL activation attempt. Reason:0x8007232B AppId = 0ff1ce15-a989-479d-af46-f275c6370663, SkuId = b322da9c-a2e2-4058-9e4e-f59a6970bd69 Trigger=UserLogon(1)
Application	Warning	None	2015-04-24 19:38:04		Software Protection Platform Service	8233: The rules engine reported a failed VL activation attempt. Reason:0x8007232B AppId = 0ff1ce15-a989-479d-af46-f275c6370663, SkuId = b322da9c-a2e2-4058-9e4e-f59a6970bd69 Trigger=UserLogon(1)
Application	Warning	None	2015-04-24 19:38:06		Software Protection Platform Service	8233: The rules engine reported a failed VL activation attempt. Reason:0x8007232B AppId = 0ff1ce15-a989-479d-af46-f275c6370663, SkuId = b322da9c-a2e2-4058-9e4e-f59a6970bd69 Trigger=NetworkAvailable
Application	Warning	None	2015-04-24 19:42:03		Software Protection Platform Service	8233: The rules engine reported a failed VL activation attempt. Reason:0x8007232B AppId = 0ff1ce15-a989-479d-af46-f275c6370663, SkuId = b322da9c-a2e2-4058-9e4e-f59a6970bd69 Trigger=UserLogon(1)
Application	Warning	None	2015-04-24 19:42:05		Software Protection Platform Service	8233: The rules engine reported a failed VL activation attempt. Reason:0x8007232B AppId = 0ff1ce15-a989-479d-af46-f275c6370663, SkuId = b322da9c-a2e2-4058-9e4e-f59a6970bd69 Trigger=NetworkAvailable
Application	Error	None	2015-04-24 19:46:02	SYSTEM	Microsoft-Windows-LoadPerf	3012: The performance strings in the Performance registry value is corrupted when process Performance extension counter provider. The BaseIndex value from the Performance registry is the first DWORD in the Data section, LastCounter value is the second DWORD in the Data section, and LastHelp value is the third DWORD in the Data section.
Application	Error	None	2015-04-24 19:46:02	SYSTEM	Microsoft-Windows-LoadPerf	3011: Unloading the performance counter strings for service WmiApRpl (WmiApRpl) failed. The first DWORD in the Data section contains the error code.
Application	Warning	3	2015-04-24 19:50:04		Windows Search Service	3036: Crawl could not be completed on content source <StickyNotes://{S-1-5-21-1888849264-3803429180-4108621888-1001}/notes/>. Context: Application, SystemIndex Catalog Details: The filtering process has been terminated (HRESULT : 0x80040db4) (0x80040db4)
Application	Error	1	2015-04-24 20:35:24		Windows Search Service	7040: The search service has detected corrupted data files in the index {id=4810 - enduser\mssearch2\search\ytrip\common\util\jetutil.cpp (167)}. The service will attempt to automatically correct this problem by rebuilding the index. Details: 0x8e5e0210 (0x8e5e0210)
Application	Error	1	2015-04-24 20:35:24		Windows Search Service	7042: The Windows Search Service is being stopped because there is a problem with the indexer: The catalog is corrupt. Details: The content index catalog is corrupt. 0xc0041801 (0xc0041801)
Application	Error	3	2015-04-24 20:35:24		ESENT	455: SearchIndexer (2260) Windows: Error -1811 (0xfffff8ed) occurred while opening logfile C:\ProgramData\Microsoft\Search\Data\Applications\Windows\edb0000A.log.
Application	Error	3	2015-04-24 20:35:24		Windows Search Service	3057: The plug-in manager <Search.TripoliIndexer> cannot be initialized. Context: Windows Application Details: (HRESULT : 0x8e5e0210) (0x8e5e0210)
Application	Error	3	2015-04-24 20:35:24		Windows Search Service	3029: The plug-in in <Search.TripoliIndexer> cannot be initialized. Context: Windows Application, SystemIndex Catalog Details: The specified object cannot be found. Specify the name of an existing object. (HRESULT : 0x80040d06) (0x80040d06)
Application	Error	3	2015-04-24 20:35:24		Windows Search Service	3028: The gatherer object cannot be initialized. Context: Windows Application, SystemIndex Catalog Details: The specified object cannot be found. Specify the name of an existing object. (HRESULT : 0x80040d06) (0x80040d06)
Application	Error	3	2015-04-24 20:35:24		Windows Search Service	3058: The application cannot be initialized. Context: Windows Application Details: The specified object cannot be found. Specify the name of an existing object. (HRESULT : 0x80040d06) (0x80040d06)
Application	Error	3	2015-04-24 20:35:24		Windows Search Service	7010: The index cannot be initialized. Details: The specified object cannot be found. Specify the name of an existing object. (HRESULT : 0x80040d06) (0x80040d06)
Application	Warning	1	2015-04-24 20:35:25		Windows Search Service	1008: The Windows Search Service is starting up and attempting to remove the old search index {Reason: Index Corruption}.
Application	Error	3	2015-04-24 20:35:26		Windows Search Service	1019: Windows Search Service failed to process the list of included and excluded locations with the error <30, 0x80040d07, "file:///B:\[2be3cb0f-27a0-48bc-b2b7-f1525ce1859d]\Contacts\">.
			2015-04-			

Application	Error	3	24 20:35:26	Windows Search Service	1019: Windows Search Service failed to process the list of included and excluded locations with the error <30, 0x80040d07, "file:///B:\[2be3cb0f-27a0-48bc-b2b7-f1525ce1859d]\Desktop\">.
Application	Error	3	2015-04-24 20:35:26	Windows Search Service	1019: Windows Search Service failed to process the list of included and excluded locations with the error <30, 0x80040d07, "file:///B:\[2be3cb0f-27a0-48bc-b2b7-f1525ce1859d]\Documents\">.
Application	Error	3	2015-04-24 20:35:26	Windows Search Service	1019: Windows Search Service failed to process the list of included and excluded locations with the error <30, 0x80040d07, "file:///B:\[2be3cb0f-27a0-48bc-b2b7-f1525ce1859d]\Downloads\">.
Application	Error	3	2015-04-24 20:35:26	Windows Search Service	1019: Windows Search Service failed to process the list of included and excluded locations with the error <30, 0x80040d07, "file:///B:\[2be3cb0f-27a0-48bc-b2b7-f1525ce1859d]\Favorites\">.
Application	Error	3	2015-04-24 20:35:26	Windows Search Service	1019: Windows Search Service failed to process the list of included and excluded locations with the error <30, 0x80040d07, "file:///B:\[2be3cb0f-27a0-48bc-b2b7-f1525ce1859d]\Links\">.
Application	Error	3	2015-04-24 20:35:26	Windows Search Service	1019: Windows Search Service failed to process the list of included and excluded locations with the error <30, 0x80040d07, "file:///B:\[2be3cb0f-27a0-48bc-b2b7-f1525ce1859d]\Music\">.
Application	Error	3	2015-04-24 20:35:26	Windows Search Service	1019: Windows Search Service failed to process the list of included and excluded locations with the error <30, 0x80040d07, "file:///B:\[2be3cb0f-27a0-48bc-b2b7-f1525ce1859d]\Pictures\">.
Application	Error	3	2015-04-24 20:35:26	Windows Search Service	1019: Windows Search Service failed to process the list of included and excluded locations with the error <30, 0x80040d07, "file:///B:\[2be3cb0f-27a0-48bc-b2b7-f1525ce1859d]\Saved Games\">.
Application	Error	3	2015-04-24 20:35:26	Windows Search Service	1019: Windows Search Service failed to process the list of included and excluded locations with the error <30, 0x80040d07, "file:///B:\[2be3cb0f-27a0-48bc-b2b7-f1525ce1859d]\Searches\">.
Application	Error	3	2015-04-24 20:35:26	Windows Search Service	1019: Windows Search Service failed to process the list of included and excluded locations with the error <30, 0x80040d07, "file:///B:\[2be3cb0f-27a0-48bc-b2b7-f1525ce1859d]\Videos\">.
Application	Warning	3	2015-04-24 20:35:26	Windows Search Service	3037: Crawl could not be started on content source <B:\[2be3cb0f-27a0-48bc-b2b7-f1525ce1859d]\Contacts\>. Context: Windows Application, SystemIndex Catalog Details: The specified address was excluded from the index. The site path rules may have to be modified to include this address. (HRESULT : 0x80040d07) (0x80040d07)
Application	Warning	3	2015-04-24 20:35:26	Windows Search Service	3023: The update cannot be started because all of the content sources were excluded by site path rules, or removed from the index configuration. Context: Windows Application, SystemIndex Catalog Details: (HRESULT : 0x1) (0x00000001)
Application	Warning	3	2015-04-24 20:35:26	Windows Search Service	3037: Crawl could not be started on content source <B:\[2be3cb0f-27a0-48bc-b2b7-f1525ce1859d]\Desktop\>. Context: Windows Application, SystemIndex Catalog Details: The specified address was excluded from the index. The site path rules may have to be modified to include this address. (HRESULT : 0x80040d07) (0x80040d07)
Application	Warning	3	2015-04-24 20:35:26	Windows Search Service	3023: The update cannot be started because all of the content sources were excluded by site path rules, or removed from the index configuration. Context: Windows Application, SystemIndex Catalog Details: (HRESULT : 0x1) (0x00000001)
Application	Warning	3	2015-04-24 20:35:26	Windows Search Service	3037: Crawl could not be started on content source <B:\[2be3cb0f-27a0-48bc-b2b7-f1525ce1859d]\Documents\>. Context: Windows Application, SystemIndex Catalog Details: The specified address was excluded from the index. The site path rules may have to be modified to include this address. (HRESULT : 0x80040d07) (0x80040d07)
Application	Warning	3	2015-04-24 20:35:26	Windows Search Service	3023: The update cannot be started because all of the content sources were excluded by site path rules, or removed from the index configuration. Context: Windows Application, SystemIndex Catalog Details: (HRESULT : 0x1) (0x00000001)
Application	Warning	3	2015-04-24 20:35:26	Windows Search Service	3037: Crawl could not be started on content source <B:\[2be3cb0f-27a0-48bc-b2b7-f1525ce1859d]\Downloads\>. Context: Windows Application, SystemIndex Catalog Details: The specified address was excluded from the index. The site path rules may have to be modified to include this address. (HRESULT : 0x80040d07) (0x80040d07)
Application	Warning	3	2015-04-24 20:35:26	Windows Search Service	3023: The update cannot be started because all of the content sources were excluded by site path rules, or removed from the index configuration. Context: Windows Application, SystemIndex Catalog Details: (HRESULT : 0x1) (0x00000001)
Application	Warning	3	2015-04-24 20:35:26	Windows Search Service	3037: Crawl could not be started on content source <B:\[2be3cb0f-27a0-48bc-b2b7-f1525ce1859d]\Favorites\>. Context: Windows Application, SystemIndex Catalog Details: The specified address was excluded from the index. The site path rules may have to be modified to include this address. (HRESULT : 0x80040d07) (0x80040d07)
			2015-04-		3023: The update cannot be started because all of the content sources were excluded by site path rules, or

	Application	Warning	3	24 20:35:26		Windows Search Service	removed from the index configuration. Context: Windows Application, SystemIndex Catalog Details: (HRESULT : 0x1) (0x00000001)
	Application	Warning	3	2015-04-24 20:35:26		Windows Search Service	3037: Crawl could not be started on content source <B:\[2be3cb0f-27a0-48bc-b2b7-f1525ce1859d]\Links\>. Context: Windows Application, SystemIndex Catalog Details: The specified address was excluded from the index. The site path rules may have to be modified to include this address. (HRESULT : 0x80040d07) (0x80040d07)
	Application	Warning	3	2015-04-24 20:35:26		Windows Search Service	3023: The update cannot be started because all of the content sources were excluded by site path rules, or removed from the index configuration. Context: Windows Application, SystemIndex Catalog Details: (HRESULT : 0x1) (0x00000001)
	Application	Warning	3	2015-04-24 20:35:26		Windows Search Service	3037: Crawl could not be started on content source <B:\[2be3cb0f-27a0-48bc-b2b7-f1525ce1859d]\Music\>. Context: Windows Application, SystemIndex Catalog Details: The specified address was excluded from the index. The site path rules may have to be modified to include this address. (HRESULT : 0x80040d07) (0x80040d07)
	Application	Warning	3	2015-04-24 20:35:26		Windows Search Service	3023: The update cannot be started because all of the content sources were excluded by site path rules, or removed from the index configuration. Context: Windows Application, SystemIndex Catalog Details: (HRESULT : 0x1) (0x00000001)
	Application	Warning	3	2015-04-24 20:35:26		Windows Search Service	3037: Crawl could not be started on content source <B:\[2be3cb0f-27a0-48bc-b2b7-f1525ce1859d]\Pictures\>. Context: Windows Application, SystemIndex Catalog Details: The specified address was excluded from the index. The site path rules may have to be modified to include this address. (HRESULT : 0x80040d07) (0x80040d07)
	Application	Warning	3	2015-04-24 20:35:26		Windows Search Service	3023: The update cannot be started because all of the content sources were excluded by site path rules, or removed from the index configuration. Context: Windows Application, SystemIndex Catalog Details: (HRESULT : 0x1) (0x00000001)
	Application	Warning	3	2015-04-24 20:35:26		Windows Search Service	3037: Crawl could not be started on content source <B:\[2be3cb0f-27a0-48bc-b2b7-f1525ce1859d]\Saved Games\>. Context: Windows Application, SystemIndex Catalog Details: The specified address was excluded from the index. The site path rules may have to be modified to include this address. (HRESULT : 0x80040d07) (0x80040d07)
	Application	Warning	3	2015-04-24 20:35:26		Windows Search Service	3023: The update cannot be started because all of the content sources were excluded by site path rules, or removed from the index configuration. Context: Windows Application, SystemIndex Catalog Details: (HRESULT : 0x1) (0x00000001)
	Application	Warning	3	2015-04-24 20:35:26		Windows Search Service	3037: Crawl could not be started on content source <B:\[2be3cb0f-27a0-48bc-b2b7-f1525ce1859d]\Searches\>. Context: Windows Application, SystemIndex Catalog Details: The specified address was excluded from the index. The site path rules may have to be modified to include this address. (HRESULT : 0x80040d07) (0x80040d07)
	Application	Warning	3	2015-04-24 20:35:26		Windows Search Service	3023: The update cannot be started because all of the content sources were excluded by site path rules, or removed from the index configuration. Context: Windows Application, SystemIndex Catalog Details: (HRESULT : 0x1) (0x00000001)
	Application	Warning	3	2015-04-24 20:35:26		Windows Search Service	3037: Crawl could not be started on content source <B:\[2be3cb0f-27a0-48bc-b2b7-f1525ce1859d]\Videos\>. Context: Windows Application, SystemIndex Catalog Details: The specified address was excluded from the index. The site path rules may have to be modified to include this address. (HRESULT : 0x80040d07) (0x80040d07)
	Application	Warning	3	2015-04-24 20:35:26		Windows Search Service	3023: The update cannot be started because all of the content sources were excluded by site path rules, or removed from the index configuration. Context: Windows Application, SystemIndex Catalog Details: (HRESULT : 0x1) (0x00000001)
	Application	Warning	3	2015-04-24 20:35:26		Windows Search Service	3036: Crawl could not be completed on content source <winrt://{S-1-5-21-1888849264-3803429180-4108621888-1001}/>. Context: Windows Application, SystemIndex Catalog Details: The parameter is incorrect. (HRESULT : 0x80070057) (0x80070057)
	Application	Warning	None	2015-04-24 20:35:29		Software Protection Platform Service	8233: The rules engine reported a failed VL activation attempt. Reason:0x8007232B AppId = 0ff1ce15-a989-479d-af46-f275c6370663, SkuId = b322da9c-a2e2-4058-9e4e-f59a6970bd69 Trigger=UserLogon(1)
	Application	Warning	None	2015-04-24 20:35:32		Software Protection Platform Service	8233: The rules engine reported a failed VL activation attempt. Reason:0x8007232B AppId = 0ff1ce15-a989-479d-af46-f275c6370663, SkuId = b322da9c-a2e2-4058-9e4e-f59a6970bd69 Trigger=NetworkAvailable
	Application	Error	None	2015-04-24 20:39:43	SYSTEM	Microsoft-Windows-LoadPerf	3012: The performance strings in the Performance registry value is corrupted when process Performance extension counter provider. The BaseIndex value from the Performance registry is the first DWORD in the Data section, LastCounter value is the second DWORD in the Data section, and LastHelp value is the third DWORD in the Data section.
	Application	Error	None	2015-04-24 20:39:43	SYSTEM	Microsoft-Windows-LoadPerf	3011: Unloading the performance counter strings for service WmiApRpl (WmiApRpl) failed. The first DWORD in the Data section contains the error code.
	Application	Warning	None	2015-04-24 20:47:14		WlcIntfy	6000: The winlogon notification subscriber <GPClient> was unavailable to handle a notification event.

Application	Warning	None	2015-04-24 20:48:58		WlcIntfy	6000: The winlogon notification subscriber <GPClient> was unavailable to handle a notification event.
Application	Warning	None	2015-04-24 20:48:58		WlcIntfy	6000: The winlogon notification subscriber <GPClient> was unavailable to handle a notification event.
Application	Warning	None	2015-04-24 20:49:20		Software Protection Platform Service	8233: The rules engine reported a failed VL activation attempt. Reason:0x8007232B AppId = 0ff1ce15-a989-479d-af46-f275c6370663, SkuId = b322da9c-a2e2-4058-9e4e-f59a6970bd69 Trigger=UserLogon(1)
Application	Warning	None	2015-04-24 20:49:23		Software Protection Platform Service	8233: The rules engine reported a failed VL activation attempt. Reason:0x8007232B AppId = 0ff1ce15-a989-479d-af46-f275c6370663, SkuId = b322da9c-a2e2-4058-9e4e-f59a6970bd69 Trigger=NetworkAvailable
Application	Warning	None	2015-04-24 20:49:25		Software Protection Platform Service	8233: The rules engine reported a failed VL activation attempt. Reason:0x8007232B AppId = 0ff1ce15-a989-479d-af46-f275c6370663, SkuId = b322da9c-a2e2-4058-9e4e-f59a6970bd69 Trigger=NetworkAvailable
Application	Error	None	2015-04-24 20:55:55	SYSTEM	Microsoft-Windows-LoadPerf	3012: The performance strings in the Performance registry value is corrupted when process Performance extension counter provider. The BaseIndex value from the Performance registry is the first DWORD in the Data section, LastCounter value is the second DWORD in the Data section, and LastHelp value is the third DWORD in the Data section.
Application	Error	None	2015-04-24 20:55:55	SYSTEM	Microsoft-Windows-LoadPerf	3011: Unloading the performance counter strings for service WmiApRpl (WmiApRpl) failed. The first DWORD in the Data section contains the error code.
Application	Warning	None	2015-04-24 21:04:55		Software Protection Platform Service	8233: The rules engine reported a failed VL activation attempt. Reason:0x8007232B AppId = 0ff1ce15-a989-479d-af46-f275c6370663, SkuId = b322da9c-a2e2-4058-9e4e-f59a6970bd69 Trigger=UserLogon(1)
Application	Warning	None	2015-04-24 21:04:58		Software Protection Platform Service	8233: The rules engine reported a failed VL activation attempt. Reason:0x8007232B AppId = 0ff1ce15-a989-479d-af46-f275c6370663, SkuId = b322da9c-a2e2-4058-9e4e-f59a6970bd69 Trigger=NetworkAvailable
Application	Error	None	2015-04-24 21:05:18		AdvancedSystemCareService8	0:
Application	Error	None	2015-04-24 21:05:18		AdvancedSystemCareService8	0:
Application	Warning	None	2015-04-24 21:06:26		Software Protection Platform Service	8233: The rules engine reported a failed VL activation attempt. Reason:0x8007267C AppId = 0ff1ce15-a989-479d-af46-f275c6370663, SkuId = b322da9c-a2e2-4058-9e4e-f59a6970bd69 Trigger=UserLogon(1)
Application	Warning	None	2015-04-24 21:06:32		Software Protection Platform Service	8233: The rules engine reported a failed VL activation attempt. Reason:0x8007232B AppId = 0ff1ce15-a989-479d-af46-f275c6370663, SkuId = b322da9c-a2e2-4058-9e4e-f59a6970bd69 Trigger=NetworkAvailable
Application	Warning	None	2015-04-24 21:06:35		Software Protection Platform Service	8233: The rules engine reported a failed VL activation attempt. Reason:0x8007232B AppId = 0ff1ce15-a989-479d-af46-f275c6370663, SkuId = b322da9c-a2e2-4058-9e4e-f59a6970bd69 Trigger=NetworkAvailable
Application	Error	None	2015-04-24 21:10:36	SYSTEM	Microsoft-Windows-LoadPerf	3012: The performance strings in the Performance registry value is corrupted when process Performance extension counter provider. The BaseIndex value from the Performance registry is the first DWORD in the Data section, LastCounter value is the second DWORD in the Data section, and LastHelp value is the third DWORD in the Data section.
Application	Error	None	2015-04-24 21:10:36	SYSTEM	Microsoft-Windows-LoadPerf	3011: Unloading the performance counter strings for service WmiApRpl (WmiApRpl) failed. The first DWORD in the Data section contains the error code.
Application	Warning	None	2015-04-24 21:36:43		Software Protection Platform Service	8233: The rules engine reported a failed VL activation attempt. Reason:0x8007232B AppId = 0ff1ce15-a989-479d-af46-f275c6370663, SkuId = b322da9c-a2e2-4058-9e4e-f59a6970bd69 Trigger=UserLogon(1)
Application	Warning	None	2015-04-24 21:36:46		Software Protection Platform Service	8233: The rules engine reported a failed VL activation attempt. Reason:0x8007232B AppId = 0ff1ce15-a989-479d-af46-f275c6370663, SkuId = b322da9c-a2e2-4058-9e4e-f59a6970bd69 Trigger=NetworkAvailable
Application	Error	None	2015-04-24 21:40:53	SYSTEM	Microsoft-Windows-LoadPerf	3012: The performance strings in the Performance registry value is corrupted when process Performance extension counter provider. The BaseIndex value from the Performance registry is the first DWORD in the Data section, LastCounter value is the second DWORD in the Data section, and LastHelp value is the third DWORD in the Data section.
Application	Error	None	2015-04-24 21:40:53	SYSTEM	Microsoft-Windows-LoadPerf	3011: Unloading the performance counter strings for service WmiApRpl (WmiApRpl) failed. The first DWORD in the Data section contains the error code.

Application	Warning	None	2015-04-24 22:06:50		Software Protection Platform Service	8233: The rules engine reported a failed VL activation attempt. Reason:0x8007232B AppId = 0ff1ce15-a989-479d-af46-f275c6370663, SkuId = b322da9c-a2e2-4058-9e4e-f59a6970bd69 Trigger=UserLogon(1)
Application	Warning	None	2015-04-24 22:06:53		Software Protection Platform Service	8233: The rules engine reported a failed VL activation attempt. Reason:0x8007232B AppId = 0ff1ce15-a989-479d-af46-f275c6370663, SkuId = b322da9c-a2e2-4058-9e4e-f59a6970bd69 Trigger=NetworkAvailable
Application	Error	None	2015-04-24 22:10:52	SYSTEM	Microsoft-Windows-LoadPerf	3012: The performance strings in the Performance registry value is corrupted when process Performance extension counter provider. The BaseIndex value from the Performance registry is the first DWORD in the Data section, LastCounter value is the second DWORD in the Data section, and LastHelp value is the third DWORD in the Data section.
Application	Error	None	2015-04-24 22:10:52	SYSTEM	Microsoft-Windows-LoadPerf	3011: Unloading the performance counter strings for service WmiApRpl (WmiApRpl) failed. The first DWORD in the Data section contains the error code.
Application	Warning	None	2015-04-24 22:16:57		Software Protection Platform Service	8233: The rules engine reported a failed VL activation attempt. Reason:0x8007267C AppId = 0ff1ce15-a989-479d-af46-f275c6370663, SkuId = b322da9c-a2e2-4058-9e4e-f59a6970bd69 Trigger=UserLogon(1)
Application	Warning	None	2015-04-24 22:17:03		Software Protection Platform Service	8233: The rules engine reported a failed VL activation attempt. Reason:0x8007232B AppId = 0ff1ce15-a989-479d-af46-f275c6370663, SkuId = b322da9c-a2e2-4058-9e4e-f59a6970bd69 Trigger=NetworkAvailable
Application	Warning	None	2015-04-24 22:17:07		Software Protection Platform Service	8233: The rules engine reported a failed VL activation attempt. Reason:0x8007232B AppId = 0ff1ce15-a989-479d-af46-f275c6370663, SkuId = b322da9c-a2e2-4058-9e4e-f59a6970bd69 Trigger=NetworkAvailable
Application	Error	None	2015-04-24 22:21:05	SYSTEM	Microsoft-Windows-LoadPerf	3012: The performance strings in the Performance registry value is corrupted when process Performance extension counter provider. The BaseIndex value from the Performance registry is the first DWORD in the Data section, LastCounter value is the second DWORD in the Data section, and LastHelp value is the third DWORD in the Data section.
Application	Error	None	2015-04-24 22:21:05	SYSTEM	Microsoft-Windows-LoadPerf	3011: Unloading the performance counter strings for service WmiApRpl (WmiApRpl) failed. The first DWORD in the Data section contains the error code.
Application	Warning	None	2015-04-24 22:33:33		Software Protection Platform Service	8233: The rules engine reported a failed VL activation attempt. Reason:0x8007232B AppId = 0ff1ce15-a989-479d-af46-f275c6370663, SkuId = b322da9c-a2e2-4058-9e4e-f59a6970bd69 Trigger=NetworkAvailable
Application	Warning	None	2015-04-24 22:33:50		Software Protection Platform Service	8233: The rules engine reported a failed VL activation attempt. Reason:0x8007232B AppId = 0ff1ce15-a989-479d-af46-f275c6370663, SkuId = b322da9c-a2e2-4058-9e4e-f59a6970bd69 Trigger=UserLogon(2)
Application	Warning	None	2015-04-25 07:22:41		Software Protection Platform Service	8233: The rules engine reported a failed VL activation attempt. Reason:0x8007267C AppId = 0ff1ce15-a989-479d-af46-f275c6370663, SkuId = b322da9c-a2e2-4058-9e4e-f59a6970bd69 Trigger=UserLogon(1)
Application	Warning	None	2015-04-25 07:22:46		Software Protection Platform Service	8233: The rules engine reported a failed VL activation attempt. Reason:0x8007232B AppId = 0ff1ce15-a989-479d-af46-f275c6370663, SkuId = b322da9c-a2e2-4058-9e4e-f59a6970bd69 Trigger=NetworkAvailable
Application	Warning	None	2015-04-25 07:22:53		Software Protection Platform Service	8233: The rules engine reported a failed VL activation attempt. Reason:0x8007232B AppId = 0ff1ce15-a989-479d-af46-f275c6370663, SkuId = b322da9c-a2e2-4058-9e4e-f59a6970bd69 Trigger=NetworkAvailable
Application	Error	3	2015-04-25 07:26:39		Windows Search Service	3079: Notifications for the volume C:\ are not active. Context: Windows Application Details: The parameter is incorrect. (HRESULT : 0x80070057) (0x80070057)
Application	Warning	3	2015-04-25 07:26:40		Windows Search Service	3036: Crawl could not be completed on content source <winrt://{S-1-5-21-1888849264-3803429180-4108621888-1001}/>. Context: Application, SystemIndex Catalog Details: The parameter is incorrect. (HRESULT : 0x80070057) (0x80070057)
Application	Error	None	2015-04-25 07:26:51	SYSTEM	Microsoft-Windows-LoadPerf	3012: The performance strings in the Performance registry value is corrupted when process Performance extension counter provider. The BaseIndex value from the Performance registry is the first DWORD in the Data section, LastCounter value is the second DWORD in the Data section, and LastHelp value is the third DWORD in the Data section.
Application	Error	None	2015-04-25 07:26:51	SYSTEM	Microsoft-Windows-LoadPerf	3011: Unloading the performance counter strings for service WmiApRpl (WmiApRpl) failed. The first DWORD in the Data section contains the error code.
Application	Warning	None	2015-04-25 07:53:04		Software Protection Platform Service	8233: The rules engine reported a failed VL activation attempt. Reason:0x8007232B AppId = 0ff1ce15-a989-479d-af46-f275c6370663, SkuId = b322da9c-a2e2-4058-9e4e-f59a6970bd69 Trigger=NetworkAvailable
Application	Warning	None	2015-04-25 07:53:07		Software Protection Platform Service	8233: The rules engine reported a failed VL activation attempt. Reason:0x8007232B AppId = 0ff1ce15-a989-479d-af46-f275c6370663, SkuId = b322da9c-a2e2-4058-9e4e-f59a6970bd69 Trigger=UserLogon(1)

	Application	Warning	3	2015-04-25 07:56:59		Windows Search Service	3036: Crawl could not be completed on content source <winrt://{S-1-5-21-1888849264-3803429180-4108621888-1001}/>. Context: Application, SystemIndex Catalog Details: The parameter is incorrect. (HRESULT : 0x80070057) (0x80070057)
	Application	Error	None	2015-04-25 07:57:01	SYSTEM	Microsoft-Windows-LoadPerf	3012: The performance strings in the Performance registry value is corrupted when process Performance extension counter provider. The BaseIndex value from the Performance registry is the first DWORD in the Data section, LastCounter value is the second DWORD in the Data section, and LastHelp value is the third DWORD in the Data section.
	Application	Error	None	2015-04-25 07:57:01	SYSTEM	Microsoft-Windows-LoadPerf	3011: Unloading the performance counter strings for service WmiApRpl (WmiApRpl) failed. The first DWORD in the Data section contains the error code.
	Application	Warning	None	2015-04-25 07:58:04		Software Protection Platform Service	8233: The rules engine reported a failed VL activation attempt. Reason:0x8007232B AppId = 0ff1ce15-a989-479d-af46-f275c6370663, SkuId = b322da9c-a2e2-4058-9e4e-f59a6970bd69 Trigger=NetworkQuarantineRetry
	Application	Error	None	2015-04-25 08:05:30		SideBySide	33: Activation context generation failed for "c:\program files (x86)\IObit\advanced systemcare 8\kb3000850.cab_temp\5666fc85-066a-466c-b765-feb1c72f64a4\amd64_microsoft-windows-narrator_31bf3856ad364e35_6.3.9600.17415_none_af28d3d777766b35\narrator.exe". Dependent Assembly SRH,type="win32",version="1.0.0.0" could not be found. Please use sxstrace.exe for detailed diagnosis.
	Application	Error	None	2015-04-25 08:06:12		SideBySide	33: Activation context generation failed for "c:\program files (x86)\IObit\advanced systemcare 8\kb3000850.cab_temp\5666fc85-066a-466c-b765-feb1c72f64a4\wow64_microsoft-windows-narrator_31bf3856ad364e35_6.3.9600.17415_none_b97d7e29abd72d30\narrator.exe". Dependent Assembly SRH,type="win32",version="1.0.0.0" could not be found. Please use sxstrace.exe for detailed diagnosis.
	Application	Warning	None	2015-04-25 08:14:37		Software Protection Platform Service	8233: The rules engine reported a failed VL activation attempt. Reason:0x8007232B AppId = 0ff1ce15-a989-479d-af46-f275c6370663, SkuId = b322da9c-a2e2-4058-9e4e-f59a6970bd69 Trigger=NetworkAvailable
	Application	Warning	None	2015-04-25 08:14:46		Software Protection Platform Service	8233: The rules engine reported a failed VL activation attempt. Reason:0x8007232B AppId = 0ff1ce15-a989-479d-af46-f275c6370663, SkuId = b322da9c-a2e2-4058-9e4e-f59a6970bd69 Trigger=NetworkAvailable
	Application	Warning	None	2015-04-25 08:19:46		Software Protection Platform Service	8233: The rules engine reported a failed VL activation attempt. Reason:0x8007232B AppId = 0ff1ce15-a989-479d-af46-f275c6370663, SkuId = b322da9c-a2e2-4058-9e4e-f59a6970bd69 Trigger=NetworkQuarantineRetry
	Application	Error	None	2015-04-25 08:25:41		SideBySide	33: Activation context generation failed for "c:\program files (x86)\IObit\advanced systemcare 8\kb3000850.cab_temp\5666fc85-066a-466c-b765-feb1c72f64a4\amd64_microsoft-windows-narrator_31bf3856ad364e35_6.3.9600.17415_none_af28d3d777766b35\narrator.exe". Dependent Assembly SRH,type="win32",version="1.0.0.0" could not be found. Please use sxstrace.exe for detailed diagnosis.
	Application	Error	None	2015-04-25 08:25:44		SideBySide	33: Activation context generation failed for "c:\program files (x86)\IObit\advanced systemcare 8\kb3000850.cab_temp\5666fc85-066a-466c-b765-feb1c72f64a4\wow64_microsoft-windows-narrator_31bf3856ad364e35_6.3.9600.17415_none_b97d7e29abd72d30\narrator.exe". Dependent Assembly SRH,type="win32",version="1.0.0.0" could not be found. Please use sxstrace.exe for detailed diagnosis.
	Application	Warning	None	2015-04-25 08:45:11		Software Protection Platform Service	8233: The rules engine reported a failed VL activation attempt. Reason:0x8007232B AppId = 0ff1ce15-a989-479d-af46-f275c6370663, SkuId = b322da9c-a2e2-4058-9e4e-f59a6970bd69 Trigger=NetworkAvailable
	Application	Warning	None	2015-04-25 08:46:04		Software Protection Platform Service	8233: The rules engine reported a failed VL activation attempt. Reason:0x8007232B AppId = 0ff1ce15-a989-479d-af46-f275c6370663, SkuId = b322da9c-a2e2-4058-9e4e-f59a6970bd69 Trigger=UserLogon(1)
	Application	Warning	None	2015-04-25 08:46:06		Software Protection Platform Service	8233: The rules engine reported a failed VL activation attempt. Reason:0x8007232B AppId = 0ff1ce15-a989-479d-af46-f275c6370663, SkuId = b322da9c-a2e2-4058-9e4e-f59a6970bd69 Trigger=NetworkAvailable
	Application	Error	None	2015-04-25 08:47:08	SYSTEM	Microsoft-Windows-LoadPerf	3012: The performance strings in the Performance registry value is corrupted when process Performance extension counter provider. The BaseIndex value from the Performance registry is the first DWORD in the Data section, LastCounter value is the second DWORD in the Data section, and LastHelp value is the third DWORD in the Data section.
	Application	Error	None	2015-04-25 08:47:08	SYSTEM	Microsoft-Windows-LoadPerf	3011: Unloading the performance counter strings for service WmiApRpl (WmiApRpl) failed. The first DWORD in the Data section contains the error code.
	Application	Error	None	2015-04-25 08:50:31	SYSTEM	Microsoft-Windows-LoadPerf	3012: The performance strings in the Performance registry value is corrupted when process Performance extension counter provider. The BaseIndex value from the Performance registry is the first DWORD in the Data section, LastCounter value is the second DWORD in the Data section, and LastHelp value is the third DWORD in the Data section.
	Application	Error	None	2015-04-25 08:50:31	SYSTEM	Microsoft-Windows-LoadPerf	3011: Unloading the performance counter strings for service WmiApRpl (WmiApRpl) failed. The first DWORD in the Data section contains the error code.
	Application	Warning	None	2015-04-25		Software Protection Platform Service	8233: The rules engine reported a failed VL activation attempt. Reason:0x8007232B AppId = 0ff1ce15-a989-479d-af46-f275c6370663, SkuId = b322da9c-a2e2-4058-9e4e-f59a6970bd69 Trigger=NetworkAvailable

			09:01:25			
Application	Warning	None	2015-04-25 09:01:32		Software Protection Platform Service	8233: The rules engine reported a failed VL activation attempt. Reason:0x8007232B AppId = 0ff1ce15-a989-479d-af46-f275c6370663, SkuId = b322da9c-a2e2-4058-9e4e-f59a6970bd69 Trigger=NetworkAvailable
Application	Warning	None	2015-04-25 09:02:47		Software Protection Platform Service	8233: The rules engine reported a failed VL activation attempt. Reason:0x8007232B AppId = 0ff1ce15-a989-479d-af46-f275c6370663, SkuId = b322da9c-a2e2-4058-9e4e-f59a6970bd69 Trigger=NetworkAvailable
Application	Warning	None	2015-04-25 09:02:53		Software Protection Platform Service	8233: The rules engine reported a failed VL activation attempt. Reason:0x8007232B AppId = 0ff1ce15-a989-479d-af46-f275c6370663, SkuId = b322da9c-a2e2-4058-9e4e-f59a6970bd69 Trigger=NetworkAvailable
Application	Warning	None	2015-04-25 09:07:53		Software Protection Platform Service	8233: The rules engine reported a failed VL activation attempt. Reason:0x8007232B AppId = 0ff1ce15-a989-479d-af46-f275c6370663, SkuId = b322da9c-a2e2-4058-9e4e-f59a6970bd69 Trigger=NetworkQuarantineRetry
Application	Warning	None	2015-04-25 10:14:34		Software Protection Platform Service	8233: The rules engine reported a failed VL activation attempt. Reason:0x8007232B AppId = 0ff1ce15-a989-479d-af46-f275c6370663, SkuId = b322da9c-a2e2-4058-9e4e-f59a6970bd69 Trigger=UserLogon(1)
Application	Warning	None	2015-04-25 10:14:36		Software Protection Platform Service	8233: The rules engine reported a failed VL activation attempt. Reason:0x8007232B AppId = 0ff1ce15-a989-479d-af46-f275c6370663, SkuId = b322da9c-a2e2-4058-9e4e-f59a6970bd69 Trigger=NetworkAvailable
Application	Error	None	2015-04-25 10:18:33	SYSTEM	Microsoft-Windows-LoadPerf	3012: The performance strings in the Performance registry value is corrupted when process Performance extension counter provider. The BaseIndex value from the Performance registry is the first DWORD in the Data section, LastCounter value is the second DWORD in the Data section, and LastHelp value is the third DWORD in the Data section.
Application	Error	None	2015-04-25 10:18:33	SYSTEM	Microsoft-Windows-LoadPerf	3011: Unloading the performance counter strings for service WmiApRpl (WmiApRpl) failed. The first DWORD in the Data section contains the error code.
Application	Warning	None	2015-04-25 10:38:02		Software Protection Platform Service	8233: The rules engine reported a failed VL activation attempt. Reason:0x8007267C AppId = 0ff1ce15-a989-479d-af46-f275c6370663, SkuId = b322da9c-a2e2-4058-9e4e-f59a6970bd69 Trigger=UserLogon(1)
Application	Warning	None	2015-04-25 10:38:09		Software Protection Platform Service	8233: The rules engine reported a failed VL activation attempt. Reason:0x8007232B AppId = 0ff1ce15-a989-479d-af46-f275c6370663, SkuId = b322da9c-a2e2-4058-9e4e-f59a6970bd69 Trigger=NetworkAvailable
Application	Warning	None	2015-04-25 10:38:11		Software Protection Platform Service	8233: The rules engine reported a failed VL activation attempt. Reason:0x8007232B AppId = 0ff1ce15-a989-479d-af46-f275c6370663, SkuId = b322da9c-a2e2-4058-9e4e-f59a6970bd69 Trigger=NetworkAvailable
Application	Error	None	2015-04-25 10:39:27	SYSTEM	Microsoft-Windows-LoadPerf	3012: The performance strings in the Performance registry value is corrupted when process Performance extension counter provider. The BaseIndex value from the Performance registry is the first DWORD in the Data section, LastCounter value is the second DWORD in the Data section, and LastHelp value is the third DWORD in the Data section.
Application	Error	None	2015-04-25 10:39:27	SYSTEM	Microsoft-Windows-LoadPerf	3011: Unloading the performance counter strings for service WmiApRpl (WmiApRpl) failed. The first DWORD in the Data section contains the error code.
Application	Warning	None	2015-04-25 10:42:31		Software Protection Platform Service	8233: The rules engine reported a failed VL activation attempt. Reason:0x8007267C AppId = 0ff1ce15-a989-479d-af46-f275c6370663, SkuId = b322da9c-a2e2-4058-9e4e-f59a6970bd69 Trigger=UserLogon(1)
Application	Warning	None	2015-04-25 10:42:37		Software Protection Platform Service	8233: The rules engine reported a failed VL activation attempt. Reason:0x8007232B AppId = 0ff1ce15-a989-479d-af46-f275c6370663, SkuId = b322da9c-a2e2-4058-9e4e-f59a6970bd69 Trigger=NetworkAvailable
Application	Warning	None	2015-04-25 10:42:41		Software Protection Platform Service	8233: The rules engine reported a failed VL activation attempt. Reason:0x8007232B AppId = 0ff1ce15-a989-479d-af46-f275c6370663, SkuId = b322da9c-a2e2-4058-9e4e-f59a6970bd69 Trigger=NetworkAvailable
Application	Warning	None	2015-04-25 10:48:34		Software Protection Platform Service	8233: The rules engine reported a failed VL activation attempt. Reason:0x8007232B AppId = 0ff1ce15-a989-479d-af46-f275c6370663, SkuId = b322da9c-a2e2-4058-9e4e-f59a6970bd69 Trigger=UserLogon(1)
Application	Error	None	2015-04-25 10:48:35		Software Protection Platform Service	8200: License acquisition failure details. hr=0xC004C008
Application	Error	None	2015-04-25 10:48:35		Software Protection Platform Service	1014: Acquisition of End User License failed. hr=0xC004C008 Sku Id=8da2dfae-e4f5-4e6a-9272-96f8470e033e
Application	Error	None	2015-04-25		Software Protection Platform Service	8198: License Activation (slui.exe) failed with the following error code: hr=0xC004C008 Command-line arguments: RuleId=31e71c49-8da7-4a2f-ad92-45d98a1c79ba;Action=AutoActivate;AppId=55c92734-d682-4d71-983e-d6ec3f16059f;SkuId=8da2dfae-e4f5-4e6a-9272-

			10:48:35			96f8470e033e;NotificationInterval=1440;Trigger=UserLogon;SessionId=1
Application	Warning	None	2015-04-25 10:48:38		Software Protection Platform Service	8233: The rules engine reported a failed VL activation attempt. Reason:0x8007232B AppId = 0ff1ce15-a989-479d-af46-f275c6370663, SkuId = b322da9c-a2e2-4058-9e4e-f59a6970bd69 Trigger=NetworkAvailable
Application	Error	None	2015-04-25 10:52:43	SYSTEM	Microsoft-Windows-LoadPerf	3012: The performance strings in the Performance registry value is corrupted when process Performance extension counter provider. The BaseIndex value from the Performance registry is the first DWORD in the Data section, LastCounter value is the second DWORD in the Data section, and LastHelp value is the third DWORD in the Data section.
Application	Error	None	2015-04-25 10:52:43	SYSTEM	Microsoft-Windows-LoadPerf	3011: Unloading the performance counter strings for service WmiApRpl (WmiApRpl) failed. The first DWORD in the Data section contains the error code.
Application	Warning	None	2015-04-25 11:12:05		Software Protection Platform Service	8233: The rules engine reported a failed VL activation attempt. Reason:0x8007232B AppId = 0ff1ce15-a989-479d-af46-f275c6370663, SkuId = b322da9c-a2e2-4058-9e4e-f59a6970bd69 Trigger=UserLogon(1)
Application	Warning	None	2015-04-25 11:12:08		Software Protection Platform Service	8233: The rules engine reported a failed VL activation attempt. Reason:0x8007232B AppId = 0ff1ce15-a989-479d-af46-f275c6370663, SkuId = b322da9c-a2e2-4058-9e4e-f59a6970bd69 Trigger=NetworkAvailable
Application	Warning	None	2015-04-25 11:12:10		Software Protection Platform Service	8233: The rules engine reported a failed VL activation attempt. Reason:0x8007232B AppId = 0ff1ce15-a989-479d-af46-f275c6370663, SkuId = b322da9c-a2e2-4058-9e4e-f59a6970bd69 Trigger=NetworkAvailable
Application	Error	None	2015-04-25 11:12:11		AdvancedSystemCareService8	0:
Application	Warning	None	2015-04-25 11:12:31		Software Protection Platform Service	8233: The rules engine reported a failed VL activation attempt. Reason:0x8007232B AppId = 0ff1ce15-a989-479d-af46-f275c6370663, SkuId = b322da9c-a2e2-4058-9e4e-f59a6970bd69 Trigger=UserLogon(1)
Application	Warning	None	2015-04-25 11:12:34		Software Protection Platform Service	8233: The rules engine reported a failed VL activation attempt. Reason:0x8007232B AppId = 0ff1ce15-a989-479d-af46-f275c6370663, SkuId = b322da9c-a2e2-4058-9e4e-f59a6970bd69 Trigger=NetworkAvailable
Application	Error	None	2015-04-25 11:13:52	SYSTEM	Microsoft-Windows-LoadPerf	3012: The performance strings in the Performance registry value is corrupted when process Performance extension counter provider. The BaseIndex value from the Performance registry is the first DWORD in the Data section, LastCounter value is the second DWORD in the Data section, and LastHelp value is the third DWORD in the Data section.
Application	Error	None	2015-04-25 11:13:52	SYSTEM	Microsoft-Windows-LoadPerf	3011: Unloading the performance counter strings for service WmiApRpl (WmiApRpl) failed. The first DWORD in the Data section contains the error code.
Application	Error	None	2015-04-25 11:16:59	SYSTEM	Microsoft-Windows-LoadPerf	3012: The performance strings in the Performance registry value is corrupted when process Performance extension counter provider. The BaseIndex value from the Performance registry is the first DWORD in the Data section, LastCounter value is the second DWORD in the Data section, and LastHelp value is the third DWORD in the Data section.
Application	Error	None	2015-04-25 11:16:59	SYSTEM	Microsoft-Windows-LoadPerf	3011: Unloading the performance counter strings for service WmiApRpl (WmiApRpl) failed. The first DWORD in the Data section contains the error code.
Application	Warning	None	2015-04-25 15:32:58		Software Protection Platform Service	8233: The rules engine reported a failed VL activation attempt. Reason:0x8007232B AppId = 0ff1ce15-a989-479d-af46-f275c6370663, SkuId = b322da9c-a2e2-4058-9e4e-f59a6970bd69 Trigger=UserLogon(1)
Application	Warning	None	2015-04-25 15:33:01		Software Protection Platform Service	8233: The rules engine reported a failed VL activation attempt. Reason:0x8007232B AppId = 0ff1ce15-a989-479d-af46-f275c6370663, SkuId = b322da9c-a2e2-4058-9e4e-f59a6970bd69 Trigger=NetworkAvailable
Application	Warning	None	2015-04-25 15:33:03		Software Protection Platform Service	8233: The rules engine reported a failed VL activation attempt. Reason:0x8007232B AppId = 0ff1ce15-a989-479d-af46-f275c6370663, SkuId = b322da9c-a2e2-4058-9e4e-f59a6970bd69 Trigger=NetworkAvailable
Application	Error	3	2015-04-25 15:36:49		Windows Search Service	3079: Notifications for the volume C:\ are not active. Context: Windows Application Details: The parameter is incorrect. (HRESULT : 0x80070057) (0x80070057)
Application	Error	None	2015-04-25 15:37:27	SYSTEM	Microsoft-Windows-LoadPerf	3012: The performance strings in the Performance registry value is corrupted when process Performance extension counter provider. The BaseIndex value from the Performance registry is the first DWORD in the Data section, LastCounter value is the second DWORD in the Data section, and LastHelp value is the third DWORD in the Data section.
Application	Error	None	2015-04-25 15:37:27	SYSTEM	Microsoft-Windows-LoadPerf	3011: Unloading the performance counter strings for service WmiApRpl (WmiApRpl) failed. The first DWORD in the Data section contains the error code.

Application	Warning	None	2015-04-25 16:03:11		Software Protection Platform Service	8233: The rules engine reported a failed VL activation attempt. Reason:0x8007232B AppId = 0ff1ce15-a989-479d-af46-f275c6370663, SkuId = b322da9c-a2e2-4058-9e4e-f59a6970bd69 Trigger=UserLogon(1)
Application	Warning	None	2015-04-25 16:03:14		Software Protection Platform Service	8233: The rules engine reported a failed VL activation attempt. Reason:0x8007232B AppId = 0ff1ce15-a989-479d-af46-f275c6370663, SkuId = b322da9c-a2e2-4058-9e4e-f59a6970bd69 Trigger=NetworkAvailable
Application	Error	None	2015-04-25 16:07:23	SYSTEM	Microsoft-Windows-LoadPerf	3012: The performance strings in the Performance registry value is corrupted when process Performance extension counter provider. The BaseIndex value from the Performance registry is the first DWORD in the Data section, LastCounter value is the second DWORD in the Data section, and LastHelp value is the third DWORD in the Data section.
Application	Error	None	2015-04-25 16:07:23	SYSTEM	Microsoft-Windows-LoadPerf	3011: Unloading the performance counter strings for service WmiApRpl (WmiApRpl) failed. The first DWORD in the Data section contains the error code.
Application	Warning	None	2015-04-25 17:13:37		Software Protection Platform Service	8233: The rules engine reported a failed VL activation attempt. Reason:0x8007232B AppId = 0ff1ce15-a989-479d-af46-f275c6370663, SkuId = b322da9c-a2e2-4058-9e4e-f59a6970bd69 Trigger=NetworkAvailable
Application	Warning	None	2015-04-25 17:13:39		Software Protection Platform Service	8233: The rules engine reported a failed VL activation attempt. Reason:0x8007232B AppId = 0ff1ce15-a989-479d-af46-f275c6370663, SkuId = b322da9c-a2e2-4058-9e4e-f59a6970bd69 Trigger=UserLogon(1)
Application	Error	None	2015-04-25 17:17:31	SYSTEM	Microsoft-Windows-LoadPerf	3012: The performance strings in the Performance registry value is corrupted when process Performance extension counter provider. The BaseIndex value from the Performance registry is the first DWORD in the Data section, LastCounter value is the second DWORD in the Data section, and LastHelp value is the third DWORD in the Data section.
Application	Error	None	2015-04-25 17:17:31	SYSTEM	Microsoft-Windows-LoadPerf	3011: Unloading the performance counter strings for service WmiApRpl (WmiApRpl) failed. The first DWORD in the Data section contains the error code.
Application	Warning	None	2015-04-25 17:49:53		Software Protection Platform Service	8233: The rules engine reported a failed VL activation attempt. Reason:0x8007232B AppId = 0ff1ce15-a989-479d-af46-f275c6370663, SkuId = b322da9c-a2e2-4058-9e4e-f59a6970bd69 Trigger=NetworkAvailable
Application	Warning	None	2015-04-25 17:49:55		Software Protection Platform Service	8233: The rules engine reported a failed VL activation attempt. Reason:0x8007232B AppId = 0ff1ce15-a989-479d-af46-f275c6370663, SkuId = b322da9c-a2e2-4058-9e4e-f59a6970bd69 Trigger=UserLogon(1)
Application	Warning	None	2015-04-25 17:49:58		Software Protection Platform Service	8233: The rules engine reported a failed VL activation attempt. Reason:0x8007232B AppId = 0ff1ce15-a989-479d-af46-f275c6370663, SkuId = b322da9c-a2e2-4058-9e4e-f59a6970bd69 Trigger=NetworkAvailable
Application	Error	None	2015-04-25 17:54:03	SYSTEM	Microsoft-Windows-LoadPerf	3012: The performance strings in the Performance registry value is corrupted when process Performance extension counter provider. The BaseIndex value from the Performance registry is the first DWORD in the Data section, LastCounter value is the second DWORD in the Data section, and LastHelp value is the third DWORD in the Data section.
Application	Error	None	2015-04-25 17:54:03	SYSTEM	Microsoft-Windows-LoadPerf	3011: Unloading the performance counter strings for service WmiApRpl (WmiApRpl) failed. The first DWORD in the Data section contains the error code.
Application	Warning	None	2015-04-26 08:56:39		Software Protection Platform Service	8233: The rules engine reported a failed VL activation attempt. Reason:0x8007232B AppId = 0ff1ce15-a989-479d-af46-f275c6370663, SkuId = b322da9c-a2e2-4058-9e4e-f59a6970bd69 Trigger=UserLogon(1)
Application	Warning	None	2015-04-26 08:56:42		Software Protection Platform Service	8233: The rules engine reported a failed VL activation attempt. Reason:0x8007232B AppId = 0ff1ce15-a989-479d-af46-f275c6370663, SkuId = b322da9c-a2e2-4058-9e4e-f59a6970bd69 Trigger=NetworkAvailable
Application	Error	3	2015-04-26 09:00:24		Windows Search Service	3079: Notifications for the volume C:\ are not active. Context: Windows Application Details: The parameter is incorrect. (HRESULT : 0x80070057) (0x80070057)
Application	Error	None	2015-04-26 09:01:06	SYSTEM	Microsoft-Windows-LoadPerf	3012: The performance strings in the Performance registry value is corrupted when process Performance extension counter provider. The BaseIndex value from the Performance registry is the first DWORD in the Data section, LastCounter value is the second DWORD in the Data section, and LastHelp value is the third DWORD in the Data section.
Application	Error	None	2015-04-26 09:01:06	SYSTEM	Microsoft-Windows-LoadPerf	3011: Unloading the performance counter strings for service WmiApRpl (WmiApRpl) failed. The first DWORD in the Data section contains the error code.
Application	Error	None	2015-04-26 09:07:42		SideBySide	33: Activation context generation failed for "c:\program files (x86)\IObit\advanced systemcare 8\kb3000850.cab_temp\5666fc85-066a-466c-b765-feb1c72f64a4\amd64_microsoft-windows-narrator_31bf3856ad364e35_6.3.9600.17415_none_af28d3d777766b35\narrator.exe". Dependent Assembly SRH,type="win32",version="1.0.0.0" could not be found. Please use sxstrace.exe for detailed diagnosis.
						33: Activation context generation failed for "c:\program files (x86)\IObit\advanced systemcare

	Application	Error	None	2015-04-26 09:08:25		SideBySide	8\kb3000850.cab_temp\5666fc85-066a-466c-b765-feb1c72f64a4\wow64_microsoft-windows-narrator_31bf3856ad364e35_6.3.9600.17415_none_b97d7e29abd72d30\narrator.exe". Dependent Assembly SRH,type="win32",version="1.0.0.0" could not be found. Please use sxstrace.exe for detailed diagnosis.
	Application	Warning	None	2015-04-26 09:30:19		Software Protection Platform Service	8233: The rules engine reported a failed VL activation attempt. Reason:0x8007232B AppId = 0ff1ce15-a989-479d-af46-f275c6370663, SkuId = b322da9c-a2e2-4058-9e4e-f59a6970bd69 Trigger=NetworkAvailable
	Application	Warning	None	2015-04-26 09:30:23		Software Protection Platform Service	8233: The rules engine reported a failed VL activation attempt. Reason:0x8007232B AppId = 0ff1ce15-a989-479d-af46-f275c6370663, SkuId = b322da9c-a2e2-4058-9e4e-f59a6970bd69 Trigger=UserLogon(1)
	Application	Error	None	2015-04-26 09:34:15	SYSTEM	Microsoft-Windows-LoadPerf	3012: The performance strings in the Performance registry value is corrupted when process Performance extension counter provider. The BaseIndex value from the Performance registry is the first DWORD in the Data section, LastCounter value is the second DWORD in the Data section, and LastHelp value is the third DWORD in the Data section.
	Application	Error	None	2015-04-26 09:34:15	SYSTEM	Microsoft-Windows-LoadPerf	3011: Unloading the performance counter strings for service WmiApRpl (WmiApRpl) failed. The first DWORD in the Data section contains the error code.
	Application	Warning	None	2015-04-26 10:00:07		WlcIntfy	6004: The winlogon notification subscriber <TrustedInstaller> failed a critical notification event.
	Application	Warning	None	2015-04-26 10:00:16		Software Protection Platform Service	8233: The rules engine reported a failed VL activation attempt. Reason:0x8007232B AppId = 0ff1ce15-a989-479d-af46-f275c6370663, SkuId = b322da9c-a2e2-4058-9e4e-f59a6970bd69 Trigger=NetworkAvailable
	Application	Warning	None	2015-04-26 10:00:19		Software Protection Platform Service	8233: The rules engine reported a failed VL activation attempt. Reason:0x8007232B AppId = 0ff1ce15-a989-479d-af46-f275c6370663, SkuId = b322da9c-a2e2-4058-9e4e-f59a6970bd69 Trigger=UserLogon(1)
	Application	Error	None	2015-04-26 10:04:13	SYSTEM	Microsoft-Windows-LoadPerf	3012: The performance strings in the Performance registry value is corrupted when process Performance extension counter provider. The BaseIndex value from the Performance registry is the first DWORD in the Data section, LastCounter value is the second DWORD in the Data section, and LastHelp value is the third DWORD in the Data section.
	Application	Error	None	2015-04-26 10:04:13	SYSTEM	Microsoft-Windows-LoadPerf	3011: Unloading the performance counter strings for service WmiApRpl (WmiApRpl) failed. The first DWORD in the Data section contains the error code.
	Application	Warning	None	2015-04-26 12:25:57		Software Protection Platform Service	8233: The rules engine reported a failed VL activation attempt. Reason:0x8007232B AppId = 0ff1ce15-a989-479d-af46-f275c6370663, SkuId = b322da9c-a2e2-4058-9e4e-f59a6970bd69 Trigger=NetworkAvailable
	Application	Warning	None	2015-04-26 12:26:00		Software Protection Platform Service	8233: The rules engine reported a failed VL activation attempt. Reason:0x8007232B AppId = 0ff1ce15-a989-479d-af46-f275c6370663, SkuId = b322da9c-a2e2-4058-9e4e-f59a6970bd69 Trigger=NetworkAvailable
	Application	Warning	3	2015-04-26 12:27:04		Windows Search Service	3036: Crawl could not be completed on content source <winrt://{S-1-5-21-1888849264-3803429180-4108621888-1001}/>. Context: Application, SystemIndex Catalog Details: The parameter is incorrect. (HRESULT : 0x80070057) (0x80070057)
	Application	Warning	None	2015-04-26 12:56:21		Software Protection Platform Service	8233: The rules engine reported a failed VL activation attempt. Reason:0x8007232B AppId = 0ff1ce15-a989-479d-af46-f275c6370663, SkuId = b322da9c-a2e2-4058-9e4e-f59a6970bd69 Trigger=NetworkAvailable
	Application	Warning	None	2015-04-26 12:56:24		Software Protection Platform Service	8233: The rules engine reported a failed VL activation attempt. Reason:0x8007232B AppId = 0ff1ce15-a989-479d-af46-f275c6370663, SkuId = b322da9c-a2e2-4058-9e4e-f59a6970bd69 Trigger=UserLogon(1)
	Application	Warning	None	2015-04-26 12:56:26		Software Protection Platform Service	8233: The rules engine reported a failed VL activation attempt. Reason:0x8007232B AppId = 0ff1ce15-a989-479d-af46-f275c6370663, SkuId = b322da9c-a2e2-4058-9e4e-f59a6970bd69 Trigger=NetworkAvailable
	Application	Error	None	2015-04-26 13:00:27	SYSTEM	Microsoft-Windows-LoadPerf	3012: The performance strings in the Performance registry value is corrupted when process Performance extension counter provider. The BaseIndex value from the Performance registry is the first DWORD in the Data section, LastCounter value is the second DWORD in the Data section, and LastHelp value is the third DWORD in the Data section.
	Application	Error	None	2015-04-26 13:00:27	SYSTEM	Microsoft-Windows-LoadPerf	3011: Unloading the performance counter strings for service WmiApRpl (WmiApRpl) failed. The first DWORD in the Data section contains the error code.
	Application	Warning	None	2015-04-26 13:26:24		Software Protection Platform Service	8233: The rules engine reported a failed VL activation attempt. Reason:0x8007232B AppId = 0ff1ce15-a989-479d-af46-f275c6370663, SkuId = b322da9c-a2e2-4058-9e4e-f59a6970bd69 Trigger=UserLogon(1)
	Application	Warning	None	2015-04-26		Software Protection Platform Service	8233: The rules engine reported a failed VL activation attempt. Reason:0x8007232B AppId = 0ff1ce15-a989-479d-af46-f275c6370663, SkuId = b322da9c-a2e2-4058-9e4e-f59a6970bd69 Trigger=NetworkAvailable

			13:26:27			
	Application	Error	None	2015-04-26 13:30:29	SYSTEM	Microsoft-Windows-LoadPerf	3012: The performance strings in the Performance registry value is corrupted when process Performance extension counter provider. The BaseIndex value from the Performance registry is the first DWORD in the Data section, LastCounter value is the second DWORD in the Data section, and LastHelp value is the third DWORD in the Data section.
	Application	Error	None	2015-04-26 13:30:29	SYSTEM	Microsoft-Windows-LoadPerf	3011: Unloading the performance counter strings for service WmiApRpl (WmiApRpl) failed. The first DWORD in the Data section contains the error code.
	Application	Warning	None	2015-04-27 17:04:54		Software Protection Platform Service	8233: The rules engine reported a failed VL activation attempt. Reason:0x8007007B AppId = 0ff1ce15-a989-479d-af46-f275c6370663, SkuId = b322da9c-a2e2-4058-9e4e-f59a6970bd69 Trigger=NetworkAvailable
	Application	Warning	None	2015-04-27 17:04:55		Software Protection Platform Service	8233: The rules engine reported a failed VL activation attempt. Reason:0x8007007B AppId = 0ff1ce15-a989-479d-af46-f275c6370663, SkuId = b322da9c-a2e2-4058-9e4e-f59a6970bd69 Trigger=UserLogon(1)
	Application	Warning	None	2015-04-27 17:05:03		Software Protection Platform Service	8233: The rules engine reported a failed VL activation attempt. Reason:0x8007232B AppId = 0ff1ce15-a989-479d-af46-f275c6370663, SkuId = b322da9c-a2e2-4058-9e4e-f59a6970bd69 Trigger=NetworkAvailable
	Application	Error	3	2015-04-27 17:08:50		Windows Search Service	3079: Notifications for the volume C:\ are not active. Context: Windows Application Details: The parameter is incorrect. (HRESULT : 0x80070057) (0x80070057)
	Application	Error	None	2015-04-27 17:09:19	SYSTEM	Microsoft-Windows-LoadPerf	3012: The performance strings in the Performance registry value is corrupted when process Performance extension counter provider. The BaseIndex value from the Performance registry is the first DWORD in the Data section, LastCounter value is the second DWORD in the Data section, and LastHelp value is the third DWORD in the Data section.
	Application	Error	None	2015-04-27 17:09:19	SYSTEM	Microsoft-Windows-LoadPerf	3011: Unloading the performance counter strings for service WmiApRpl (WmiApRpl) failed. The first DWORD in the Data section contains the error code.
	Application	Warning	None	2015-04-27 17:35:17		Software Protection Platform Service	8233: The rules engine reported a failed VL activation attempt. Reason:0x8007232B AppId = 0ff1ce15-a989-479d-af46-f275c6370663, SkuId = b322da9c-a2e2-4058-9e4e-f59a6970bd69 Trigger=UserLogon(1)
	Application	Warning	None	2015-04-27 17:35:20		Software Protection Platform Service	8233: The rules engine reported a failed VL activation attempt. Reason:0x8007232B AppId = 0ff1ce15-a989-479d-af46-f275c6370663, SkuId = b322da9c-a2e2-4058-9e4e-f59a6970bd69 Trigger=NetworkAvailable
	Application	Error	None	2015-04-27 17:39:27	SYSTEM	Microsoft-Windows-LoadPerf	3012: The performance strings in the Performance registry value is corrupted when process Performance extension counter provider. The BaseIndex value from the Performance registry is the first DWORD in the Data section, LastCounter value is the second DWORD in the Data section, and LastHelp value is the third DWORD in the Data section.
	Application	Error	None	2015-04-27 17:39:27	SYSTEM	Microsoft-Windows-LoadPerf	3011: Unloading the performance counter strings for service WmiApRpl (WmiApRpl) failed. The first DWORD in the Data section contains the error code.
	Application	Error	None	2015-04-27 18:03:05		SideBySide	33: Activation context generation failed for "c:\program files (x86)\IObit\advanced systemcare 8\kb3000850.cab_temp\5666fc85-066a-466c-b765-feb1c72f64a4\amd64_microsoft-windows-narrator_31bf3856ad364e35_6.3.9600.17415_none_af28d3d777766b35\narrator.exe". Dependent Assembly SRH,type="win32",version="1.0.0.0" could not be found. Please use sxstrace.exe for detailed diagnosis.
	Application	Error	None	2015-04-27 18:03:48		SideBySide	33: Activation context generation failed for "c:\program files (x86)\IObit\advanced systemcare 8\kb3000850.cab_temp\5666fc85-066a-466c-b765-feb1c72f64a4\wow64_microsoft-windows-narrator_31bf3856ad364e35_6.3.9600.17415_none_b97d7e29abd72d30\narrator.exe". Dependent Assembly SRH,type="win32",version="1.0.0.0" could not be found. Please use sxstrace.exe for detailed diagnosis.
	Application	Warning	None	2015-04-27 18:32:33		Software Protection Platform Service	8233: The rules engine reported a failed VL activation attempt. Reason:0x8007232B AppId = 0ff1ce15-a989-479d-af46-f275c6370663, SkuId = b322da9c-a2e2-4058-9e4e-f59a6970bd69 Trigger=NetworkAvailable
	Application	Warning	None	2015-04-27 18:32:36		Software Protection Platform Service	8233: The rules engine reported a failed VL activation attempt. Reason:0x8007232B AppId = 0ff1ce15-a989-479d-af46-f275c6370663, SkuId = b322da9c-a2e2-4058-9e4e-f59a6970bd69 Trigger=UserLogon(1)
	Application	Warning	None	2015-04-27 18:32:38		Software Protection Platform Service	8233: The rules engine reported a failed VL activation attempt. Reason:0x8007232B AppId = 0ff1ce15-a989-479d-af46-f275c6370663, SkuId = b322da9c-a2e2-4058-9e4e-f59a6970bd69 Trigger=NetworkAvailable
	Application	Error	None	2015-04-27 18:36:53	SYSTEM	Microsoft-Windows-LoadPerf	3012: The performance strings in the Performance registry value is corrupted when process Performance extension counter provider. The BaseIndex value from the Performance registry is the first DWORD in the Data section, LastCounter value is the second DWORD in the Data section, and LastHelp value is the third DWORD in the Data section.
	Application	Error	None	2015-04-27	SYSTEM	Microsoft-Windows-LoadPerf	3011: Unloading the performance counter strings for service WmiApRpl (WmiApRpl) failed. The first DWORD in

			18:36:53			the Data section contains the error code.
	Application	Warning	None	2015-04-28 18:36:46		Software Protection Platform Service	8233: The rules engine reported a failed VL activation attempt. Reason:0x8007232B AppId = 0ff1ce15-a989-479d-af46-f275c6370663, SkuId = b322da9c-a2e2-4058-9e4e-f59a6970bd69 Trigger=UserLogon(1)
	Application	Warning	None	2015-04-28 18:36:48		Software Protection Platform Service	8233: The rules engine reported a failed VL activation attempt. Reason:0x8007232B AppId = 0ff1ce15-a989-479d-af46-f275c6370663, SkuId = b322da9c-a2e2-4058-9e4e-f59a6970bd69 Trigger=NetworkAvailable
	Application	Error	3	2015-04-28 18:40:23		Windows Search Service	3079: Notifications for the volume C:\ are not active. Context: Windows Application Details: The parameter is incorrect. (HRESULT : 0x80070057) (0x80070057)
	Application	Error	None	2015-04-28 18:40:43	SYSTEM	Microsoft-Windows-LoadPerf	3012: The performance strings in the Performance registry value is corrupted when process Performance extension counter provider. The BaseIndex value from the Performance registry is the first DWORD in the Data section, LastCounter value is the second DWORD in the Data section, and LastHelp value is the third DWORD in the Data section.
	Application	Error	None	2015-04-28 18:40:43	SYSTEM	Microsoft-Windows-LoadPerf	3011: Unloading the performance counter strings for service WmiApRpl (WmiApRpl) failed. The first DWORD in the Data section contains the error code.
	Application	Warning	None	2015-04-28 19:06:50		Software Protection Platform Service	8233: The rules engine reported a failed VL activation attempt. Reason:0x8007232B AppId = 0ff1ce15-a989-479d-af46-f275c6370663, SkuId = b322da9c-a2e2-4058-9e4e-f59a6970bd69 Trigger=NetworkAvailable
	Application	Error	None	2015-04-28 19:10:44	SYSTEM	Microsoft-Windows-LoadPerf	3012: The performance strings in the Performance registry value is corrupted when process Performance extension counter provider. The BaseIndex value from the Performance registry is the first DWORD in the Data section, LastCounter value is the second DWORD in the Data section, and LastHelp value is the third DWORD in the Data section.
	Application	Error	None	2015-04-28 19:10:44	SYSTEM	Microsoft-Windows-LoadPerf	3011: Unloading the performance counter strings for service WmiApRpl (WmiApRpl) failed. The first DWORD in the Data section contains the error code.
	Application	Warning	None	2015-04-28 19:37:58		Software Protection Platform Service	8233: The rules engine reported a failed VL activation attempt. Reason:0x8007232B AppId = 0ff1ce15-a989-479d-af46-f275c6370663, SkuId = b322da9c-a2e2-4058-9e4e-f59a6970bd69 Trigger=NetworkAvailable
	Application	Warning	None	2015-04-28 19:38:03		Software Protection Platform Service	8233: The rules engine reported a failed VL activation attempt. Reason:0x8007232B AppId = 0ff1ce15-a989-479d-af46-f275c6370663, SkuId = b322da9c-a2e2-4058-9e4e-f59a6970bd69 Trigger=UserLogon(1)
	Application	Warning	None	2015-04-28 19:38:05		Software Protection Platform Service	8233: The rules engine reported a failed VL activation attempt. Reason:0x8007232B AppId = 0ff1ce15-a989-479d-af46-f275c6370663, SkuId = b322da9c-a2e2-4058-9e4e-f59a6970bd69 Trigger=NetworkAvailable
	Application	Error	None	2015-04-28 19:41:56	SYSTEM	Microsoft-Windows-LoadPerf	3012: The performance strings in the Performance registry value is corrupted when process Performance extension counter provider. The BaseIndex value from the Performance registry is the first DWORD in the Data section, LastCounter value is the second DWORD in the Data section, and LastHelp value is the third DWORD in the Data section.
	Application	Error	None	2015-04-28 19:41:56	SYSTEM	Microsoft-Windows-LoadPerf	3011: Unloading the performance counter strings for service WmiApRpl (WmiApRpl) failed. The first DWORD in the Data section contains the error code.
	Application	Warning	None	2015-04-28 20:15:34		Software Protection Platform Service	8233: The rules engine reported a failed VL activation attempt. Reason:0x8007232B AppId = 0ff1ce15-a989-479d-af46-f275c6370663, SkuId = b322da9c-a2e2-4058-9e4e-f59a6970bd69 Trigger=UserLogon(1)
	Application	Warning	None	2015-04-28 20:15:36		Software Protection Platform Service	8233: The rules engine reported a failed VL activation attempt. Reason:0x8007232B AppId = 0ff1ce15-a989-479d-af46-f275c6370663, SkuId = b322da9c-a2e2-4058-9e4e-f59a6970bd69 Trigger=NetworkAvailable
	Application	Error	None	2015-04-28 20:19:34	SYSTEM	Microsoft-Windows-LoadPerf	3012: The performance strings in the Performance registry value is corrupted when process Performance extension counter provider. The BaseIndex value from the Performance registry is the first DWORD in the Data section, LastCounter value is the second DWORD in the Data section, and LastHelp value is the third DWORD in the Data section.
	Application	Error	None	2015-04-28 20:19:34	SYSTEM	Microsoft-Windows-LoadPerf	3011: Unloading the performance counter strings for service WmiApRpl (WmiApRpl) failed. The first DWORD in the Data section contains the error code.
	Application	Warning	None	2015-04-28 20:20:35		Software Protection Platform Service	8233: The rules engine reported a failed VL activation attempt. Reason:0x8007232B AppId = 0ff1ce15-a989-479d-af46-f275c6370663, SkuId = b322da9c-a2e2-4058-9e4e-f59a6970bd69 Trigger=NetworkQuarantineRetry
	Application	Warning	None	2015-04-28 20:42:51		Software Protection Platform Service	8233: The rules engine reported a failed VL activation attempt. Reason:0x8007232B AppId = 0ff1ce15-a989-479d-af46-f275c6370663, SkuId = b322da9c-a2e2-4058-9e4e-f59a6970bd69 Trigger=NetworkAvailable

	Application	Warning	None	2015-04-28 20:43:02		Software Protection Platform Service	8233: The rules engine reported a failed VL activation attempt. Reason:0x8007232B AppId = 0ff1ce15-a989-479d-af46-f275c6370663, SkuId = b322da9c-a2e2-4058-9e4e-f59a6970bd69 Trigger=UserLogon(1)
	Application	Error	None	2015-04-28 20:46:46	SYSTEM	Microsoft-Windows-LoadPerf	3012: The performance strings in the Performance registry value is corrupted when process Performance extension counter provider. The BaseIndex value from the Performance registry is the first DWORD in the Data section, LastCounter value is the second DWORD in the Data section, and LastHelp value is the third DWORD in the Data section.
	Application	Error	None	2015-04-28 20:46:46	SYSTEM	Microsoft-Windows-LoadPerf	3011: Unloading the performance counter strings for service WmiApRpl (WmiApRpl) failed. The first DWORD in the Data section contains the error code.
	Application	Warning	None	2015-04-29 11:34:32		Software Protection Platform Service	8233: The rules engine reported a failed VL activation attempt. Reason:0x8007232B AppId = 0ff1ce15-a989-479d-af46-f275c6370663, SkuId = b322da9c-a2e2-4058-9e4e-f59a6970bd69 Trigger=UserLogon(1)
	Application	Warning	None	2015-04-29 11:34:34		Software Protection Platform Service	8233: The rules engine reported a failed VL activation attempt. Reason:0x8007232B AppId = 0ff1ce15-a989-479d-af46-f275c6370663, SkuId = b322da9c-a2e2-4058-9e4e-f59a6970bd69 Trigger=NetworkAvailable
	Application	Error	3	2015-04-29 11:38:20		Windows Search Service	3079: Notifications for the volume C:\ are not active. Context: Windows Application Details: The parameter is incorrect. (HRESULT : 0x80070057) (0x80070057)
	Application	Error	None	2015-04-29 11:38:34	SYSTEM	Microsoft-Windows-LoadPerf	3012: The performance strings in the Performance registry value is corrupted when process Performance extension counter provider. The BaseIndex value from the Performance registry is the first DWORD in the Data section, LastCounter value is the second DWORD in the Data section, and LastHelp value is the third DWORD in the Data section.
	Application	Error	None	2015-04-29 11:38:34	SYSTEM	Microsoft-Windows-LoadPerf	3011: Unloading the performance counter strings for service WmiApRpl (WmiApRpl) failed. The first DWORD in the Data section contains the error code.
	Security	Audit Success	12288	2015-04-22 16:22:26		Microsoft-Windows-Security-Auditing	4608: Windows is starting up. This event is logged when LSASS.EXE starts and the auditing subsystem is initialized.
	Security	Audit Success	12544	2015-04-22 16:22:26		Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-0-0 Account Name: - Account Domain: - Logon ID: 0x0 Logon Type: 0 Impersonation Level: - New Logon: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Logon ID: 0x3e7 Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x4 Process Name: Network Information: Workstation Name: - Source Network Address: - Source Port: - Detailed Authentication Information: Logon Process: - Authentication Package: - Transited Services: - Package Name (NTLM only): - Key Length: 0 This event is generated when a logon session is created. It is generated on the computer that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service such as the Server service, or a local process such as Winlogon.exe or Services.exe. The logon type field indicates the kind of logon that occurred. The most common types are 2 (interactive) and 3 (network). The New Logon fields indicate the account for whom the new logon was created, i.e. the account that was logged on. The network fields indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impersonation level field indicates the extent to which a process in the logon session can impersonate. The authentication information fields provide detailed information about this specific logon request. - Logon GUID is a unique identifier that can be used to correlate this event with a KDC event. - Transited services indicate which intermediate services have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indicates the length of the generated session key. This will be 0 if no session key was requested.
	Security	Audit Success	12544	2015-04-22 16:22:26		Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: LTRANPHD$ Account Domain: WORKGROUP Logon ID: 0x3e7 Logon Type: 5 Impersonation Level: %%1833 New Logon: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Logon ID: 0x3e7 Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x234 Process Name: C:\Windows\System32\services.exe Network Information: Workstation Name: Source Network Address: - Source Port: - Detailed Authentication Information: Logon Process: Advapi Authentication Package: Negotiate Transited Services: - Package Name (NTLM only): - Key Length: 0 This event is generated when a logon session is created. It is generated on the computer that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service such as the Server service, or a local process such as Winlogon.exe or Services.exe. The logon type field indicates the kind of logon that occurred. The most common types are 2 (interactive) and 3 (network). The New Logon fields indicate the account for whom the new logon was created, i.e. the account that was logged on. The network fields indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impersonation level field indicates the extent to which a process in the logon session can impersonate. The authentication information fields provide detailed information about this specific logon request. - Logon GUID is a unique identifier that can be used to correlate this event with a KDC event. - Transited services indicate which intermediate services have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indicates the length of the generated

					session key. This will be 0 if no session key was requested.
Security	Audit Success	12544	2015-04-22 16:22:26	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: LTRANPHD$ Account Domain: WORKGROUP Logon ID: 0x3e7 Logon Type: 5 Impersonation Level: %%1833 New Logon: Security ID: S-1-5-20 Account Name: NETWORK SERVICE Account Domain: NT AUTHORITY Logon ID: 0x3e4 Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x234 Process Name: C:\Windows\System32\services.exe Network Information: Workstation Name: Source Network Address: - Source Port: - Detailed Authentication Information: Logon Process: Advapi Authentication Package: Negotiate Transited Services: - Package Name (NTLM only): - Key Length: 0 This event is generated when a logon session is created. It is generated on the computer that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service such as the Server service, or a local process such as Winlogon.exe or Services.exe. The logon type field indicates the kind of logon that occurred. The most common types are 2 (interactive) and 3 (network). The New Logon fields indicate the account for whom the new logon was created, i.e. the account that was logged on. The network fields indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impersonation level field indicates the extent to which a process in the logon session can impersonate. The authentication information fields provide detailed information about this specific logon request. - Logon GUID is a unique identifier that can be used to correlate this event with a KDC event. - Transited services indicate which intermediate services have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indicates the length of the generated session key. This will be 0 if no session key was requested.
Security	Audit Success	12544	2015-04-22 16:22:26	Microsoft-Windows-Security-Auditing	4648: A logon was attempted using explicit credentials. Subject: Security ID: S-1-5-18 Account Name: LTRANPHD$ Account Domain: WORKGROUP Logon ID: 0x3e7 Logon GUID: {00000000-0000-0000-0000-000000000000} Account Whose Credentials Were Used: Account Name: DWM-1 Account Domain: Window Manager Logon GUID: {00000000-0000-0000-0000-000000000000} Target Server: Target Server Name: localhost Additional Information: localhost Process Information: Process ID: 0x20c Process Name: C:\Windows\System32\winlogon.exe Network Information: Network Address: - Port: - This event is generated when a process attempts to log on an account by explicitly specifying that account's credentials. This most commonly occurs in batch-type configurations such as scheduled tasks, or when using the RUNAS command.
Security	Audit Success	12544	2015-04-22 16:22:26	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: LTRANPHD$ Account Domain: WORKGROUP Logon ID: 0x3e7 Logon Type: 2 Impersonation Level: %%1833 New Logon: Security ID: S-1-5-90-1 Account Name: DWM-1 Account Domain: Window Manager Logon ID: 0xe79f Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x20c Process Name: C:\Windows\System32\winlogon.exe Network Information: Workstation Name: Source Network Address: - Source Port: - Detailed Authentication Information: Logon Process: Advapi Authentication Package: Negotiate Transited Services: - Package Name (NTLM only): - Key Length: 0 This event is generated when a logon session is created. It is generated on the computer that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service such as the Server service, or a local process such as Winlogon.exe or Services.exe. The logon type field indicates the kind of logon that occurred. The most common types are 2 (interactive) and 3 (network). The New Logon fields indicate the account for whom the new logon was created, i.e. the account that was logged on. The network fields indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impersonation level field indicates the extent to which a process in the logon session can impersonate. The authentication information fields provide detailed information about this specific logon request. - Logon GUID is a unique identifier that can be used to correlate this event with a KDC event. - Transited services indicate which intermediate services have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indicates the length of the generated session key. This will be 0 if no session key was requested.
Security	Audit Success	12544	2015-04-22 16:22:26	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: LTRANPHD$ Account Domain: WORKGROUP Logon ID: 0x3e7 Logon Type: 2 Impersonation Level: %%1833 New Logon: Security ID: S-1-5-90-1 Account Name: DWM-1 Account Domain: Window Manager Logon ID: 0xe7bd Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x20c Process Name: C:\Windows\System32\winlogon.exe Network Information: Workstation Name: Source Network Address: - Source Port: - Detailed Authentication Information: Logon Process: Advapi Authentication Package: Negotiate Transited Services: - Package Name (NTLM only): - Key Length: 0 This event is generated when a logon session is created. It is generated on the computer that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service such as the Server service, or a local process such as Winlogon.exe or Services.exe. The logon type field indicates the kind of logon that occurred. The most common types are 2 (interactive) and 3 (network). The New Logon fields indicate the account for whom the new logon was created, i.e. the account that was logged on. The network fields indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impersonation level field indicates the extent to which a process in the logon session can impersonate. The authentication information fields provide detailed information about this specific logon request. - Logon GUID is a unique identifier that can be used to correlate this event with a KDC event. - Transited services indicate which intermediate services have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indicates the length of the generated session key. This will be 0 if no session key was requested.

Security	Audit Success	12544	2015-04-22 16:22:26	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: LTRANPHD$ Account Domain: WORKGROUP Logon ID: 0x3e7 Logon Type: 5 Impersonation Level: %%1833 New Logon: Security ID: S-1-5-19 Account Name: LOCAL SERVICE Account Domain: NT AUTHORITY Logon ID: 0x3e5 Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x234 Process Name: C:\Windows\System32\services.exe Network Information: Workstation Name: Source Network Address: - Source Port: - Detailed Authentication Information: Logon Process: Advapi Authentication Package: Negotiate Transited Services: - Package Name (NTLM only): - Key Length: 0 This event is generated when a logon session is created. It is generated on the computer that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service such as the Server service, or a local process such as Winlogon.exe or Services.exe. The logon type field indicates the kind of logon that occurred. The most common types are 2 (interactive) and 3 (network). The New Logon fields indicate the account for whom the new logon was created, i.e. the account that was logged on. The network fields indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impersonation level field indicates the extent to which a process in the logon session can impersonate. The authentication information fields provide detailed information about this specific logon request. - Logon GUID is a unique identifier that can be used to correlate this event with a KDC event. - Transited services indicate which intermediate services have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indicates the length of the generated session key. This will be 0 if no session key was requested.
Security	Audit Success	12544	2015-04-22 16:22:26	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: LTRANPHD$ Account Domain: WORKGROUP Logon ID: 0x3e7 Logon Type: 5 Impersonation Level: %%1833 New Logon: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Logon ID: 0x3e7 Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x234 Process Name: C:\Windows\System32\services.exe Network Information: Workstation Name: Source Network Address: - Source Port: - Detailed Authentication Information: Logon Process: Advapi Authentication Package: Negotiate Transited Services: - Package Name (NTLM only): - Key Length: 0 This event is generated when a logon session is created. It is generated on the computer that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service such as the Server service, or a local process such as Winlogon.exe or Services.exe. The logon type field indicates the kind of logon that occurred. The most common types are 2 (interactive) and 3 (network). The New Logon fields indicate the account for whom the new logon was created, i.e. the account that was logged on. The network fields indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impersonation level field indicates the extent to which a process in the logon session can impersonate. The authentication information fields provide detailed information about this specific logon request. - Logon GUID is a unique identifier that can be used to correlate this event with a KDC event. - Transited services indicate which intermediate services have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indicates the length of the generated session key. This will be 0 if no session key was requested.
Security	Audit Success	12548	2015-04-22 16:22:26	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Logon ID: 0x3e7 Privileges: SeAssignPrimaryTokenPrivilege SeTcbPrivilege SeSecurityPrivilege SeTakeOwnershipPrivilege SeLoadDriverPrivilege SeBackupPrivilege SeRestorePrivilege SeDebugPrivilege SeAuditPrivilege SeSystemEnvironmentPrivilege SeImpersonatePrivilege
Security	Audit Success	12548	2015-04-22 16:22:26	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-20 Account Name: NETWORK SERVICE Account Domain: NT AUTHORITY Logon ID: 0x3e4 Privileges: SeAssignPrimaryTokenPrivilege SeAuditPrivilege SeImpersonatePrivilege
Security	Audit Success	12548	2015-04-22 16:22:26	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-90-1 Account Name: DWM-1 Account Domain: Window Manager Logon ID: 0xe79f Privileges: SeAssignPrimaryTokenPrivilege SeAuditPrivilege SeImpersonatePrivilege
Security	Audit Success	12548	2015-04-22 16:22:26	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-90-1 Account Name: DWM-1 Account Domain: Window Manager Logon ID: 0xe7bd Privileges: SeAssignPrimaryTokenPrivilege SeAuditPrivilege
Security	Audit Success	12548	2015-04-22 16:22:26	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-19 Account Name: LOCAL SERVICE Account Domain: NT AUTHORITY Logon ID: 0x3e5 Privileges: SeAssignPrimaryTokenPrivilege SeAuditPrivilege SeImpersonatePrivilege
Security	Audit Success	12548	2015-04-22 16:22:26	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Logon ID: 0x3e7 Privileges: SeAssignPrimaryTokenPrivilege SeTcbPrivilege SeSecurityPrivilege SeTakeOwnershipPrivilege SeLoadDriverPrivilege SeBackupPrivilege SeRestorePrivilege SeDebugPrivilege SeAuditPrivilege SeSystemEnvironmentPrivilege SeImpersonatePrivilege
Security	Audit Success	13568	2015-04-22 16:22:26	Microsoft-Windows-Security-Auditing	4902: The Per-user audit policy table was created. Number of Elements: 0 Policy ID: 0x900e
Security	Audit Success	12292	2015-04-22 16:22:27	Microsoft-Windows-Security-Auditing	5033: The Windows Firewall Driver started successfully.
					4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: LTRANPHD$

Security	Audit Success	12544	2015-04-22 16:22:27	Microsoft-Windows-Security-Auditing	Account Domain: WORKGROUP Logon ID: 0x3e7 Logon Type: 5 Impersonation Level: %%1833 New Logon: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Logon ID: 0x3e7 Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x234 Process Name: C:\Windows\System32\services.exe Network Information: Workstation Name: Source Network Address: - Source Port: - Detailed Authentication Information: Logon Process: Advapi Authentication Package: Negotiate Transited Services: - Package Name (NTLM only): - Key Length: 0 This event is generated when a logon session is created. It is generated on the computer that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service such as the Server service, or a local process such as Winlogon.exe or Services.exe. The logon type field indicates the kind of logon that occurred. The most common types are 2 (interactive) and 3 (network). The New Logon fields indicate the account for whom the new logon was created, i.e. the account that was logged on. The network fields indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impersonation level field indicates the extent to which a process in the logon session can impersonate. The authentication information fields provide detailed information about this specific logon request. - Logon GUID is a unique identifier that can be used to correlate this event with a KDC event. - Transited services indicate which intermediate services have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indicates the length of the generated session key. This will be 0 if no session key was requested.
Security	Audit Success	12544	2015-04-22 16:22:27	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: LTRANPHD$ Account Domain: WORKGROUP Logon ID: 0x3e7 Logon Type: 5 Impersonation Level: %%1833 New Logon: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Logon ID: 0x3e7 Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x234 Process Name: C:\Windows\System32\services.exe Network Information: Workstation Name: Source Network Address: - Source Port: - Detailed Authentication Information: Logon Process: Advapi Authentication Package: Negotiate Transited Services: - Package Name (NTLM only): - Key Length: 0 This event is generated when a logon session is created. It is generated on the computer that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service such as the Server service, or a local process such as Winlogon.exe or Services.exe. The logon type field indicates the kind of logon that occurred. The most common types are 2 (interactive) and 3 (network). The New Logon fields indicate the account for whom the new logon was created, i.e. the account that was logged on. The network fields indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impersonation level field indicates the extent to which a process in the logon session can impersonate. The authentication information fields provide detailed information about this specific logon request. - Logon GUID is a unique identifier that can be used to correlate this event with a KDC event. - Transited services indicate which intermediate services have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indicates the length of the generated session key. This will be 0 if no session key was requested.
Security	Audit Success	12548	2015-04-22 16:22:27	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Logon ID: 0x3e7 Privileges: SeAssignPrimaryTokenPrivilege SeTcbPrivilege SeSecurityPrivilege SeTakeOwnershipPrivilege SeLoadDriverPrivilege SeBackupPrivilege SeRestorePrivilege SeDebugPrivilege SeAuditPrivilege SeSystemEnvironmentPrivilege SeImpersonatePrivilege
Security	Audit Success	12548	2015-04-22 16:22:27	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Logon ID: 0x3e7 Privileges: SeAssignPrimaryTokenPrivilege SeTcbPrivilege SeSecurityPrivilege SeTakeOwnershipPrivilege SeLoadDriverPrivilege SeBackupPrivilege SeRestorePrivilege SeDebugPrivilege SeAuditPrivilege SeSystemEnvironmentPrivilege SeImpersonatePrivilege
Security	Audit Success	12292	2015-04-22 16:22:28	Microsoft-Windows-Security-Auditing	5024: The Windows Firewall service started successfully.
Security	Audit Success	12544	2015-04-22 16:22:28	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: LTRANPHD$ Account Domain: WORKGROUP Logon ID: 0x3e7 Logon Type: 5 Impersonation Level: %%1833 New Logon: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Logon ID: 0x3e7 Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x234 Process Name: C:\Windows\System32\services.exe Network Information: Workstation Name: Source Network Address: - Source Port: - Detailed Authentication Information: Logon Process: Advapi Authentication Package: Negotiate Transited Services: - Package Name (NTLM only): - Key Length: 0 This event is generated when a logon session is created. It is generated on the computer that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service such as the Server service, or a local process such as Winlogon.exe or Services.exe. The logon type field indicates the kind of logon that occurred. The most common types are 2 (interactive) and 3 (network). The New Logon fields indicate the account for whom the new logon was created, i.e. the account that was logged on. The network fields indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impersonation level field indicates the extent to which a process in the logon session can impersonate. The authentication information fields provide detailed information about this specific logon request. - Logon GUID is a unique identifier that can be used to correlate this event with a KDC event. - Transited services indicate which intermediate services have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indicates the length of the generated

					session key. This will be 0 if no session key was requested.
Security	Audit Success	12544	2015-04-22 16:22:28	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-0-0 Account Name: - Account Domain: - Logon ID: 0x0 Logon Type: 3 Impersonation Level: %%1833 New Logon: Security ID: S-1-5-7 Account Name: ANONYMOUS LOGON Account Domain: NT AUTHORITY Logon ID: 0x172dd Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x0 Process Name: - Network Information: Workstation Name: Source Network Address: - Source Port: - Detailed Authentication Information: Logon Process: NtLmSsp Authentication Package: NTLM Transited Services: - Package Name (NTLM only): NTLM V1 Key Length: 0 This event is generated when a logon session is created. It is generated on the computer that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service such as the Server service, or a local process such as Winlogon.exe or Services.exe. The logon type field indicates the kind of logon that occurred. The most common types are 2 (interactive) and 3 (network). The New Logon fields indicate the account for whom the new logon was created, i.e. the account that was logged on. The network fields indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impersonation level field indicates the extent to which a process in the logon session can impersonate. The authentication information fields provide detailed information about this specific logon request. - Logon GUID is a unique identifier that can be used to correlate this event with a KDC event. - Transited services indicate which intermediate services have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indicates the length of the generated session key. This will be 0 if no session key was requested.
Security	Audit Success	12548	2015-04-22 16:22:28	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Logon ID: 0x3e7 Privileges: SeAssignPrimaryTokenPrivilege SeTcbPrivilege SeSecurityPrivilege SeTakeOwnershipPrivilege SeLoadDriverPrivilege SeBackupPrivilege SeRestorePrivilege SeDebugPrivilege SeAuditPrivilege SeSystemEnvironmentPrivilege SeImpersonatePrivilege
Security	Audit Success	12544	2015-04-22 16:22:57	Microsoft-Windows-Security-Auditing	4648: A logon was attempted using explicit credentials. Subject: Security ID: S-1-5-18 Account Name: LTRANPHD$ Account Domain: WORKGROUP Logon ID: 0x3e7 Logon GUID: {00000000-0000-0000-0000-000000000000} Account Whose Credentials Were Used: Account Name: Liem Account Domain: LTRANPHD Logon GUID: {00000000-0000-0000-0000-000000000000} Target Server: Target Server Name: localhost Additional Information: localhost Process Information: Process ID: 0x20c Process Name: C:\Windows\System32\winlogon.exe Network Information: Network Address: 127.0.0.1 Port: 0 This event is generated when a process attempts to log on an account by explicitly specifying that account's credentials. This most commonly occurs in batch-type configurations such as scheduled tasks, or when using the RUNAS command.
Security	Audit Success	12544	2015-04-22 16:22:57	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: LTRANPHD$ Account Domain: WORKGROUP Logon ID: 0x3e7 Logon Type: 2 Impersonation Level: %%1833 New Logon: Security ID: S-1-5-21-1888849264-3803429180-4108621888-1001 Account Name: Liem Account Domain: LTRANPHD Logon ID: 0x20503 Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x20c Process Name: C:\Windows\System32\winlogon.exe Network Information: Workstation Name: LTRANPHD Source Network Address: 127.0.0.1 Source Port: 0 Detailed Authentication Information: Logon Process: User32 Authentication Package: Negotiate Transited Services: - Package Name (NTLM only): - Key Length: 0 This event is generated when a logon session is created. It is generated on the computer that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service such as the Server service, or a local process such as Winlogon.exe or Services.exe. The logon type field indicates the kind of logon that occurred. The most common types are 2 (interactive) and 3 (network). The New Logon fields indicate the account for whom the new logon was created, i.e. the account that was logged on. The network fields indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impersonation level field indicates the extent to which a process in the logon session can impersonate. The authentication information fields provide detailed information about this specific logon request. - Logon GUID is a unique identifier that can be used to correlate this event with a KDC event. - Transited services indicate which intermediate services have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indicates the length of the generated session key. This will be 0 if no session key was requested.
Security	Audit Success	12544	2015-04-22 16:22:57	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: LTRANPHD$ Account Domain: WORKGROUP Logon ID: 0x3e7 Logon Type: 2 Impersonation Level: %%1833 New Logon: Security ID: S-1-5-21-1888849264-3803429180-4108621888-1001 Account Name: Liem Account Domain: LTRANPHD Logon ID: 0x20558 Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x20c Process Name: C:\Windows\System32\winlogon.exe Network Information: Workstation Name: LTRANPHD Source Network Address: 127.0.0.1 Source Port: 0 Detailed Authentication Information: Logon Process: User32 Authentication Package: Negotiate Transited Services: - Package Name (NTLM only): - Key Length: 0 This event is generated when a logon session is created. It is generated on the computer that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service such as the Server service, or a local process such as Winlogon.exe or Services.exe. The logon type field indicates the kind of logon that occurred. The most common types are 2 (interactive) and 3 (network). The New Logon fields indicate the account for whom the new logon was created, i.e. the account that was logged on. The network fields indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impersonation level field indicates the extent to which a process in the logon session can impersonate. The authentication information fields provide detailed

					information about this specific logon request. - Logon GUID is a unique identifier that can be used to correlate this event with a KDC event. - Transited services indicate which intermediate services have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indicates the length of the generated session key. This will be 0 if no session key was requested.
Security	Audit Success	12548	2015-04-22 16:22:57	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-21-1888849264-3803429180-4108621888-1001 Account Name: Liem Account Domain: LTRANPHD Logon ID: 0x20503 Privileges: SeSecurityPrivilege SeTakeOwnershipPrivilege SeLoadDriverPrivilege SeBackupPrivilege SeRestorePrivilege SeDebugPrivilege SeSystemEnvironmentPrivilege SeImpersonatePrivilege
Security	Audit Success	12544	2015-04-22 16:22:58	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: LTRANPHD$ Account Domain: WORKGROUP Logon ID: 0x3e7 Logon Type: 5 Impersonation Level: %%1833 New Logon: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Logon ID: 0x3e7 Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x234 Process Name: C:\Windows\System32\services.exe Network Information: Workstation Name: Source Network Address: - Source Port: - Detailed Authentication Information: Logon Process: Advapi Authentication Package: Negotiate Transited Services: - Package Name (NTLM only): - Key Length: 0 This event is generated when a logon session is created. It is generated on the computer that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service such as the Server service, or a local process such as Winlogon.exe or Services.exe. The logon type field indicates the kind of logon that occurred. The most common types are 2 (interactive) and 3 (network). The New Logon fields indicate the account for whom the new logon was created, i.e. the account that was logged on. The network fields indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impersonation level field indicates the extent to which a process in the logon session can impersonate. The authentication information fields provide detailed information about this specific logon request. - Logon GUID is a unique identifier that can be used to correlate this event with a KDC event. - Transited services indicate which intermediate services have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indicates the length of the generated session key. This will be 0 if no session key was requested.
Security	Audit Success	12548	2015-04-22 16:22:58	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Logon ID: 0x3e7 Privileges: SeAssignPrimaryTokenPrivilege SeTcbPrivilege SeSecurityPrivilege SeTakeOwnershipPrivilege SeLoadDriverPrivilege SeBackupPrivilege SeRestorePrivilege SeDebugPrivilege SeAuditPrivilege SeSystemEnvironmentPrivilege SeImpersonatePrivilege
Security	Audit Success	13824	2015-04-22 16:23:01	Microsoft-Windows-Security-Auditing	4797: An attempt was made to query the existence of a blank password for an account. Subject: Security ID: S-1-5-21-1888849264-3803429180-4108621888-1001 Account Name: Liem Account Domain: LTRANPHD Logon ID: 0x20558 Additional Information: Caller Workstation: LTRANPHD Target Account Name: Administrator Target Account Domain: LTRANPHD
Security	Audit Success	13824	2015-04-22 16:23:01	Microsoft-Windows-Security-Auditing	4797: An attempt was made to query the existence of a blank password for an account. Subject: Security ID: S-1-5-21-1888849264-3803429180-4108621888-1001 Account Name: Liem Account Domain: LTRANPHD Logon ID: 0x20558 Additional Information: Caller Workstation: LTRANPHD Target Account Name: Guest Target Account Domain: LTRANPHD
Security	Audit Success	13824	2015-04-22 16:23:01	Microsoft-Windows-Security-Auditing	4797: An attempt was made to query the existence of a blank password for an account. Subject: Security ID: S-1-5-21-1888849264-3803429180-4108621888-1001 Account Name: Liem Account Domain: LTRANPHD Logon ID: 0x20558 Additional Information: Caller Workstation: LTRANPHD Target Account Name: Administrator Target Account Domain: LTRANPHD
Security	Audit Success	13824	2015-04-22 16:23:01	Microsoft-Windows-Security-Auditing	4797: An attempt was made to query the existence of a blank password for an account. Subject: Security ID: S-1-5-21-1888849264-3803429180-4108621888-1001 Account Name: Liem Account Domain: LTRANPHD Logon ID: 0x20558 Additional Information: Caller Workstation: LTRANPHD Target Account Name: Guest Target Account Domain: LTRANPHD
Security	Audit Success	13824	2015-04-22 16:23:01	Microsoft-Windows-Security-Auditing	4797: An attempt was made to query the existence of a blank password for an account. Subject: Security ID: S-1-5-19 Account Name: LOCAL SERVICE Account Domain: NT AUTHORITY Logon ID: 0x3e5 Additional Information: Caller Workstation: LTRANPHD Target Account Name: Administrator Target Account Domain: LTRANPHD
Security	Audit Success	13824	2015-04-22 16:23:01	Microsoft-Windows-Security-Auditing	4797: An attempt was made to query the existence of a blank password for an account. Subject: Security ID: S-1-5-19 Account Name: LOCAL SERVICE Account Domain: NT AUTHORITY Logon ID: 0x3e5 Additional Information: Caller Workstation: LTRANPHD Target Account Name: Guest Target Account Domain: LTRANPHD
Security	Audit Success	13824	2015-04-22 16:23:01	Microsoft-Windows-Security-Auditing	4797: An attempt was made to query the existence of a blank password for an account. Subject: Security ID: S-1-5-19 Account Name: LOCAL SERVICE Account Domain: NT AUTHORITY Logon ID: 0x3e5 Additional Information: Caller Workstation: LTRANPHD Target Account Name: Liem Target Account Domain: LTRANPHD
Security	Audit Success	13824	2015-04-22 16:23:01	Microsoft-Windows-Security-Auditing	4797: An attempt was made to query the existence of a blank password for an account. Subject: Security ID: S-1-5-19 Account Name: LOCAL SERVICE Account Domain: NT AUTHORITY Logon ID: 0x3e5 Additional Information: Caller Workstation: LTRANPHD Target Account Name: Liem Target Account Domain: LTRANPHD
Security	Audit Success	13824	2015-04-22 16:23:01	Microsoft-Windows-Security-Auditing	4797: An attempt was made to query the existence of a blank password for an account. Subject: Security ID: S-1-5-19 Account Name: LOCAL SERVICE Account Domain: NT AUTHORITY Logon ID: 0x3e5 Additional Information: Caller Workstation: LTRANPHD Target Account Name: Administrator Target Account Domain: LTRANPHD

Security	Audit Success	13824	2015-04-22 16:23:01	Microsoft-Windows-Security-Auditing	4797: An attempt was made to query the existence of a blank password for an account. Subject: Security ID: S-1-5-19 Account Name: LOCAL SERVICE Account Domain: NT AUTHORITY Logon ID: 0x3e5 Additional Information: Caller Workstation: LTRANPHD Target Account Name: Guest Target Account Domain: LTRANPHD
Security	Audit Success	13824	2015-04-22 16:23:01	Microsoft-Windows-Security-Auditing	4797: An attempt was made to query the existence of a blank password for an account. Subject: Security ID: S-1-5-19 Account Name: LOCAL SERVICE Account Domain: NT AUTHORITY Logon ID: 0x3e5 Additional Information: Caller Workstation: LTRANPHD Target Account Name: Liem Target Account Domain: LTRANPHD
Security	Audit Success	13824	2015-04-22 16:23:01	Microsoft-Windows-Security-Auditing	4797: An attempt was made to query the existence of a blank password for an account. Subject: Security ID: S-1-5-19 Account Name: LOCAL SERVICE Account Domain: NT AUTHORITY Logon ID: 0x3e5 Additional Information: Caller Workstation: LTRANPHD Target Account Name: Administrator Target Account Domain: LTRANPHD
Security	Audit Success	13824	2015-04-22 16:23:01	Microsoft-Windows-Security-Auditing	4797: An attempt was made to query the existence of a blank password for an account. Subject: Security ID: S-1-5-19 Account Name: LOCAL SERVICE Account Domain: NT AUTHORITY Logon ID: 0x3e5 Additional Information: Caller Workstation: LTRANPHD Target Account Name: Liem Target Account Domain: LTRANPHD
Security	Audit Success	13824	2015-04-22 16:23:02	Microsoft-Windows-Security-Auditing	4797: An attempt was made to query the existence of a blank password for an account. Subject: Security ID: S-1-5-19 Account Name: LOCAL SERVICE Account Domain: NT AUTHORITY Logon ID: 0x3e5 Additional Information: Caller Workstation: LTRANPHD Target Account Name: Administrator Target Account Domain: LTRANPHD
Security	Audit Success	13824	2015-04-22 16:23:02	Microsoft-Windows-Security-Auditing	4797: An attempt was made to query the existence of a blank password for an account. Subject: Security ID: S-1-5-19 Account Name: LOCAL SERVICE Account Domain: NT AUTHORITY Logon ID: 0x3e5 Additional Information: Caller Workstation: LTRANPHD Target Account Name: Guest Target Account Domain: LTRANPHD
Security	Audit Success	13824	2015-04-22 16:23:02	Microsoft-Windows-Security-Auditing	4797: An attempt was made to query the existence of a blank password for an account. Subject: Security ID: S-1-5-19 Account Name: LOCAL SERVICE Account Domain: NT AUTHORITY Logon ID: 0x3e5 Additional Information: Caller Workstation: LTRANPHD Target Account Name: Liem Target Account Domain: LTRANPHD
Security	Audit Success	13824	2015-04-22 16:23:02	Microsoft-Windows-Security-Auditing	4797: An attempt was made to query the existence of a blank password for an account. Subject: Security ID: S-1-5-19 Account Name: LOCAL SERVICE Account Domain: NT AUTHORITY Logon ID: 0x3e5 Additional Information: Caller Workstation: LTRANPHD Target Account Name: Liem Target Account Domain: LTRANPHD
Security	Audit Success	13824	2015-04-22 16:23:02	Microsoft-Windows-Security-Auditing	4797: An attempt was made to query the existence of a blank password for an account. Subject: Security ID: S-1-5-19 Account Name: LOCAL SERVICE Account Domain: NT AUTHORITY Logon ID: 0x3e5 Additional Information: Caller Workstation: LTRANPHD Target Account Name: Administrator Target Account Domain: LTRANPHD
Security	Audit Success	13824	2015-04-22 16:23:02	Microsoft-Windows-Security-Auditing	4797: An attempt was made to query the existence of a blank password for an account. Subject: Security ID: S-1-5-19 Account Name: LOCAL SERVICE Account Domain: NT AUTHORITY Logon ID: 0x3e5 Additional Information: Caller Workstation: LTRANPHD Target Account Name: Guest Target Account Domain: LTRANPHD
Security	Audit Success	13824	2015-04-22 16:23:02	Microsoft-Windows-Security-Auditing	4797: An attempt was made to query the existence of a blank password for an account. Subject: Security ID: S-1-5-19 Account Name: LOCAL SERVICE Account Domain: NT AUTHORITY Logon ID: 0x3e5 Additional Information: Caller Workstation: LTRANPHD Target Account Name: Liem Target Account Domain: LTRANPHD
Security	Audit Success	13824	2015-04-22 16:23:02	Microsoft-Windows-Security-Auditing	4797: An attempt was made to query the existence of a blank password for an account. Subject: Security ID: S-1-5-19 Account Name: LOCAL SERVICE Account Domain: NT AUTHORITY Logon ID: 0x3e5 Additional Information: Caller Workstation: LTRANPHD Target Account Name: Liem Target Account Domain: LTRANPHD
Security	Audit Success	12544	2015-04-22 16:30:29	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: LTRANPHD$ Account Domain: WORKGROUP Logon ID: 0x3e7 Logon Type: 5 Impersonation Level: %%1833 New Logon: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Logon ID: 0x3e7 Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x234 Process Name: C:\Windows\System32\services.exe Network Information: Workstation Name: Source Network Address: - Source Port: - Detailed Authentication Information: Logon Process: Advapi Authentication Package: Negotiate Transited Services: - Package Name (NTLM only): - Key Length: 0 This event is generated when a logon session is created. It is generated on the computer that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service such as the Server service, or a local process such as Winlogon.exe or Services.exe. The logon type field indicates the kind of logon that occurred. The most common types are 2 (interactive) and 3 (network). The New Logon fields indicate the account for whom the new logon was created, i.e. the account that was logged on. The network fields indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impersonation level field indicates the extent to which a process in the logon session can impersonate. The authentication information fields provide detailed information about this specific logon request. - Logon GUID is a unique identifier that can be used to correlate this event with a KDC event. - Transited services indicate which intermediate services have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indicates the length of the generated session key. This will be 0 if no session key was requested.
Security	Audit Success	12548	2015-04-22 16:30:29	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Logon ID: 0x3e7 Privileges: SeAssignPrimaryTokenPrivilege SeTcbPrivilege SeSecurityPrivilege SeTakeOwnershipPrivilege SeLoadDriverPrivilege SeBackupPrivilege SeRestorePrivilege SeDebugPrivilege SeAuditPrivilege SeSystemEnvironmentPrivilege SeImpersonatePrivilege
					4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: LTRANPHD$ Account Domain: WORKGROUP Logon ID: 0x3e7 Logon Type: 5 Impersonation Level: %%1833 New Logon:

Security	Audit Success	12544	2015-04-22 16:30:31	Microsoft-Windows-Security-Auditing	Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Logon ID: 0x3e7 Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x234 Process Name: C:\Windows\System32\services.exe Network Information: Workstation Name: Source Network Address: - Source Port: - Detailed Authentication Information: Logon Process: Advapi Authentication Package: Negotiate Transited Services: - Package Name (NTLM only): - Key Length: 0 This event is generated when a logon session is created. It is generated on the computer that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service such as the Server service, or a local process such as Winlogon.exe or Services.exe. The logon type field indicates the kind of logon that occurred. The most common types are 2 (interactive) and 3 (network). The New Logon fields indicate the account for whom the new logon was created, i.e. the account that was logged on. The network fields indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impersonation level field indicates the extent to which a process in the logon session can impersonate. The authentication information fields provide detailed information about this specific logon request. - Logon GUID is a unique identifier that can be used to correlate this event with a KDC event. - Transited services indicate which intermediate services have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indicates the length of the generated session key. This will be 0 if no session key was requested.
Security	Audit Success	12548	2015-04-22 16:30:31	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Logon ID: 0x3e7 Privileges: SeAssignPrimaryTokenPrivilege SeTcbPrivilege SeSecurityPrivilege SeTakeOwnershipPrivilege SeLoadDriverPrivilege SeBackupPrivilege SeRestorePrivilege SeDebugPrivilege SeAuditPrivilege SeSystemEnvironmentPrivilege SeImpersonatePrivilege
Security	Audit Success	12545	2015-04-22 16:42:03	Microsoft-Windows-Security-Auditing	4647: User initiated logoff: Subject: Security ID: S-1-5-21-1888849264-3803429180-4108621888-1001 Account Name: Liem Account Domain: LTRANPHD Logon ID: 0x20558 This event is generated when a logoff is initiated. No further user-initiated activity can occur. This event can be interpreted as a logoff event.
Security	Audit Success	103	2015-04-22 16:42:06	Microsoft-Windows-Eventlog	1100: The event logging service has shut down.
Security	Audit Success	12288	2015-04-22 18:07:18	Microsoft-Windows-Security-Auditing	4608: Windows is starting up. This event is logged when LSASS.EXE starts and the auditing subsystem is initialized.
Security	Audit Success	12292	2015-04-22 18:07:18	Microsoft-Windows-Security-Auditing	5033: The Windows Firewall Driver started successfully.
Security	Audit Success	12544	2015-04-22 18:07:18	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-0-0 Account Name: - Account Domain: - Logon ID: 0x0 Logon Type: 0 Impersonation Level: - New Logon: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Logon ID: 0x3e7 Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x4 Process Name: Network Information: Workstation Name: - Source Network Address: - Source Port: - Detailed Authentication Information: Logon Process: - Authentication Package: - Transited Services: - Package Name (NTLM only): - Key Length: 0 This event is generated when a logon session is created. It is generated on the computer that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service such as the Server service, or a local process such as Winlogon.exe or Services.exe. The logon type field indicates the kind of logon that occurred. The most common types are 2 (interactive) and 3 (network). The New Logon fields indicate the account for whom the new logon was created, i.e. the account that was logged on. The network fields indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impersonation level field indicates the extent to which a process in the logon session can impersonate. The authentication information fields provide detailed information about this specific logon request. - Logon GUID is a unique identifier that can be used to correlate this event with a KDC event. - Transited services indicate which intermediate services have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indicates the length of the generated session key. This will be 0 if no session key was requested.
Security	Audit Success	12544	2015-04-22 18:07:18	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: LTRANPHD$ Account Domain: WORKGROUP Logon ID: 0x3e7 Logon Type: 5 Impersonation Level: %%1833 New Logon: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Logon ID: 0x3e7 Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x228 Process Name: C:\Windows\System32\services.exe Network Information: Workstation Name: Source Network Address: - Source Port: - Detailed Authentication Information: Logon Process: Advapi Authentication Package: Negotiate Transited Services: - Package Name (NTLM only): - Key Length: 0 This event is generated when a logon session is created. It is generated on the computer that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service such as the Server service, or a local process such as Winlogon.exe or Services.exe. The logon type field indicates the kind of logon that occurred. The most common types are 2 (interactive) and 3 (network). The New Logon fields indicate the account for whom the new logon was created, i.e. the account that was logged on. The network fields indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impersonation level field indicates the extent to which a process in the logon session can impersonate. The authentication information fields provide detailed information about this specific logon request.

					- Logon GUID is a unique identifier that can be used to correlate this event with a KDC event. - Transited services indicate which intermediate services have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indicates the length of the generated session key. This will be 0 if no session key was requested.
Security	Audit Success	12544	2015-04-22 18:07:18	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: LTRANPHD$ Account Domain: WORKGROUP Logon ID: 0x3e7 Logon Type: 5 Impersonation Level: %%1833 New Logon: Security ID: S-1-5-20 Account Name: NETWORK SERVICE Account Domain: NT AUTHORITY Logon ID: 0x3e4 Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x228 Process Name: C:\Windows\System32\services.exe Network Information: Workstation Name: Source Network Address: - Source Port: - Detailed Authentication Information: Logon Process: Advapi Authentication Package: Negotiate Transited Services: - Package Name (NTLM only): - Key Length: 0 This event is generated when a logon session is created. It is generated on the computer that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service such as the Server service, or a local process such as Winlogon.exe or Services.exe. The logon type field indicates the kind of logon that occurred. The most common types are 2 (interactive) and 3 (network). The New Logon fields indicate the account for whom the new logon was created, i.e. the account that was logged on. The network fields indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impersonation level field indicates the extent to which a process in the logon session can impersonate. The authentication information fields provide detailed information about this specific logon request. - Logon GUID is a unique identifier that can be used to correlate this event with a KDC event. - Transited services indicate which intermediate services have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indicates the length of the generated session key. This will be 0 if no session key was requested.
Security	Audit Success	12544	2015-04-22 18:07:18	Microsoft-Windows-Security-Auditing	4648: A logon was attempted using explicit credentials. Subject: Security ID: S-1-5-18 Account Name: LTRANPHD$ Account Domain: WORKGROUP Logon ID: 0x3e7 Logon GUID: {00000000-0000-0000-0000-000000000000} Account Whose Credentials Were Used: Account Name: DWM-1 Account Domain: Window Manager Logon GUID: {00000000-0000-0000-0000-000000000000} Target Server: Target Server Name: localhost Additional Information: localhost Process Information: Process ID: 0x210 Process Name: C:\Windows\System32\winlogon.exe Network Information: Network Address: - Port: - This event is generated when a process attempts to log on an account by explicitly specifying that account's credentials. This most commonly occurs in batch-type configurations such as scheduled tasks, or when using the RUNAS command.
Security	Audit Success	12544	2015-04-22 18:07:18	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: LTRANPHD$ Account Domain: WORKGROUP Logon ID: 0x3e7 Logon Type: 2 Impersonation Level: %%1833 New Logon: Security ID: S-1-5-90-1 Account Name: DWM-1 Account Domain: Window Manager Logon ID: 0xd8b3 Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x210 Process Name: C:\Windows\System32\winlogon.exe Network Information: Workstation Name: Source Network Address: - Source Port: - Detailed Authentication Information: Logon Process: Advapi Authentication Package: Negotiate Transited Services: - Package Name (NTLM only): - Key Length: 0 This event is generated when a logon session is created. It is generated on the computer that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service such as the Server service, or a local process such as Winlogon.exe or Services.exe. The logon type field indicates the kind of logon that occurred. The most common types are 2 (interactive) and 3 (network). The New Logon fields indicate the account for whom the new logon was created, i.e. the account that was logged on. The network fields indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impersonation level field indicates the extent to which a process in the logon session can impersonate. The authentication information fields provide detailed information about this specific logon request. - Logon GUID is a unique identifier that can be used to correlate this event with a KDC event. - Transited services indicate which intermediate services have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indicates the length of the generated session key. This will be 0 if no session key was requested.
Security	Audit Success	12544	2015-04-22 18:07:18	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: LTRANPHD$ Account Domain: WORKGROUP Logon ID: 0x3e7 Logon Type: 2 Impersonation Level: %%1833 New Logon: Security ID: S-1-5-90-1 Account Name: DWM-1 Account Domain: Window Manager Logon ID: 0xd8ce Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x210 Process Name: C:\Windows\System32\winlogon.exe Network Information: Workstation Name: Source Network Address: - Source Port: - Detailed Authentication Information: Logon Process: Advapi Authentication Package: Negotiate Transited Services: - Package Name (NTLM only): - Key Length: 0 This event is generated when a logon session is created. It is generated on the computer that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service such as the Server service, or a local process such as Winlogon.exe or Services.exe. The logon type field indicates the kind of logon that occurred. The most common types are 2 (interactive) and 3 (network). The New Logon fields indicate the account for whom the new logon was created, i.e. the account that was logged on. The network fields indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impersonation level field indicates the extent to which a process in the logon session can impersonate. The authentication information fields provide detailed information about this specific logon request. - Logon GUID is a unique identifier that can be used to correlate this event with a KDC event. - Transited services indicate which intermediate services have participated in this logon request. - Package name indicates

					which sub-protocol was used among the NTLM protocols. - Key length indicates the length of the generated session key. This will be 0 if no session key was requested.
Security	Audit Success	12544	2015-04-22 18:07:18	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: LTRANPHD$ Account Domain: WORKGROUP Logon ID: 0x3e7 Logon Type: 5 Impersonation Level: %%1833 New Logon: Security ID: S-1-5-19 Account Name: LOCAL SERVICE Account Domain: NT AUTHORITY Logon ID: 0x3e5 Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x228 Process Name: C:\Windows\System32\services.exe Network Information: Workstation Name: Source Network Address: - Source Port: - Detailed Authentication Information: Logon Process: Advapi Authentication Package: Negotiate Transited Services: - Package Name (NTLM only): - Key Length: 0 This event is generated when a logon session is created. It is generated on the computer that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service such as the Server service, or a local process such as Winlogon.exe or Services.exe. The logon type field indicates the kind of logon that occurred. The most common types are 2 (interactive) and 3 (network). The New Logon fields indicate the account for whom the new logon was created, i.e. the account that was logged on. The network fields indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impersonation level field indicates the extent to which a process in the logon session can impersonate. The authentication information fields provide detailed information about this specific logon request. - Logon GUID is a unique identifier that can be used to correlate this event with a KDC event. - Transited services indicate which intermediate services have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indicates the length of the generated session key. This will be 0 if no session key was requested.
Security	Audit Success	12544	2015-04-22 18:07:18	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: LTRANPHD$ Account Domain: WORKGROUP Logon ID: 0x3e7 Logon Type: 5 Impersonation Level: %%1833 New Logon: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Logon ID: 0x3e7 Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x228 Process Name: C:\Windows\System32\services.exe Network Information: Workstation Name: Source Network Address: - Source Port: - Detailed Authentication Information: Logon Process: Advapi Authentication Package: Negotiate Transited Services: - Package Name (NTLM only): - Key Length: 0 This event is generated when a logon session is created. It is generated on the computer that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service such as the Server service, or a local process such as Winlogon.exe or Services.exe. The logon type field indicates the kind of logon that occurred. The most common types are 2 (interactive) and 3 (network). The New Logon fields indicate the account for whom the new logon was created, i.e. the account that was logged on. The network fields indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impersonation level field indicates the extent to which a process in the logon session can impersonate. The authentication information fields provide detailed information about this specific logon request. - Logon GUID is a unique identifier that can be used to correlate this event with a KDC event. - Transited services indicate which intermediate services have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indicates the length of the generated session key. This will be 0 if no session key was requested.
Security	Audit Success	12544	2015-04-22 18:07:18	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: LTRANPHD$ Account Domain: WORKGROUP Logon ID: 0x3e7 Logon Type: 5 Impersonation Level: %%1833 New Logon: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Logon ID: 0x3e7 Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x228 Process Name: C:\Windows\System32\services.exe Network Information: Workstation Name: Source Network Address: - Source Port: - Detailed Authentication Information: Logon Process: Advapi Authentication Package: Negotiate Transited Services: - Package Name (NTLM only): - Key Length: 0 This event is generated when a logon session is created. It is generated on the computer that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service such as the Server service, or a local process such as Winlogon.exe or Services.exe. The logon type field indicates the kind of logon that occurred. The most common types are 2 (interactive) and 3 (network). The New Logon fields indicate the account for whom the new logon was created, i.e. the account that was logged on. The network fields indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impersonation level field indicates the extent to which a process in the logon session can impersonate. The authentication information fields provide detailed information about this specific logon request. - Logon GUID is a unique identifier that can be used to correlate this event with a KDC event. - Transited services indicate which intermediate services have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indicates the length of the generated session key. This will be 0 if no session key was requested.
					4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: LTRANPHD$ Account Domain: WORKGROUP Logon ID: 0x3e7 Logon Type: 5 Impersonation Level: %%1833 New Logon: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Logon ID: 0x3e7 Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x228 Process Name: C:\Windows\System32\services.exe Network Information: Workstation Name: Source Network Address: - Source Port: - Detailed Authentication Information: Logon Process: Advapi Authentication Package: Negotiate Transited Services: - Package Name (NTLM only): - Key Length: 0 This event is generated when a logon session is created. It is generated on the computer that was accessed. The subject fields indicate the account on the local

Security	Audit Success	12544	2015-04-22 18:07:18	Microsoft-Windows-Security-Auditing	system which requested the logon. This is most commonly a service such as the Server service, or a local process such as Winlogon.exe or Services.exe. The logon type field indicates the kind of logon that occurred. The most common types are 2 (interactive) and 3 (network). The New Logon fields indicate the account for whom the new logon was created, i.e. the account that was logged on. The network fields indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impersonation level field indicates the extent to which a process in the logon session can impersonate. The authentication information fields provide detailed information about this specific logon request. - Logon GUID is a unique identifier that can be used to correlate this event with a KDC event. - Transited services indicate which intermediate services have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indicates the length of the generated session key. This will be 0 if no session key was requested.
Security	Audit Success	12548	2015-04-22 18:07:18	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Logon ID: 0x3e7 Privileges: SeAssignPrimaryTokenPrivilege SeTcbPrivilege SeSecurityPrivilege SeTakeOwnershipPrivilege SeLoadDriverPrivilege SeBackupPrivilege SeRestorePrivilege SeDebugPrivilege SeAuditPrivilege SeSystemEnvironmentPrivilege SeImpersonatePrivilege
Security	Audit Success	12548	2015-04-22 18:07:18	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-20 Account Name: NETWORK SERVICE Account Domain: NT AUTHORITY Logon ID: 0x3e4 Privileges: SeAssignPrimaryTokenPrivilege SeAuditPrivilege SeImpersonatePrivilege
Security	Audit Success	12548	2015-04-22 18:07:18	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-90-1 Account Name: DWM-1 Account Domain: Window Manager Logon ID: 0xd8b3 Privileges: SeAssignPrimaryTokenPrivilege SeAuditPrivilege SeImpersonatePrivilege
Security	Audit Success	12548	2015-04-22 18:07:18	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-90-1 Account Name: DWM-1 Account Domain: Window Manager Logon ID: 0xd8ce Privileges: SeAssignPrimaryTokenPrivilege SeAuditPrivilege
Security	Audit Success	12548	2015-04-22 18:07:18	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-19 Account Name: LOCAL SERVICE Account Domain: NT AUTHORITY Logon ID: 0x3e5 Privileges: SeAssignPrimaryTokenPrivilege SeAuditPrivilege SeImpersonatePrivilege
Security	Audit Success	12548	2015-04-22 18:07:18	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Logon ID: 0x3e7 Privileges: SeAssignPrimaryTokenPrivilege SeTcbPrivilege SeSecurityPrivilege SeTakeOwnershipPrivilege SeLoadDriverPrivilege SeBackupPrivilege SeRestorePrivilege SeDebugPrivilege SeAuditPrivilege SeSystemEnvironmentPrivilege SeImpersonatePrivilege
Security	Audit Success	12548	2015-04-22 18:07:18	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Logon ID: 0x3e7 Privileges: SeAssignPrimaryTokenPrivilege SeTcbPrivilege SeSecurityPrivilege SeTakeOwnershipPrivilege SeLoadDriverPrivilege SeBackupPrivilege SeRestorePrivilege SeDebugPrivilege SeAuditPrivilege SeSystemEnvironmentPrivilege SeImpersonatePrivilege
Security	Audit Success	12548	2015-04-22 18:07:18	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Logon ID: 0x3e7 Privileges: SeAssignPrimaryTokenPrivilege SeTcbPrivilege SeSecurityPrivilege SeTakeOwnershipPrivilege SeLoadDriverPrivilege SeBackupPrivilege SeRestorePrivilege SeDebugPrivilege SeAuditPrivilege SeSystemEnvironmentPrivilege SeImpersonatePrivilege
Security	Audit Success	13568	2015-04-22 18:07:18	Microsoft-Windows-Security-Auditing	4902: The Per-user audit policy table was created. Number of Elements: 0 Policy ID: 0x88fb
Security	Audit Success	12292	2015-04-22 18:07:19	Microsoft-Windows-Security-Auditing	5024: The Windows Firewall service started successfully.
Security	Audit Success	12544	2015-04-22 18:07:19	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: LTRANPHD$ Account Domain: WORKGROUP Logon ID: 0x3e7 Logon Type: 5 Impersonation Level: %%1833 New Logon: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Logon ID: 0x3e7 Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x228 Process Name: C:\Windows\System32\services.exe Network Information: Workstation Name: Source Network Address: - Source Port: - Detailed Authentication Information: Logon Process: Advapi Authentication Package: Negotiate Transited Services: - Package Name (NTLM only): - Key Length: 0 This event is generated when a logon session is created. It is generated on the computer that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service such as the Server service, or a local process such as Winlogon.exe or Services.exe. The logon type field indicates the kind of logon that occurred. The most common types are 2 (interactive) and 3 (network). The New Logon fields indicate the account for whom the new logon was created, i.e. the account that was logged on. The network fields indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impersonation level field indicates the extent to which a process in the logon session can impersonate. The authentication information fields provide detailed information about this specific logon request. - Logon GUID is a unique identifier that can be used to correlate this event with a KDC event. - Transited services indicate which intermediate services have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indicates the length of the generated session key. This will be 0 if no session key was requested.
					4624: An account was successfully logged on. Subject: Security ID: S-1-0-0 Account Name: - Account Domain:

Security	Audit Success	12544	2015-04-22 18:07:19	Microsoft-Windows-Security-Auditing	- Logon ID: 0x0 Logon Type: 3 Impersonation Level: %%1833 New Logon: Security ID: S-1-5-7 Account Name: ANONYMOUS LOGON Account Domain: NT AUTHORITY Logon ID: 0x15777 Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x0 Process Name: - Network Information: Workstation Name: Source Network Address: - Source Port: - Detailed Authentication Information: Logon Process: NtLmSsp Authentication Package: NTLM Transited Services: - Package Name (NTLM only): NTLM V1 Key Length: 0 This event is generated when a logon session is created. It is generated on the computer that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service such as the Server service, or a local process such as Winlogon.exe or Services.exe. The logon type field indicates the kind of logon that occurred. The most common types are 2 (interactive) and 3 (network). The New Logon fields indicate the account for whom the new logon was created, i.e. the account that was logged on. The network fields indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impersonation level field indicates the extent to which a process in the logon session can impersonate. The authentication information fields provide detailed information about this specific logon request. - Logon GUID is a unique identifier that can be used to correlate this event with a KDC event. - Transited services indicate which intermediate services have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indicates the length of the generated session key. This will be 0 if no session key was requested.
Security	Audit Success	12548	2015-04-22 18:07:19	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Logon ID: 0x3e7 Privileges: SeAssignPrimaryTokenPrivilege SeTcbPrivilege SeSecurityPrivilege SeTakeOwnershipPrivilege SeLoadDriverPrivilege SeBackupPrivilege SeRestorePrivilege SeDebugPrivilege SeAuditPrivilege SeSystemEnvironmentPrivilege SeImpersonatePrivilege
Security	Audit Success	12544	2015-04-22 18:07:24	Microsoft-Windows-Security-Auditing	4648: A logon was attempted using explicit credentials. Subject: Security ID: S-1-5-18 Account Name: LTRANPHD$ Account Domain: WORKGROUP Logon ID: 0x3e7 Logon GUID: {00000000-0000-0000-0000-000000000000} Account Whose Credentials Were Used: Account Name: Liem Account Domain: LTRANPHD Logon GUID: {00000000-0000-0000-0000-000000000000} Target Server: Target Server Name: localhost Additional Information: localhost Process Information: Process ID: 0x210 Process Name: C:\Windows\System32\winlogon.exe Network Information: Network Address: 127.0.0.1 Port: 0 This event is generated when a process attempts to log on an account by explicitly specifying that account's credentials. This most commonly occurs in batch-type configurations such as scheduled tasks, or when using the RUNAS command.
Security	Audit Success	12544	2015-04-22 18:07:24	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: LTRANPHD$ Account Domain: WORKGROUP Logon ID: 0x3e7 Logon Type: 2 Impersonation Level: %%1833 New Logon: Security ID: S-1-5-21-1888849264-3803429180-4108621888-1001 Account Name: Liem Account Domain: LTRANPHD Logon ID: 0x2b2fe Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x210 Process Name: C:\Windows\System32\winlogon.exe Network Information: Workstation Name: LTRANPHD Source Network Address: 127.0.0.1 Source Port: 0 Detailed Authentication Information: Logon Process: User32 Authentication Package: Negotiate Transited Services: - Package Name (NTLM only): - Key Length: 0 This event is generated when a logon session is created. It is generated on the computer that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service such as the Server service, or a local process such as Winlogon.exe or Services.exe. The logon type field indicates the kind of logon that occurred. The most common types are 2 (interactive) and 3 (network). The New Logon fields indicate the account for whom the new logon was created, i.e. the account that was logged on. The network fields indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impersonation level field indicates the extent to which a process in the logon session can impersonate. The authentication information fields provide detailed information about this specific logon request. - Logon GUID is a unique identifier that can be used to correlate this event with a KDC event. - Transited services indicate which intermediate services have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indicates the length of the generated session key. This will be 0 if no session key was requested.
Security	Audit Success	12544	2015-04-22 18:07:24	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: LTRANPHD$ Account Domain: WORKGROUP Logon ID: 0x3e7 Logon Type: 2 Impersonation Level: %%1833 New Logon: Security ID: S-1-5-21-1888849264-3803429180-4108621888-1001 Account Name: Liem Account Domain: LTRANPHD Logon ID: 0x2b34b Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x210 Process Name: C:\Windows\System32\winlogon.exe Network Information: Workstation Name: LTRANPHD Source Network Address: 127.0.0.1 Source Port: 0 Detailed Authentication Information: Logon Process: User32 Authentication Package: Negotiate Transited Services: - Package Name (NTLM only): - Key Length: 0 This event is generated when a logon session is created. It is generated on the computer that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service such as the Server service, or a local process such as Winlogon.exe or Services.exe. The logon type field indicates the kind of logon that occurred. The most common types are 2 (interactive) and 3 (network). The New Logon fields indicate the account for whom the new logon was created, i.e. the account that was logged on. The network fields indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impersonation level field indicates the extent to which a process in the logon session can impersonate. The authentication information fields provide detailed information about this specific logon request. - Logon GUID is a unique identifier that can be used to correlate this event with a KDC event. - Transited services indicate which intermediate services have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length

					indicates the length of the generated session key. This will be 0 if no session key was requested.
Security	Audit Success	12544	2015-04-22 18:07:24	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: LTRANPHD$ Account Domain: WORKGROUP Logon ID: 0x3e7 Logon Type: 5 Impersonation Level: %%1833 New Logon: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Logon ID: 0x3e7 Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x228 Process Name: C:\Windows\System32\services.exe Network Information: Workstation Name: Source Network Address: - Source Port: - Detailed Authentication Information: Logon Process: Advapi Authentication Package: Negotiate Transited Services: - Package Name (NTLM only): - Key Length: 0 This event is generated when a logon session is created. It is generated on the computer that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service such as the Server service, or a local process such as Winlogon.exe or Services.exe. The logon type field indicates the kind of logon that occurred. The most common types are 2 (interactive) and 3 (network). The New Logon fields indicate the account for whom the new logon was created, i.e. the account that was logged on. The network fields indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impersonation level field indicates the extent to which a process in the logon session can impersonate. The authentication information fields provide detailed information about this specific logon request. - Logon GUID is a unique identifier that can be used to correlate this event with a KDC event. - Transited services indicate which intermediate services have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indicates the length of the generated session key. This will be 0 if no session key was requested.
Security	Audit Success	12548	2015-04-22 18:07:24	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-21-1888849264-3803429180-4108621888-1001 Account Name: Liem Account Domain: LTRANPHD Logon ID: 0x2b2fe Privileges: SeSecurityPrivilege SeTakeOwnershipPrivilege SeLoadDriverPrivilege SeBackupPrivilege SeRestorePrivilege SeDebugPrivilege SeSystemEnvironmentPrivilege SeImpersonatePrivilege
Security	Audit Success	12548	2015-04-22 18:07:24	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Logon ID: 0x3e7 Privileges: SeAssignPrimaryTokenPrivilege SeTcbPrivilege SeSecurityPrivilege SeTakeOwnershipPrivilege SeLoadDriverPrivilege SeBackupPrivilege SeRestorePrivilege SeDebugPrivilege SeAuditPrivilege SeSystemEnvironmentPrivilege SeImpersonatePrivilege
Security	Audit Success	13824	2015-04-22 18:07:26	Microsoft-Windows-Security-Auditing	4797: An attempt was made to query the existence of a blank password for an account. Subject: Security ID: S-1-5-21-1888849264-3803429180-4108621888-1001 Account Name: Liem Account Domain: LTRANPHD Logon ID: 0x2b34b Additional Information: Caller Workstation: LTRANPHD Target Account Name: Administrator Target Account Domain: LTRANPHD
Security	Audit Success	13824	2015-04-22 18:07:26	Microsoft-Windows-Security-Auditing	4797: An attempt was made to query the existence of a blank password for an account. Subject: Security ID: S-1-5-21-1888849264-3803429180-4108621888-1001 Account Name: Liem Account Domain: LTRANPHD Logon ID: 0x2b34b Additional Information: Caller Workstation: LTRANPHD Target Account Name: Guest Target Account Domain: LTRANPHD
Security	Audit Success	13824	2015-04-22 18:07:26	Microsoft-Windows-Security-Auditing	4797: An attempt was made to query the existence of a blank password for an account. Subject: Security ID: S-1-5-21-1888849264-3803429180-4108621888-1001 Account Name: Liem Account Domain: LTRANPHD Logon ID: 0x2b34b Additional Information: Caller Workstation: LTRANPHD Target Account Name: Administrator Target Account Domain: LTRANPHD
Security	Audit Success	13824	2015-04-22 18:07:26	Microsoft-Windows-Security-Auditing	4797: An attempt was made to query the existence of a blank password for an account. Subject: Security ID: S-1-5-21-1888849264-3803429180-4108621888-1001 Account Name: Liem Account Domain: LTRANPHD Logon ID: 0x2b34b Additional Information: Caller Workstation: LTRANPHD Target Account Name: Guest Target Account Domain: LTRANPHD
Security	Audit Success	13824	2015-04-22 18:07:46	Microsoft-Windows-Security-Auditing	4797: An attempt was made to query the existence of a blank password for an account. Subject: Security ID: S-1-5-19 Account Name: LOCAL SERVICE Account Domain: NT AUTHORITY Logon ID: 0x3e5 Additional Information: Caller Workstation: LTRANPHD Target Account Name: Administrator Target Account Domain: LTRANPHD
Security	Audit Success	13824	2015-04-22 18:07:46	Microsoft-Windows-Security-Auditing	4797: An attempt was made to query the existence of a blank password for an account. Subject: Security ID: S-1-5-19 Account Name: LOCAL SERVICE Account Domain: NT AUTHORITY Logon ID: 0x3e5 Additional Information: Caller Workstation: LTRANPHD Target Account Name: Guest Target Account Domain: LTRANPHD
Security	Audit Success	13824	2015-04-22 18:07:46	Microsoft-Windows-Security-Auditing	4797: An attempt was made to query the existence of a blank password for an account. Subject: Security ID: S-1-5-19 Account Name: LOCAL SERVICE Account Domain: NT AUTHORITY Logon ID: 0x3e5 Additional Information: Caller Workstation: LTRANPHD Target Account Name: Liem Target Account Domain: LTRANPHD
Security	Audit Success	13824	2015-04-22 18:07:46	Microsoft-Windows-Security-Auditing	4797: An attempt was made to query the existence of a blank password for an account. Subject: Security ID: S-1-5-19 Account Name: LOCAL SERVICE Account Domain: NT AUTHORITY Logon ID: 0x3e5 Additional Information: Caller Workstation: LTRANPHD Target Account Name: Liem Target Account Domain: LTRANPHD
Security	Audit Success	13824	2015-04-22 18:07:46	Microsoft-Windows-Security-Auditing	4797: An attempt was made to query the existence of a blank password for an account. Subject: Security ID: S-1-5-19 Account Name: LOCAL SERVICE Account Domain: NT AUTHORITY Logon ID: 0x3e5 Additional Information: Caller Workstation: LTRANPHD Target Account Name: Administrator Target Account Domain: LTRANPHD
Security	Audit Success	13824	2015-04-22 18:07:46	Microsoft-Windows-Security-Auditing	4797: An attempt was made to query the existence of a blank password for an account. Subject: Security ID: S-1-5-19 Account Name: LOCAL SERVICE Account Domain: NT AUTHORITY Logon ID: 0x3e5 Additional Information: Caller Workstation: LTRANPHD Target Account Name: Guest Target Account Domain: LTRANPHD

Security	Audit Success	13824	2015-04-22 18:07:46	Microsoft-Windows-Security-Auditing	4797: An attempt was made to query the existence of a blank password for an account. Subject: Security ID: S-1-5-19 Account Name: LOCAL SERVICE Account Domain: NT AUTHORITY Logon ID: 0x3e5 Additional Information: Caller Workstation: LTRANPHD Target Account Name: Liem Target Account Domain: LTRANPHD
Security	Audit Success	13824	2015-04-22 18:07:46	Microsoft-Windows-Security-Auditing	4797: An attempt was made to query the existence of a blank password for an account. Subject: Security ID: S-1-5-19 Account Name: LOCAL SERVICE Account Domain: NT AUTHORITY Logon ID: 0x3e5 Additional Information: Caller Workstation: LTRANPHD Target Account Name: Liem Target Account Domain: LTRANPHD
Security	Audit Success	12544	2015-04-22 18:07:50	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: LTRANPHD$ Account Domain: WORKGROUP Logon ID: 0x3e7 Logon Type: 5 Impersonation Level: %%1833 New Logon: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Logon ID: 0x3e7 Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x228 Process Name: C:\Windows\System32\services.exe Network Information: Workstation Name: Source Network Address: - Source Port: - Detailed Authentication Information: Logon Process: Advapi Authentication Package: Negotiate Transited Services: - Package Name (NTLM only): - Key Length: 0 This event is generated when a logon session is created. It is generated on the computer that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service such as the Server service, or a local process such as Winlogon.exe or Services.exe. The logon type field indicates the kind of logon that occurred. The most common types are 2 (interactive) and 3 (network). The New Logon fields indicate the account for whom the new logon was created, i.e. the account that was logged on. The network fields indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impersonation level field indicates the extent to which a process in the logon session can impersonate. The authentication information fields provide detailed information about this specific logon request. - Logon GUID is a unique identifier that can be used to correlate this event with a KDC event. - Transited services indicate which intermediate services have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indicates the length of the generated session key. This will be 0 if no session key was requested.
Security	Audit Success	12548	2015-04-22 18:07:50	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Logon ID: 0x3e7 Privileges: SeAssignPrimaryTokenPrivilege SeTcbPrivilege SeSecurityPrivilege SeTakeOwnershipPrivilege SeLoadDriverPrivilege SeBackupPrivilege SeRestorePrivilege SeDebugPrivilege SeAuditPrivilege SeSystemEnvironmentPrivilege SeImpersonatePrivilege
Security	Audit Success	13824	2015-04-22 18:08:10	Microsoft-Windows-Security-Auditing	4797: An attempt was made to query the existence of a blank password for an account. Subject: Security ID: S-1-5-21-1888849264-3803429180-4108621888-1001 Account Name: Liem Account Domain: LTRANPHD Logon ID: 0x2b34b Additional Information: Caller Workstation: LTRANPHD Target Account Name: Administrator Target Account Domain: LTRANPHD
Security	Audit Success	13824	2015-04-22 18:08:10	Microsoft-Windows-Security-Auditing	4797: An attempt was made to query the existence of a blank password for an account. Subject: Security ID: S-1-5-21-1888849264-3803429180-4108621888-1001 Account Name: Liem Account Domain: LTRANPHD Logon ID: 0x2b34b Additional Information: Caller Workstation: LTRANPHD Target Account Name: Guest Target Account Domain: LTRANPHD
Security	Audit Success	13824	2015-04-22 18:08:10	Microsoft-Windows-Security-Auditing	4797: An attempt was made to query the existence of a blank password for an account. Subject: Security ID: S-1-5-21-1888849264-3803429180-4108621888-1001 Account Name: Liem Account Domain: LTRANPHD Logon ID: 0x2b34b Additional Information: Caller Workstation: LTRANPHD Target Account Name: Administrator Target Account Domain: LTRANPHD
Security	Audit Success	13824	2015-04-22 18:08:10	Microsoft-Windows-Security-Auditing	4797: An attempt was made to query the existence of a blank password for an account. Subject: Security ID: S-1-5-21-1888849264-3803429180-4108621888-1001 Account Name: Liem Account Domain: LTRANPHD Logon ID: 0x2b34b Additional Information: Caller Workstation: LTRANPHD Target Account Name: Guest Target Account Domain: LTRANPHD
Security	Audit Success	103	2015-04-22 18:16:03	Microsoft-Windows-Eventlog	1100: The event logging service has shut down.
Security	Audit Success	12545	2015-04-22 18:16:03	Microsoft-Windows-Security-Auditing	4647: User initiated logoff: Subject: Security ID: S-1-5-21-1888849264-3803429180-4108621888-1001 Account Name: Liem Account Domain: LTRANPHD Logon ID: 0x2b34b This event is generated when a logoff is initiated. No further user-initiated activity can occur. This event can be interpreted as a logoff event.
Security	Audit Success	12288	2015-04-22 18:52:56	Microsoft-Windows-Security-Auditing	4608: Windows is starting up. This event is logged when LSASS.EXE starts and the auditing subsystem is initialized.
Security	Audit Success	12544	2015-04-22 18:52:56	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-0-0 Account Name: - Account Domain: - Logon ID: 0x0 Logon Type: 0 Impersonation Level: - New Logon: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Logon ID: 0x3e7 Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x4 Process Name: Network Information: Workstation Name: - Source Network Address: - Source Port: - Detailed Authentication Information: Logon Process: - Authentication Package: - Transited Services: - Package Name (NTLM only): - Key Length: 0 This event is generated when a logon session is created. It is generated on the computer that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service such as the Server service, or a local process such as Winlogon.exe or Services.exe. The logon type field indicates the kind of logon that occurred. The most common types are 2 (interactive) and 3 (network). The New Logon fields indicate the account for whom the new logon was created, i.e. the account that was logged

					on. The network fields indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impersonation level field indicates the extent to which a process in the logon session can impersonate. The authentication information fields provide detailed information about this specific logon request. - Logon GUID is a unique identifier that can be used to correlate this event with a KDC event. - Transited services indicate which intermediate services have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indicates the length of the generated session key. This will be 0 if no session key was requested.
Security	Audit Success	13568	2015-04-22 18:52:56	Microsoft-Windows-Security-Auditing	4902: The Per-user audit policy table was created. Number of Elements: 0 Policy ID: 0x71b2
Security	Audit Success	12544	2015-04-22 18:52:57	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: LTRANPHD$ Account Domain: WORKGROUP Logon ID: 0x3e7 Logon Type: 5 Impersonation Level: %%1833 New Logon: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Logon ID: 0x3e7 Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x240 Process Name: C:\Windows\System32\services.exe Network Information: Workstation Name: Source Network Address: - Source Port: - Detailed Authentication Information: Logon Process: Advapi Authentication Package: Negotiate Transited Services: - Package Name (NTLM only): - Key Length: 0 This event is generated when a logon session is created. It is generated on the computer that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service such as the Server service, or a local process such as Winlogon.exe or Services.exe. The logon type field indicates the kind of logon that occurred. The most common types are 2 (interactive) and 3 (network). The New Logon fields indicate the account for whom the new logon was created, i.e. the account that was logged on. The network fields indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impersonation level field indicates the extent to which a process in the logon session can impersonate. The authentication information fields provide detailed information about this specific logon request. - Logon GUID is a unique identifier that can be used to correlate this event with a KDC event. - Transited services indicate which intermediate services have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indicates the length of the generated session key. This will be 0 if no session key was requested.
Security	Audit Success	12544	2015-04-22 18:52:57	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: LTRANPHD$ Account Domain: WORKGROUP Logon ID: 0x3e7 Logon Type: 5 Impersonation Level: %%1833 New Logon: Security ID: S-1-5-20 Account Name: NETWORK SERVICE Account Domain: NT AUTHORITY Logon ID: 0x3e4 Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x240 Process Name: C:\Windows\System32\services.exe Network Information: Workstation Name: Source Network Address: - Source Port: - Detailed Authentication Information: Logon Process: Advapi Authentication Package: Negotiate Transited Services: - Package Name (NTLM only): - Key Length: 0 This event is generated when a logon session is created. It is generated on the computer that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service such as the Server service, or a local process such as Winlogon.exe or Services.exe. The logon type field indicates the kind of logon that occurred. The most common types are 2 (interactive) and 3 (network). The New Logon fields indicate the account for whom the new logon was created, i.e. the account that was logged on. The network fields indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impersonation level field indicates the extent to which a process in the logon session can impersonate. The authentication information fields provide detailed information about this specific logon request. - Logon GUID is a unique identifier that can be used to correlate this event with a KDC event. - Transited services indicate which intermediate services have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indicates the length of the generated session key. This will be 0 if no session key was requested.
Security	Audit Success	12544	2015-04-22 18:52:57	Microsoft-Windows-Security-Auditing	4648: A logon was attempted using explicit credentials. Subject: Security ID: S-1-5-18 Account Name: LTRANPHD$ Account Domain: WORKGROUP Logon ID: 0x3e7 Logon GUID: {00000000-0000-0000-0000-000000000000} Account Whose Credentials Were Used: Account Name: DWM-1 Account Domain: Window Manager Logon GUID: {00000000-0000-0000-0000-000000000000} Target Server: Target Server Name: localhost Additional Information: localhost Process Information: Process ID: 0x208 Process Name: C:\Windows\System32\winlogon.exe Network Information: Network Address: - Port: - This event is generated when a process attempts to log on an account by explicitly specifying that account's credentials. This most commonly occurs in batch-type configurations such as scheduled tasks, or when using the RUNAS command.
Security	Audit Success	12544	2015-04-22	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: LTRANPHD$ Account Domain: WORKGROUP Logon ID: 0x3e7 Logon Type: 2 Impersonation Level: %%1833 New Logon: Security ID: S-1-5-90-1 Account Name: DWM-1 Account Domain: Window Manager Logon ID: 0xc470 Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x208 Process Name: C:\Windows\System32\winlogon.exe Network Information: Workstation Name: Source Network Address: - Source Port: - Detailed Authentication Information: Logon Process: Advapi Authentication Package: Negotiate Transited Services: - Package Name (NTLM only): - Key Length: 0 This event is generated when a logon session is created. It is generated on the computer that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service such as the Server service, or a local process such as Winlogon.exe or Services.exe. The logon type field indicates the kind of logon that occurred.

			18:52:57		The most common types are 2 (interactive) and 3 (network). The New Logon fields indicate the account for whom the new logon was created, i.e. the account that was logged on. The network fields indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impersonation level field indicates the extent to which a process in the logon session can impersonate. The authentication information fields provide detailed information about this specific logon request. - Logon GUID is a unique identifier that can be used to correlate this event with a KDC event. - Transited services indicate which intermediate services have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indicates the length of the generated session key. This will be 0 if no session key was requested.
Security	Audit Success	12544	2015-04-22 18:52:57	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: LTRANPHD$ Account Domain: WORKGROUP Logon ID: 0x3e7 Logon Type: 2 Impersonation Level: %%1833 New Logon: Security ID: S-1-5-90-1 Account Name: DWM-1 Account Domain: Window Manager Logon ID: 0xc482 Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x208 Process Name: C:\Windows\System32\winlogon.exe Network Information: Workstation Name: Source Network Address: - Source Port: - Detailed Authentication Information: Logon Process: Advapi Authentication Package: Negotiate Transited Services: - Package Name (NTLM only): - Key Length: 0 This event is generated when a logon session is created. It is generated on the computer that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service such as the Server service, or a local process such as Winlogon.exe or Services.exe. The logon type field indicates the kind of logon that occurred. The most common types are 2 (interactive) and 3 (network). The New Logon fields indicate the account for whom the new logon was created, i.e. the account that was logged on. The network fields indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impersonation level field indicates the extent to which a process in the logon session can impersonate. The authentication information fields provide detailed information about this specific logon request. - Logon GUID is a unique identifier that can be used to correlate this event with a KDC event. - Transited services indicate which intermediate services have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indicates the length of the generated session key. This will be 0 if no session key was requested.
Security	Audit Success	12544	2015-04-22 18:52:57	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: LTRANPHD$ Account Domain: WORKGROUP Logon ID: 0x3e7 Logon Type: 5 Impersonation Level: %%1833 New Logon: Security ID: S-1-5-19 Account Name: LOCAL SERVICE Account Domain: NT AUTHORITY Logon ID: 0x3e5 Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x240 Process Name: C:\Windows\System32\services.exe Network Information: Workstation Name: Source Network Address: - Source Port: - Detailed Authentication Information: Logon Process: Advapi Authentication Package: Negotiate Transited Services: - Package Name (NTLM only): - Key Length: 0 This event is generated when a logon session is created. It is generated on the computer that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service such as the Server service, or a local process such as Winlogon.exe or Services.exe. The logon type field indicates the kind of logon that occurred. The most common types are 2 (interactive) and 3 (network). The New Logon fields indicate the account for whom the new logon was created, i.e. the account that was logged on. The network fields indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impersonation level field indicates the extent to which a process in the logon session can impersonate. The authentication information fields provide detailed information about this specific logon request. - Logon GUID is a unique identifier that can be used to correlate this event with a KDC event. - Transited services indicate which intermediate services have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indicates the length of the generated session key. This will be 0 if no session key was requested.
Security	Audit Success	12544	2015-04-22 18:52:57	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: LTRANPHD$ Account Domain: WORKGROUP Logon ID: 0x3e7 Logon Type: 5 Impersonation Level: %%1833 New Logon: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Logon ID: 0x3e7 Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x240 Process Name: C:\Windows\System32\services.exe Network Information: Workstation Name: Source Network Address: - Source Port: - Detailed Authentication Information: Logon Process: Advapi Authentication Package: Negotiate Transited Services: - Package Name (NTLM only): - Key Length: 0 This event is generated when a logon session is created. It is generated on the computer that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service such as the Server service, or a local process such as Winlogon.exe or Services.exe. The logon type field indicates the kind of logon that occurred. The most common types are 2 (interactive) and 3 (network). The New Logon fields indicate the account for whom the new logon was created, i.e. the account that was logged on. The network fields indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impersonation level field indicates the extent to which a process in the logon session can impersonate. The authentication information fields provide detailed information about this specific logon request. - Logon GUID is a unique identifier that can be used to correlate this event with a KDC event. - Transited services indicate which intermediate services have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indicates the length of the generated session key. This will be 0 if no session key was requested.
					4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account

Security	Audit Success	12548	2015-04-22 18:52:57	Microsoft-Windows-Security-Auditing	Domain: NT AUTHORITY Logon ID: 0x3e7 Privileges: SeAssignPrimaryTokenPrivilege SeTcbPrivilege SeSecurityPrivilege SeTakeOwnershipPrivilege SeLoadDriverPrivilege SeBackupPrivilege SeRestorePrivilege SeDebugPrivilege SeAuditPrivilege SeSystemEnvironmentPrivilege SeImpersonatePrivilege
Security	Audit Success	12548	2015-04-22 18:52:57	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-20 Account Name: NETWORK SERVICE Account Domain: NT AUTHORITY Logon ID: 0x3e4 Privileges: SeAssignPrimaryTokenPrivilege SeAuditPrivilege SeImpersonatePrivilege
Security	Audit Success	12548	2015-04-22 18:52:57	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-90-1 Account Name: DWM-1 Account Domain: Window Manager Logon ID: 0xc470 Privileges: SeAssignPrimaryTokenPrivilege SeAuditPrivilege SeImpersonatePrivilege
Security	Audit Success	12548	2015-04-22 18:52:57	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-90-1 Account Name: DWM-1 Account Domain: Window Manager Logon ID: 0xc482 Privileges: SeAssignPrimaryTokenPrivilege SeAuditPrivilege
Security	Audit Success	12548	2015-04-22 18:52:57	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-19 Account Name: LOCAL SERVICE Account Domain: NT AUTHORITY Logon ID: 0x3e5 Privileges: SeAssignPrimaryTokenPrivilege SeAuditPrivilege SeImpersonatePrivilege
Security	Audit Success	12548	2015-04-22 18:52:57	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Logon ID: 0x3e7 Privileges: SeAssignPrimaryTokenPrivilege SeTcbPrivilege SeSecurityPrivilege SeTakeOwnershipPrivilege SeLoadDriverPrivilege SeBackupPrivilege SeRestorePrivilege SeDebugPrivilege SeAuditPrivilege SeSystemEnvironmentPrivilege SeImpersonatePrivilege
Security	Audit Success	12544	2015-04-22 18:52:58	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: LTRANPHD$ Account Domain: WORKGROUP Logon ID: 0x3e7 Logon Type: 5 Impersonation Level: %%1833 New Logon: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Logon ID: 0x3e7 Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x240 Process Name: C:\Windows\System32\services.exe Network Information: Workstation Name: Source Network Address: - Source Port: - Detailed Authentication Information: Logon Process: Advapi Authentication Package: Negotiate Transited Services: - Package Name (NTLM only): - Key Length: 0 This event is generated when a logon session is created. It is generated on the computer that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service such as the Server service, or a local process such as Winlogon.exe or Services.exe. The logon type field indicates the kind of logon that occurred. The most common types are 2 (interactive) and 3 (network). The New Logon fields indicate the account for whom the new logon was created, i.e. the account that was logged on. The network fields indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impersonation level field indicates the extent to which a process in the logon session can impersonate. The authentication information fields provide detailed information about this specific logon request. - Logon GUID is a unique identifier that can be used to correlate this event with a KDC event. - Transited services indicate which intermediate services have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indicates the length of the generated session key. This will be 0 if no session key was requested.
Security	Audit Success	12548	2015-04-22 18:52:58	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Logon ID: 0x3e7 Privileges: SeAssignPrimaryTokenPrivilege SeTcbPrivilege SeSecurityPrivilege SeTakeOwnershipPrivilege SeLoadDriverPrivilege SeBackupPrivilege SeRestorePrivilege SeDebugPrivilege SeAuditPrivilege SeSystemEnvironmentPrivilege SeImpersonatePrivilege
Security	Audit Success	12292	2015-04-22 18:52:59	Microsoft-Windows-Security-Auditing	5033: The Windows Firewall Driver started successfully.
Security	Audit Success	12292	2015-04-22 18:52:59	Microsoft-Windows-Security-Auditing	5024: The Windows Firewall service started successfully.
Security	Audit Success	12544	2015-04-22 18:52:59	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: LTRANPHD$ Account Domain: WORKGROUP Logon ID: 0x3e7 Logon Type: 5 Impersonation Level: %%1833 New Logon: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Logon ID: 0x3e7 Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x240 Process Name: C:\Windows\System32\services.exe Network Information: Workstation Name: Source Network Address: - Source Port: - Detailed Authentication Information: Logon Process: Advapi Authentication Package: Negotiate Transited Services: - Package Name (NTLM only): - Key Length: 0 This event is generated when a logon session is created. It is generated on the computer that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service such as the Server service, or a local process such as Winlogon.exe or Services.exe. The logon type field indicates the kind of logon that occurred. The most common types are 2 (interactive) and 3 (network). The New Logon fields indicate the account for whom the new logon was created, i.e. the account that was logged on. The network fields indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impersonation level field indicates the extent to which a process in the logon session can impersonate. The authentication information fields provide detailed information about this specific logon request. - Logon GUID is a unique identifier that can be used to correlate this event with a KDC event. - Transited services indicate which intermediate services have participated in this logon request. - Package name indicates

					which sub-protocol was used among the NTLM protocols. - Key length indicates the length of the generated session key. This will be 0 if no session key was requested.
Security	Audit Success	12544	2015-04-22 18:52:59	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: LTRANPHD$ Account Domain: WORKGROUP Logon ID: 0x3e7 Logon Type: 5 Impersonation Level: %%1833 New Logon: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Logon ID: 0x3e7 Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x240 Process Name: C:\Windows\System32\services.exe Network Information: Workstation Name: Source Network Address: - Source Port: - Detailed Authentication Information: Logon Process: Advapi Authentication Package: Negotiate Transited Services: - Package Name (NTLM only): - Key Length: 0 This event is generated when a logon session is created. It is generated on the computer that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service such as the Server service, or a local process such as Winlogon.exe or Services.exe. The logon type field indicates the kind of logon that occurred. The most common types are 2 (interactive) and 3 (network). The New Logon fields indicate the account for whom the new logon was created, i.e. the account that was logged on. The network fields indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impersonation level field indicates the extent to which a process in the logon session can impersonate. The authentication information fields provide detailed information about this specific logon request. - Logon GUID is a unique identifier that can be used to correlate this event with a KDC event. - Transited services indicate which intermediate services have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indicates the length of the generated session key. This will be 0 if no session key was requested.
Security	Audit Success	12544	2015-04-22 18:52:59	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-0-0 Account Name: - Account Domain: - Logon ID: 0x0 Logon Type: 3 Impersonation Level: %%1833 New Logon: Security ID: S-1-5-7 Account Name: ANONYMOUS LOGON Account Domain: NT AUTHORITY Logon ID: 0x14661 Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x0 Process Name: - Network Information: Workstation Name: Source Network Address: - Source Port: - Detailed Authentication Information: Logon Process: NtLmSsp Authentication Package: NTLM Transited Services: - Package Name (NTLM only): NTLM V1 Key Length: 0 This event is generated when a logon session is created. It is generated on the computer that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service such as the Server service, or a local process such as Winlogon.exe or Services.exe. The logon type field indicates the kind of logon that occurred. The most common types are 2 (interactive) and 3 (network). The New Logon fields indicate the account for whom the new logon was created, i.e. the account that was logged on. The network fields indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impersonation level field indicates the extent to which a process in the logon session can impersonate. The authentication information fields provide detailed information about this specific logon request. - Logon GUID is a unique identifier that can be used to correlate this event with a KDC event. - Transited services indicate which intermediate services have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indicates the length of the generated session key. This will be 0 if no session key was requested.
Security	Audit Success	12548	2015-04-22 18:52:59	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Logon ID: 0x3e7 Privileges: SeAssignPrimaryTokenPrivilege SeTcbPrivilege SeSecurityPrivilege SeTakeOwnershipPrivilege SeLoadDriverPrivilege SeBackupPrivilege SeRestorePrivilege SeDebugPrivilege SeAuditPrivilege SeSystemEnvironmentPrivilege SeImpersonatePrivilege
Security	Audit Success	12548	2015-04-22 18:52:59	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Logon ID: 0x3e7 Privileges: SeAssignPrimaryTokenPrivilege SeTcbPrivilege SeSecurityPrivilege SeTakeOwnershipPrivilege SeLoadDriverPrivilege SeBackupPrivilege SeRestorePrivilege SeDebugPrivilege SeAuditPrivilege SeSystemEnvironmentPrivilege SeImpersonatePrivilege
Security	Audit Success	12544	2015-04-22 18:53:00	Microsoft-Windows-Security-Auditing	4648: A logon was attempted using explicit credentials. Subject: Security ID: S-1-5-18 Account Name: LTRANPHD$ Account Domain: WORKGROUP Logon ID: 0x3e7 Logon GUID: {00000000-0000-0000-0000-000000000000} Account Whose Credentials Were Used: Account Name: Liem Account Domain: LTRANPHD Logon GUID: {00000000-0000-0000-0000-000000000000} Target Server: Target Server Name: localhost Additional Information: localhost Process Information: Process ID: 0x208 Process Name: C:\Windows\System32\winlogon.exe Network Information: Network Address: 127.0.0.1 Port: 0 This event is generated when a process attempts to log on an account by explicitly specifying that account's credentials. This most commonly occurs in batch-type configurations such as scheduled tasks, or when using the RUNAS command.
Security	Audit Success	12544	2015-04-22	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: LTRANPHD$ Account Domain: WORKGROUP Logon ID: 0x3e7 Logon Type: 2 Impersonation Level: %%1833 New Logon: Security ID: S-1-5-21-1888849264-3803429180-4108621888-1001 Account Name: Liem Account Domain: LTRANPHD Logon ID: 0x18424 Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x208 Process Name: C:\Windows\System32\winlogon.exe Network Information: Workstation Name: LTRANPHD Source Network Address: 127.0.0.1 Source Port: 0 Detailed Authentication Information: Logon Process: User32 Authentication Package: Negotiate Transited Services: - Package Name (NTLM only): - Key Length: 0 This event is generated when a logon session is created. It is generated on the computer that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service such as the Server service, or a local process such as Winlogon.exe or Services.exe.

			18:53:00		The logon type field indicates the kind of logon that occurred. The most common types are 2 (interactive) and 3 (network). The New Logon fields indicate the account for whom the new logon was created, i.e. the account that was logged on. The network fields indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impersonation level field indicates the extent to which a process in the logon session can impersonate. The authentication information fields provide detailed information about this specific logon request. - Logon GUID is a unique identifier that can be used to correlate this event with a KDC event. - Transited services indicate which intermediate services have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indicates the length of the generated session key. This will be 0 if no session key was requested.
Security	Audit Success	12544	2015-04-22 18:53:00	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: LTRANPHD$ Account Domain: WORKGROUP Logon ID: 0x3e7 Logon Type: 2 Impersonation Level: %%1833 New Logon: Security ID: S-1-5-21-1888849264-3803429180-4108621888-1001 Account Name: Liem Account Domain: LTRANPHD Logon ID: 0x18453 Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x208 Process Name: C:\Windows\System32\winlogon.exe Network Information: Workstation Name: LTRANPHD Source Network Address: 127.0.0.1 Source Port: 0 Detailed Authentication Information: Logon Process: User32 Authentication Package: Negotiate Transited Services: - Package Name (NTLM only): - Key Length: 0 This event is generated when a logon session is created. It is generated on the computer that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service such as the Server service, or a local process such as Winlogon.exe or Services.exe. The logon type field indicates the kind of logon that occurred. The most common types are 2 (interactive) and 3 (network). The New Logon fields indicate the account for whom the new logon was created, i.e. the account that was logged on. The network fields indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impersonation level field indicates the extent to which a process in the logon session can impersonate. The authentication information fields provide detailed information about this specific logon request. - Logon GUID is a unique identifier that can be used to correlate this event with a KDC event. - Transited services indicate which intermediate services have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indicates the length of the generated session key. This will be 0 if no session key was requested.
Security	Audit Success	12548	2015-04-22 18:53:00	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-21-1888849264-3803429180-4108621888-1001 Account Name: Liem Account Domain: LTRANPHD Logon ID: 0x18424 Privileges: SeSecurityPrivilege SeTakeOwnershipPrivilege SeLoadDriverPrivilege SeBackupPrivilege SeRestorePrivilege SeDebugPrivilege SeSystemEnvironmentPrivilege SeImpersonatePrivilege
Security	Audit Success	12544	2015-04-22 18:53:03	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: LTRANPHD$ Account Domain: WORKGROUP Logon ID: 0x3e7 Logon Type: 5 Impersonation Level: %%1833 New Logon: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Logon ID: 0x3e7 Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x240 Process Name: C:\Windows\System32\services.exe Network Information: Workstation Name: Source Network Address: - Source Port: - Detailed Authentication Information: Logon Process: Advapi Authentication Package: Negotiate Transited Services: - Package Name (NTLM only): - Key Length: 0 This event is generated when a logon session is created. It is generated on the computer that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service such as the Server service, or a local process such as Winlogon.exe or Services.exe. The logon type field indicates the kind of logon that occurred. The most common types are 2 (interactive) and 3 (network). The New Logon fields indicate the account for whom the new logon was created, i.e. the account that was logged on. The network fields indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impersonation level field indicates the extent to which a process in the logon session can impersonate. The authentication information fields provide detailed information about this specific logon request. - Logon GUID is a unique identifier that can be used to correlate this event with a KDC event. - Transited services indicate which intermediate services have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indicates the length of the generated session key. This will be 0 if no session key was requested.
Security	Audit Success	12548	2015-04-22 18:53:03	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Logon ID: 0x3e7 Privileges: SeAssignPrimaryTokenPrivilege SeTcbPrivilege SeSecurityPrivilege SeTakeOwnershipPrivilege SeLoadDriverPrivilege SeBackupPrivilege SeRestorePrivilege SeDebugPrivilege SeAuditPrivilege SeSystemEnvironmentPrivilege SeImpersonatePrivilege
Security	Audit Success	13824	2015-04-22 18:53:06	Microsoft-Windows-Security-Auditing	4797: An attempt was made to query the existence of a blank password for an account. Subject: Security ID: S-1-5-21-1888849264-3803429180-4108621888-1001 Account Name: Liem Account Domain: LTRANPHD Logon ID: 0x18453 Additional Information: Caller Workstation: LTRANPHD Target Account Name: Administrator Target Account Domain: LTRANPHD
Security	Audit Success	13824	2015-04-22 18:53:06	Microsoft-Windows-Security-Auditing	4797: An attempt was made to query the existence of a blank password for an account. Subject: Security ID: S-1-5-21-1888849264-3803429180-4108621888-1001 Account Name: Liem Account Domain: LTRANPHD Logon ID: 0x18453 Additional Information: Caller Workstation: LTRANPHD Target Account Name: Guest Target Account Domain: LTRANPHD
Security	Audit Success	13824	2015-04-22	Microsoft-Windows-Security-Auditing	4797: An attempt was made to query the existence of a blank password for an account. Subject: Security ID: S-1-5-21-1888849264-3803429180-4108621888-1001 Account Name: Liem Account Domain: LTRANPHD Logon ID: 0x18453 Additional Information: Caller Workstation: LTRANPHD Target Account Name: Administrator Target

			18:53:06		Account Domain: LTRANPHD
Security	Audit Success	13824	2015-04-22 18:53:06	Microsoft-Windows-Security-Auditing	4797: An attempt was made to query the existence of a blank password for an account. Subject: Security ID: S-1-5-21-1888849264-3803429180-4108621888-1001 Account Name: Liem Account Domain: LTRANPHD Logon ID: 0x18453 Additional Information: Caller Workstation: LTRANPHD Target Account Name: Guest Target Account Domain: LTRANPHD
Security	Audit Success	13824	2015-04-22 18:53:06	Microsoft-Windows-Security-Auditing	4797: An attempt was made to query the existence of a blank password for an account. Subject: Security ID: S-1-5-19 Account Name: LOCAL SERVICE Account Domain: NT AUTHORITY Logon ID: 0x3e5 Additional Information: Caller Workstation: LTRANPHD Target Account Name: Administrator Target Account Domain: LTRANPHD
Security	Audit Success	13824	2015-04-22 18:53:06	Microsoft-Windows-Security-Auditing	4797: An attempt was made to query the existence of a blank password for an account. Subject: Security ID: S-1-5-19 Account Name: LOCAL SERVICE Account Domain: NT AUTHORITY Logon ID: 0x3e5 Additional Information: Caller Workstation: LTRANPHD Target Account Name: Guest Target Account Domain: LTRANPHD
Security	Audit Success	13824	2015-04-22 18:53:06	Microsoft-Windows-Security-Auditing	4797: An attempt was made to query the existence of a blank password for an account. Subject: Security ID: S-1-5-19 Account Name: LOCAL SERVICE Account Domain: NT AUTHORITY Logon ID: 0x3e5 Additional Information: Caller Workstation: LTRANPHD Target Account Name: Liem Target Account Domain: LTRANPHD
Security	Audit Success	13824	2015-04-22 18:53:06	Microsoft-Windows-Security-Auditing	4797: An attempt was made to query the existence of a blank password for an account. Subject: Security ID: S-1-5-19 Account Name: LOCAL SERVICE Account Domain: NT AUTHORITY Logon ID: 0x3e5 Additional Information: Caller Workstation: LTRANPHD Target Account Name: Liem Target Account Domain: LTRANPHD
Security	Audit Success	13824	2015-04-22 18:53:06	Microsoft-Windows-Security-Auditing	4797: An attempt was made to query the existence of a blank password for an account. Subject: Security ID: S-1-5-19 Account Name: LOCAL SERVICE Account Domain: NT AUTHORITY Logon ID: 0x3e5 Additional Information: Caller Workstation: LTRANPHD Target Account Name: Administrator Target Account Domain: LTRANPHD
Security	Audit Success	13824	2015-04-22 18:53:06	Microsoft-Windows-Security-Auditing	4797: An attempt was made to query the existence of a blank password for an account. Subject: Security ID: S-1-5-19 Account Name: LOCAL SERVICE Account Domain: NT AUTHORITY Logon ID: 0x3e5 Additional Information: Caller Workstation: LTRANPHD Target Account Name: Guest Target Account Domain: LTRANPHD
Security	Audit Success	13824	2015-04-22 18:53:06	Microsoft-Windows-Security-Auditing	4797: An attempt was made to query the existence of a blank password for an account. Subject: Security ID: S-1-5-19 Account Name: LOCAL SERVICE Account Domain: NT AUTHORITY Logon ID: 0x3e5 Additional Information: Caller Workstation: LTRANPHD Target Account Name: Liem Target Account Domain: LTRANPHD
Security	Audit Success	13824	2015-04-22 18:53:06	Microsoft-Windows-Security-Auditing	4797: An attempt was made to query the existence of a blank password for an account. Subject: Security ID: S-1-5-19 Account Name: LOCAL SERVICE Account Domain: NT AUTHORITY Logon ID: 0x3e5 Additional Information: Caller Workstation: LTRANPHD Target Account Name: Liem Target Account Domain: LTRANPHD
Security	Audit Success	12544	2015-04-22 18:53:07	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: LTRANPHD$ Account Domain: WORKGROUP Logon ID: 0x3e7 Logon Type: 5 Impersonation Level: %%1833 New Logon: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Logon ID: 0x3e7 Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x240 Process Name: C:\Windows\System32\services.exe Network Information: Workstation Name: Source Network Address: - Source Port: - Detailed Authentication Information: Logon Process: Advapi Authentication Package: Negotiate Transited Services: - Package Name (NTLM only): - Key Length: 0 This event is generated when a logon session is created. It is generated on the computer that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service such as the Server service, or a local process such as Winlogon.exe or Services.exe. The logon type field indicates the kind of logon that occurred. The most common types are 2 (interactive) and 3 (network). The New Logon fields indicate the account for whom the new logon was created, i.e. the account that was logged on. The network fields indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impersonation level field indicates the extent to which a process in the logon session can impersonate. The authentication information fields provide detailed information about this specific logon request. - Logon GUID is a unique identifier that can be used to correlate this event with a KDC event. - Transited services indicate which intermediate services have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indicates the length of the generated session key. This will be 0 if no session key was requested.
Security	Audit Success	12548	2015-04-22 18:53:07	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Logon ID: 0x3e7 Privileges: SeAssignPrimaryTokenPrivilege SeTcbPrivilege SeSecurityPrivilege SeTakeOwnershipPrivilege SeLoadDriverPrivilege SeBackupPrivilege SeRestorePrivilege SeDebugPrivilege SeAuditPrivilege SeSystemEnvironmentPrivilege SeImpersonatePrivilege
Security	Audit Success	12544	2015-04-22	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: LTRANPHD$ Account Domain: WORKGROUP Logon ID: 0x3e7 Logon Type: 5 Impersonation Level: %%1833 New Logon: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Logon ID: 0x3e7 Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x240 Process Name: C:\Windows\System32\services.exe Network Information: Workstation Name: Source Network Address: - Source Port: - Detailed Authentication Information: Logon Process: Advapi Authentication Package: Negotiate Transited Services: - Package Name (NTLM only): - Key Length: 0 This event is generated when a logon session is created. It is generated on the computer that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service such as the Server service, or a local process such as Winlogon.exe or Services.exe. The logon type field indicates the kind of logon that occurred.

			18:56:05		The most common types are 2 (interactive) and 3 (network). The New Logon fields indicate the account for whom the new logon was created, i.e. the account that was logged on. The network fields indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impersonation level field indicates the extent to which a process in the logon session can impersonate. The authentication information fields provide detailed information about this specific logon request. - Logon GUID is a unique identifier that can be used to correlate this event with a KDC event. - Transited services indicate which intermediate services have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indicates the length of the generated session key. This will be 0 if no session key was requested.
Security	Audit Success	12548	2015-04-22 18:56:05	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Logon ID: 0x3e7 Privileges: SeAssignPrimaryTokenPrivilege SeTcbPrivilege SeSecurityPrivilege SeTakeOwnershipPrivilege SeLoadDriverPrivilege SeBackupPrivilege SeRestorePrivilege SeDebugPrivilege SeAuditPrivilege SeSystemEnvironmentPrivilege SeImpersonatePrivilege
Security	Audit Success	13824	2015-04-22 19:00:02	Microsoft-Windows-Security-Auditing	4797: An attempt was made to query the existence of a blank password for an account. Subject: Security ID: S-1-5-21-1888849264-3803429180-4108621888-1001 Account Name: Liem Account Domain: LTRANPHD Logon ID: 0x18453 Additional Information: Caller Workstation: LTRANPHD Target Account Name: Administrator Target Account Domain: LTRANPHD
Security	Audit Success	13824	2015-04-22 19:00:02	Microsoft-Windows-Security-Auditing	4797: An attempt was made to query the existence of a blank password for an account. Subject: Security ID: S-1-5-21-1888849264-3803429180-4108621888-1001 Account Name: Liem Account Domain: LTRANPHD Logon ID: 0x18453 Additional Information: Caller Workstation: LTRANPHD Target Account Name: Guest Target Account Domain: LTRANPHD
Security	Audit Success	13824	2015-04-22 19:00:02	Microsoft-Windows-Security-Auditing	4797: An attempt was made to query the existence of a blank password for an account. Subject: Security ID: S-1-5-21-1888849264-3803429180-4108621888-1001 Account Name: Liem Account Domain: LTRANPHD Logon ID: 0x18453 Additional Information: Caller Workstation: LTRANPHD Target Account Name: Administrator Target Account Domain: LTRANPHD
Security	Audit Success	13824	2015-04-22 19:00:02	Microsoft-Windows-Security-Auditing	4797: An attempt was made to query the existence of a blank password for an account. Subject: Security ID: S-1-5-21-1888849264-3803429180-4108621888-1001 Account Name: Liem Account Domain: LTRANPHD Logon ID: 0x18453 Additional Information: Caller Workstation: LTRANPHD Target Account Name: Guest Target Account Domain: LTRANPHD
Security	Audit Success	13824	2015-04-22 19:00:07	Microsoft-Windows-Security-Auditing	4797: An attempt was made to query the existence of a blank password for an account. Subject: Security ID: S-1-5-21-1888849264-3803429180-4108621888-1001 Account Name: Liem Account Domain: LTRANPHD Logon ID: 0x18453 Additional Information: Caller Workstation: LTRANPHD Target Account Name: Administrator Target Account Domain: LTRANPHD
Security	Audit Success	13824	2015-04-22 19:00:07	Microsoft-Windows-Security-Auditing	4797: An attempt was made to query the existence of a blank password for an account. Subject: Security ID: S-1-5-21-1888849264-3803429180-4108621888-1001 Account Name: Liem Account Domain: LTRANPHD Logon ID: 0x18453 Additional Information: Caller Workstation: LTRANPHD Target Account Name: Guest Target Account Domain: LTRANPHD
Security	Audit Success	13824	2015-04-22 19:00:12	Microsoft-Windows-Security-Auditing	4797: An attempt was made to query the existence of a blank password for an account. Subject: Security ID: S-1-5-21-1888849264-3803429180-4108621888-1001 Account Name: Liem Account Domain: LTRANPHD Logon ID: 0x18453 Additional Information: Caller Workstation: LTRANPHD Target Account Name: Guest Target Account Domain: LTRANPHD
Security	Audit Success	12544	2015-04-22 19:00:28	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: LTRANPHD$ Account Domain: WORKGROUP Logon ID: 0x3e7 Logon Type: 5 Impersonation Level: %%1833 New Logon: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Logon ID: 0x3e7 Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x240 Process Name: C:\Windows\System32\services.exe Network Information: Workstation Name: Source Network Address: - Source Port: - Detailed Authentication Information: Logon Process: Advapi Authentication Package: Negotiate Transited Services: - Package Name (NTLM only): - Key Length: 0 This event is generated when a logon session is created. It is generated on the computer that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service such as the Server service, or a local process such as Winlogon.exe or Services.exe. The logon type field indicates the kind of logon that occurred. The most common types are 2 (interactive) and 3 (network). The New Logon fields indicate the account for whom the new logon was created, i.e. the account that was logged on. The network fields indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impersonation level field indicates the extent to which a process in the logon session can impersonate. The authentication information fields provide detailed information about this specific logon request. - Logon GUID is a unique identifier that can be used to correlate this event with a KDC event. - Transited services indicate which intermediate services have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indicates the length of the generated session key. This will be 0 if no session key was requested.
Security	Audit Success	12548	2015-04-22 19:00:28	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Logon ID: 0x3e7 Privileges: SeAssignPrimaryTokenPrivilege SeTcbPrivilege SeSecurityPrivilege SeTakeOwnershipPrivilege SeLoadDriverPrivilege SeBackupPrivilege SeRestorePrivilege SeDebugPrivilege SeAuditPrivilege SeSystemEnvironmentPrivilege SeImpersonatePrivilege
					4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: LTRANPHD$

Security	Audit Success	12544	2015-04-22 19:02:00	Microsoft-Windows-Security-Auditing	Account Domain: WORKGROUP Logon ID: 0x3e7 Logon Type: 5 Impersonation Level: %%1833 New Logon: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Logon ID: 0x3e7 Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x240 Process Name: C:\Windows\System32\services.exe Network Information: Workstation Name: Source Network Address: - Source Port: - Detailed Authentication Information: Logon Process: Advapi Authentication Package: Negotiate Transited Services: - Package Name (NTLM only): - Key Length: 0 This event is generated when a logon session is created. It is generated on the computer that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service such as the Server service, or a local process such as Winlogon.exe or Services.exe. The logon type field indicates the kind of logon that occurred. The most common types are 2 (interactive) and 3 (network). The New Logon fields indicate the account for whom the new logon was created, i.e. the account that was logged on. The network fields indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impersonation level field indicates the extent to which a process in the logon session can impersonate. The authentication information fields provide detailed information about this specific logon request. - Logon GUID is a unique identifier that can be used to correlate this event with a KDC event. - Transited services indicate which intermediate services have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indicates the length of the generated session key. This will be 0 if no session key was requested.
Security	Audit Success	12544	2015-04-22 19:02:00	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: LTRANPHD$ Account Domain: WORKGROUP Logon ID: 0x3e7 Logon Type: 5 Impersonation Level: %%1833 New Logon: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Logon ID: 0x3e7 Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x240 Process Name: C:\Windows\System32\services.exe Network Information: Workstation Name: Source Network Address: - Source Port: - Detailed Authentication Information: Logon Process: Advapi Authentication Package: Negotiate Transited Services: - Package Name (NTLM only): - Key Length: 0 This event is generated when a logon session is created. It is generated on the computer that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service such as the Server service, or a local process such as Winlogon.exe or Services.exe. The logon type field indicates the kind of logon that occurred. The most common types are 2 (interactive) and 3 (network). The New Logon fields indicate the account for whom the new logon was created, i.e. the account that was logged on. The network fields indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impersonation level field indicates the extent to which a process in the logon session can impersonate. The authentication information fields provide detailed information about this specific logon request. - Logon GUID is a unique identifier that can be used to correlate this event with a KDC event. - Transited services indicate which intermediate services have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indicates the length of the generated session key. This will be 0 if no session key was requested.
Security	Audit Success	12548	2015-04-22 19:02:00	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Logon ID: 0x3e7 Privileges: SeAssignPrimaryTokenPrivilege SeTcbPrivilege SeSecurityPrivilege SeTakeOwnershipPrivilege SeLoadDriverPrivilege SeBackupPrivilege SeRestorePrivilege SeDebugPrivilege SeAuditPrivilege SeSystemEnvironmentPrivilege SeImpersonatePrivilege
Security	Audit Success	12548	2015-04-22 19:02:00	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Logon ID: 0x3e7 Privileges: SeAssignPrimaryTokenPrivilege SeTcbPrivilege SeSecurityPrivilege SeTakeOwnershipPrivilege SeLoadDriverPrivilege SeBackupPrivilege SeRestorePrivilege SeDebugPrivilege SeAuditPrivilege SeSystemEnvironmentPrivilege SeImpersonatePrivilege
Security	Audit Success	12544	2015-04-22 19:03:39	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: LTRANPHD$ Account Domain: WORKGROUP Logon ID: 0x3e7 Logon Type: 5 Impersonation Level: %%1833 New Logon: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Logon ID: 0x3e7 Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x240 Process Name: C:\Windows\System32\services.exe Network Information: Workstation Name: Source Network Address: - Source Port: - Detailed Authentication Information: Logon Process: Advapi Authentication Package: Negotiate Transited Services: - Package Name (NTLM only): - Key Length: 0 This event is generated when a logon session is created. It is generated on the computer that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service such as the Server service, or a local process such as Winlogon.exe or Services.exe. The logon type field indicates the kind of logon that occurred. The most common types are 2 (interactive) and 3 (network). The New Logon fields indicate the account for whom the new logon was created, i.e. the account that was logged on. The network fields indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impersonation level field indicates the extent to which a process in the logon session can impersonate. The authentication information fields provide detailed information about this specific logon request. - Logon GUID is a unique identifier that can be used to correlate this event with a KDC event. - Transited services indicate which intermediate services have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indicates the length of the generated session key. This will be 0 if no session key was requested.
Security	Audit	12548	2015-04-22	Microsoft-Windows-Security-	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Logon ID: 0x3e7 Privileges: SeAssignPrimaryTokenPrivilege SeTcbPrivilege

	Success		19:03:39	Auditing	SeSecurityPrivilege SeTakeOwnershipPrivilege SeLoadDriverPrivilege SeBackupPrivilege SeRestorePrivilege SeDebugPrivilege SeAuditPrivilege SeSystemEnvironmentPrivilege SeImpersonatePrivilege
Security	Audit Success	13568	2015-04-22 19:03:46	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: LTRANPHD$ Account Domain: WORKGROUP Logon ID: 0x3e7 Object: Object Server: Security Object Type: File Object Name: C:\Windows\WinSxS\FileMaps_0000000000000000.cdf-ms Handle ID: 0x67c Process Information: Process ID: 0xf34 Process Name: C:\Windows\WinSxS\amd64_microsoft-windows-servicingstack_31bf3856ad364e35_6.3.9600.17477_none_fa2b7d3b9b36c7b4\TiWorker.exe Auditing Settings: Original Security Descriptor: New Security Descriptor: S:ARAI(AU;SAFA;0x1f0116;;;WD)
Security	Audit Success	13568	2015-04-22 19:03:46	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: LTRANPHD$ Account Domain: WORKGROUP Logon ID: 0x3e7 Object: Object Server: Security Object Type: File Object Name: C:\Windows\WinSxS\FileMaps\$$.cdf-ms Handle ID: 0x4cc Process Information: Process ID: 0xf34 Process Name: C:\Windows\WinSxS\amd64_microsoft-windows-servicingstack_31bf3856ad364e35_6.3.9600.17477_none_fa2b7d3b9b36c7b4\TiWorker.exe Auditing Settings: Original Security Descriptor: New Security Descriptor: S:ARAI(AU;SAFA;0x1f0116;;;WD)
Security	Audit Success	13568	2015-04-22 19:03:46	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: LTRANPHD$ Account Domain: WORKGROUP Logon ID: 0x3e7 Object: Object Server: Security Object Type: File Object Name: C:\Windows\WinSxS\FileMaps\$$_system32_21f9a9c4a2f8b514.cdf-ms Handle ID: 0x5d8 Process Information: Process ID: 0xf34 Process Name: C:\Windows\WinSxS\amd64_microsoft-windows-servicingstack_31bf3856ad364e35_6.3.9600.17477_none_fa2b7d3b9b36c7b4\TiWorker.exe Auditing Settings: Original Security Descriptor: New Security Descriptor: S:ARAI(AU;SAFA;0x1f0116;;;WD)
Security	Audit Success	13568	2015-04-22 19:03:46	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: LTRANPHD$ Account Domain: WORKGROUP Logon ID: 0x3e7 Object: Object Server: Security Object Type: File Object Name: C:\Windows\WinSxS\FileMaps\$$_system32_en-us_429cd25484dc6f94.cdf-ms Handle ID: 0x670 Process Information: Process ID: 0xf34 Process Name: C:\Windows\WinSxS\amd64_microsoft-windows-servicingstack_31bf3856ad364e35_6.3.9600.17477_none_fa2b7d3b9b36c7b4\TiWorker.exe Auditing Settings: Original Security Descriptor: New Security Descriptor: S:ARAI(AU;SAFA;0x1f0116;;;WD)
Security	Audit Success	13568	2015-04-22 19:03:46	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: LTRANPHD$ Account Domain: WORKGROUP Logon ID: 0x3e7 Object: Object Server: Security Object Type: File Object Name: C:\Windows\WinSxS\FileMaps\programdata.cdf-ms Handle ID: 0x46c Process Information: Process ID: 0xf34 Process Name: C:\Windows\WinSxS\amd64_microsoft-windows-servicingstack_31bf3856ad364e35_6.3.9600.17477_none_fa2b7d3b9b36c7b4\TiWorker.exe Auditing Settings: Original Security Descriptor: New Security Descriptor: S:ARAI(AU;SAFA;0x1f0116;;;WD)
Security	Audit Success	13568	2015-04-22 19:03:46	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: LTRANPHD$ Account Domain: WORKGROUP Logon ID: 0x3e7 Object: Object Server: Security Object Type: File Object Name: C:\Windows\WinSxS\FileMaps\programdata_microsoft_fe5c6d762edd2110.cdf-ms Handle ID: 0x6c4 Process Information: Process ID: 0xf34 Process Name: C:\Windows\WinSxS\amd64_microsoft-windows-servicingstack_31bf3856ad364e35_6.3.9600.17477_none_fa2b7d3b9b36c7b4\TiWorker.exe Auditing Settings: Original Security Descriptor: New Security Descriptor: S:ARAI(AU;SAFA;0x1f0116;;;WD)
Security	Audit Success	13568	2015-04-22 19:03:46	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: LTRANPHD$ Account Domain: WORKGROUP Logon ID: 0x3e7 Object: Object Server: Security Object Type: File Object Name: C:\Windows\WinSxS\FileMaps\programdata_microsoft_diagnosis_af2ddc54e6a8e491.cdf-ms Handle ID: 0x670 Process Information: Process ID: 0xf34 Process Name: C:\Windows\WinSxS\amd64_microsoft-windows-servicingstack_31bf3856ad364e35_6.3.9600.17477_none_fa2b7d3b9b36c7b4\TiWorker.exe Auditing Settings: Original Security Descriptor: New Security Descriptor: S:ARAI(AU;SAFA;0x1f0116;;;WD)
Security	Audit Success	13568	2015-04-22 19:03:46	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: LTRANPHD$ Account Domain: WORKGROUP Logon ID: 0x3e7 Object: Object Server: Security Object Type: File Object Name: C:\Windows\WinSxS\FileMaps\programdata_microsoft_diagnosis_sideload_1bd7d65b4945242a.cdf-ms Handle ID: 0x46c Process Information: Process ID: 0xf34 Process Name: C:\Windows\WinSxS\amd64_microsoft-windows-servicingstack_31bf3856ad364e35_6.3.9600.17477_none_fa2b7d3b9b36c7b4\TiWorker.exe Auditing Settings: Original Security Descriptor: New Security Descriptor: S:ARAI(AU;SAFA;0x1f0116;;;WD)
Security	Audit Success	13568	2015-04-22 19:03:46	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: LTRANPHD$ Account Domain: WORKGROUP Logon ID: 0x3e7 Object: Object Server: Security Object Type: File Object Name: C:\Windows\WinSxS\FileMaps\programdata_microsoft_diagnosis_downloadedsettings_f4a4d355cda0ca19.cdf-ms Handle ID: 0x45c Process Information: Process ID: 0xf34 Process Name: C:\Windows\WinSxS\amd64_microsoft-windows-servicingstack_31bf3856ad364e35_6.3.9600.17477_none_fa2b7d3b9b36c7b4\TiWorker.exe Auditing Settings: Original Security Descriptor: New Security Descriptor: S:ARAI(AU;SAFA;0x1f0116;;;WD)
Security	Audit Success	13568	2015-04-22 19:03:46	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: LTRANPHD$ Account Domain: WORKGROUP Logon ID: 0x3e7 Object: Object Server: Security Object Type: File Object Name: C:\Windows\WinSxS\FileMaps\programdata_microsoft_diagnosis_asimovuploader_0413bca0c3dfdda4.cdf-ms Handle ID: 0x36c Process Information: Process ID: 0xf34 Process Name: C:\Windows\WinSxS\amd64_microsoft-windows-servicingstack_31bf3856ad364e35_6.3.9600.17477_none_fa2b7d3b9b36c7b4\TiWorker.exe Auditing Settings:

					Original Security Descriptor: New Security Descriptor: S:ARAI(AU;SAFA;0x1f0116;;;WD)
Security	Audit Success	13568	2015-04-22 19:03:46	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: LTRANPHD$ Account Domain: WORKGROUP Logon ID: 0x3e7 Object: Object Server: Security Object Type: File Object Name: C:\Windows\WinSxS\FileMaps\programdata_microsoft_diagnosis_uif_f8dfdef9a82062a1.cdf-ms Handle ID: 0x2c0 Process Information: Process ID: 0xf34 Process Name: C:\Windows\WinSxS\amd64_microsoft-windows-servicingstack_31bf3856ad364e35_6.3.9600.17477_none_fa2b7d3b9b36c7b4\TiWorker.exe Auditing Settings: Original Security Descriptor: New Security Descriptor: S:ARAI(AU;SAFA;0x1f0116;;;WD)
Security	Audit Success	13568	2015-04-22 19:03:46	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: LTRANPHD$ Account Domain: WORKGROUP Logon ID: 0x3e7 Object: Object Server: Security Object Type: File Object Name: C:\Windows\WinSxS\FileMaps\programdata_microsoft_diagnosis_localtracestore_b69b398684e58a86.cdf-ms Handle ID: 0x48c Process Information: Process ID: 0xf34 Process Name: C:\Windows\WinSxS\amd64_microsoft-windows-servicingstack_31bf3856ad364e35_6.3.9600.17477_none_fa2b7d3b9b36c7b4\TiWorker.exe Auditing Settings: Original Security Descriptor: New Security Descriptor: S:ARAI(AU;SAFA;0x1f0116;;;WD)
Security	Audit Success	13568	2015-04-22 19:03:46	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: LTRANPHD$ Account Domain: WORKGROUP Logon ID: 0x3e7 Object: Object Server: Security Object Type: File Object Name: C:\Windows\WinSxS\FileMaps\programdata_microsoft_diagnosis_etllogs_ffc0f561f3797ceb.cdf-ms Handle ID: 0x36c Process Information: Process ID: 0xf34 Process Name: C:\Windows\WinSxS\amd64_microsoft-windows-servicingstack_31bf3856ad364e35_6.3.9600.17477_none_fa2b7d3b9b36c7b4\TiWorker.exe Auditing Settings: Original Security Descriptor: New Security Descriptor: S:ARAI(AU;SAFA;0x1f0116;;;WD)
Security	Audit Success	13568	2015-04-22 19:03:46	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: LTRANPHD$ Account Domain: WORKGROUP Logon ID: 0x3e7 Object: Object Server: Security Object Type: File Object Name: C:\Windows\WinSxS\FileMaps\programdata_microsoft_diagnosis_etllogs_shutdownlogger_5ca7b57d60632f51.cdf-ms Handle ID: 0x2c0 Process Information: Process ID: 0xf34 Process Name: C:\Windows\WinSxS\amd64_microsoft-windows-servicingstack_31bf3856ad364e35_6.3.9600.17477_none_fa2b7d3b9b36c7b4\TiWorker.exe Auditing Settings: Original Security Descriptor: New Security Descriptor: S:ARAI(AU;SAFA;0x1f0116;;;WD)
Security	Audit Success	13568	2015-04-22 19:03:46	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: LTRANPHD$ Account Domain: WORKGROUP Logon ID: 0x3e7 Object: Object Server: Security Object Type: File Object Name: C:\Windows\WinSxS\FileMaps\programdata_microsoft_diagnosis_etllogs_autologger_91adf7c94bd2d1fa.cdf-ms Handle ID: 0x48c Process Information: Process ID: 0xf34 Process Name: C:\Windows\WinSxS\amd64_microsoft-windows-servicingstack_31bf3856ad364e35_6.3.9600.17477_none_fa2b7d3b9b36c7b4\TiWorker.exe Auditing Settings: Original Security Descriptor: New Security Descriptor: S:ARAI(AU;SAFA;0x1f0116;;;WD)
Security	Audit Success	13568	2015-04-22 19:03:46	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: LTRANPHD$ Account Domain: WORKGROUP Logon ID: 0x3e7 Object: Object Server: Security Object Type: File Object Name: C:\Windows\System32\diagtrack.dll Handle ID: 0x364 Process Information: Process ID: 0xf34 Process Name: C:\Windows\WinSxS\amd64_microsoft-windows-servicingstack_31bf3856ad364e35_6.3.9600.17477_none_fa2b7d3b9b36c7b4\TiWorker.exe Auditing Settings: Original Security Descriptor: S:AI New Security Descriptor: S:ARAI(AU;SAFA;DCLCRPCRSDWDWO;;;WD)
Security	Audit Success	13568	2015-04-22 19:03:46	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: LTRANPHD$ Account Domain: WORKGROUP Logon ID: 0x3e7 Object: Object Server: Security Object Type: File Object Name: C:\Windows\System32\en-US\diagtrack.dll.mui Handle ID: 0x36c Process Information: Process ID: 0xf34 Process Name: C:\Windows\WinSxS\amd64_microsoft-windows-servicingstack_31bf3856ad364e35_6.3.9600.17477_none_fa2b7d3b9b36c7b4\TiWorker.exe Auditing Settings: Original Security Descriptor: S:AI New Security Descriptor: S:ARAI(AU;SAFA;DCLCRPCRSDWDWO;;;WD)
Security	Audit Success	13568	2015-04-22 19:03:50	Microsoft-Windows-Security-Auditing	4904: An attempt was made to register a security event source. Subject : Security ID: S-1-5-18 Account Name: LTRANPHD$ Account Domain: WORKGROUP Logon ID: 0x3e7 Process: Process ID: 0x828 Process Name: C:\Windows\System32\VSSVC.exe Event Source: Source Name: VSSAudit Event Source ID: 0x65aa3c
Security	Audit Success	13568	2015-04-22 19:03:50	Microsoft-Windows-Security-Auditing	4905: An attempt was made to unregister a security event source. Subject Security ID: S-1-5-18 Account Name: LTRANPHD$ Account Domain: WORKGROUP Logon ID: 0x3e7 Process: Process ID: 0x828 Process Name: C:\Windows\System32\VSSVC.exe Event Source: Source Name: VSSAudit Event Source ID: 0x65aa3c
Security	Audit Success	13568	2015-04-22 19:03:51	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: LTRANPHD$ Account Domain: WORKGROUP Logon ID: 0x3e7 Object: Object Server: Security Object Type: File Object Name: C:\Windows\WinSxS\FileMaps_00000000000000000.cdf-ms Handle ID: 0x208 Process Information: Process ID: 0xf34 Process Name: C:\Windows\WinSxS\amd64_microsoft-windows-servicingstack_31bf3856ad364e35_6.3.9600.17477_none_fa2b7d3b9b36c7b4\TiWorker.exe Auditing Settings: Original Security Descriptor: New Security Descriptor: S:ARAI(AU;SAFA;0x1f0116;;;WD)
Security	Audit Success	13568	2015-04-22 19:03:51	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: LTRANPHD$ Account Domain: WORKGROUP Logon ID: 0x3e7 Object: Object Server: Security Object Type: File Object Name: C:\Windows\WinSxS\FileMaps\$$.cdf-ms Handle ID: 0x364 Process Information: Process ID: 0xf34 Process Name: C:\Windows\WinSxS\amd64_microsoft-windows-servicingstack_31bf3856ad364e35_6.3.9600.17477_none_fa2b7d3b9b36c7b4\TiWorker.exe Auditing Settings:

					Original Security Descriptor: New Security Descriptor: S:ARAI(AU;SAFA;0x1f0116;;;WD)
Security	Audit Success	13568	2015-04-22 19:03:51	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: LTRANPHD$ Account Domain: WORKGROUP Logon ID: 0x3e7 Object: Object Server: Security Object Type: File Object Name: C:\Windows\WinSxS\FileMaps\$$_syswow64_21ffbdd2a2dd92e0.cdf-ms Handle ID: 0x364 Process Information: Process ID: 0xf34 Process Name: C:\Windows\WinSxS\amd64_microsoft-windows-servicingstack_31bf3856ad364e35_6.3.9600.17477_none_fa2b7d3b9b36c7b4\TiWorker.exe Auditing Settings: Original Security Descriptor: New Security Descriptor: S:ARAI(AU;SAFA;0x1f0116;;;WD)
Security	Audit Success	13568	2015-04-22 19:03:51	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: LTRANPHD$ Account Domain: WORKGROUP Logon ID: 0x3e7 Object: Object Server: Security Object Type: File Object Name: C:\Windows\WinSxS\FileMaps\$$_system32_21f9a9c4a2f8b514.cdf-ms Handle ID: 0x358 Process Information: Process ID: 0xf34 Process Name: C:\Windows\WinSxS\amd64_microsoft-windows-servicingstack_31bf3856ad364e35_6.3.9600.17477_none_fa2b7d3b9b36c7b4\TiWorker.exe Auditing Settings: Original Security Descriptor: New Security Descriptor: S:ARAI(AU;SAFA;0x1f0116;;;WD)
Security	Audit Success	13568	2015-04-22 19:03:51	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: LTRANPHD$ Account Domain: WORKGROUP Logon ID: 0x3e7 Object: Object Server: Security Object Type: File Object Name: C:\Windows\System32\wpdshext.dll Handle ID: 0x208 Process Information: Process ID: 0xf34 Process Name: C:\Windows\WinSxS\amd64_microsoft-windows-servicingstack_31bf3856ad364e35_6.3.9600.17477_none_fa2b7d3b9b36c7b4\TiWorker.exe Auditing Settings: Original Security Descriptor: S:AI New Security Descriptor: S:ARAI(AU;SAFA;DCLCRPCRSDWDWO;;;WD)
Security	Audit Success	13568	2015-04-22 19:03:51	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: LTRANPHD$ Account Domain: WORKGROUP Logon ID: 0x3e7 Object: Object Server: Security Object Type: File Object Name: C:\Windows\SysWOW64\wpdshext.dll Handle ID: 0x364 Process Information: Process ID: 0xf34 Process Name: C:\Windows\WinSxS\amd64_microsoft-windows-servicingstack_31bf3856ad364e35_6.3.9600.17477_none_fa2b7d3b9b36c7b4\TiWorker.exe Auditing Settings: Original Security Descriptor: S:AI New Security Descriptor: S:ARAI(AU;SAFA;DCLCRPCRSDWDWO;;;WD)
Security	Audit Success	13568	2015-04-22 19:03:53	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: LTRANPHD$ Account Domain: WORKGROUP Logon ID: 0x3e7 Object: Object Server: Security Object Type: File Object Name: C:\Windows\WinSxS\FileMaps_0000000000000000.cdf-ms Handle ID: 0x5ac Process Information: Process ID: 0xf34 Process Name: C:\Windows\WinSxS\amd64_microsoft-windows-servicingstack_31bf3856ad364e35_6.3.9600.17477_none_fa2b7d3b9b36c7b4\TiWorker.exe Auditing Settings: Original Security Descriptor: New Security Descriptor: S:ARAI(AU;SAFA;0x1f0116;;;WD)
Security	Audit Success	13568	2015-04-22 19:03:53	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: LTRANPHD$ Account Domain: WORKGROUP Logon ID: 0x3e7 Object: Object Server: Security Object Type: File Object Name: C:\Windows\WinSxS\FileMaps\$$.cdf-ms Handle ID: 0x5c0 Process Information: Process ID: 0xf34 Process Name: C:\Windows\WinSxS\amd64_microsoft-windows-servicingstack_31bf3856ad364e35_6.3.9600.17477_none_fa2b7d3b9b36c7b4\TiWorker.exe Auditing Settings: Original Security Descriptor: New Security Descriptor: S:ARAI(AU;SAFA;0x1f0116;;;WD)
Security	Audit Success	13568	2015-04-22 19:03:53	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: LTRANPHD$ Account Domain: WORKGROUP Logon ID: 0x3e7 Object: Object Server: Security Object Type: File Object Name: C:\Windows\WinSxS\FileMaps\$$_syswow64_21ffbdd2a2dd92e0.cdf-ms Handle ID: 0x7c8 Process Information: Process ID: 0xf34 Process Name: C:\Windows\WinSxS\amd64_microsoft-windows-servicingstack_31bf3856ad364e35_6.3.9600.17477_none_fa2b7d3b9b36c7b4\TiWorker.exe Auditing Settings: Original Security Descriptor: New Security Descriptor: S:ARAI(AU;SAFA;0x1f0116;;;WD)
Security	Audit Success	13568	2015-04-22 19:03:53	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: LTRANPHD$ Account Domain: WORKGROUP Logon ID: 0x3e7 Object: Object Server: Security Object Type: File Object Name: C:\Windows\WinSxS\FileMaps\$$_system32_21f9a9c4a2f8b514.cdf-ms Handle ID: 0x538 Process Information: Process ID: 0xf34 Process Name: C:\Windows\WinSxS\amd64_microsoft-windows-servicingstack_31bf3856ad364e35_6.3.9600.17477_none_fa2b7d3b9b36c7b4\TiWorker.exe Auditing Settings: Original Security Descriptor: New Security Descriptor: S:ARAI(AU;SAFA;0x1f0116;;;WD)
Security	Audit Success	13568	2015-04-22 19:03:57	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: LTRANPHD$ Account Domain: WORKGROUP Logon ID: 0x3e7 Object: Object Server: Security Object Type: File Object Name: C:\Windows\WinSxS\FileMaps_0000000000000000.cdf-ms Handle ID: 0x54c Process Information: Process ID: 0xf34 Process Name: C:\Windows\WinSxS\amd64_microsoft-windows-servicingstack_31bf3856ad364e35_6.3.9600.17477_none_fa2b7d3b9b36c7b4\TiWorker.exe Auditing Settings: Original Security Descriptor: New Security Descriptor: S:ARAI(AU;SAFA;0x1f0116;;;WD)
Security	Audit Success	13568	2015-04-22 19:03:57	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: LTRANPHD$ Account Domain: WORKGROUP Logon ID: 0x3e7 Object: Object Server: Security Object Type: File Object Name: C:\Windows\WinSxS\FileMaps\$$.cdf-ms Handle ID: 0x3b4 Process Information: Process ID: 0xf34 Process Name: C:\Windows\WinSxS\amd64_microsoft-windows-servicingstack_31bf3856ad364e35_6.3.9600.17477_none_fa2b7d3b9b36c7b4\TiWorker.exe Auditing Settings: Original Security Descriptor: New Security Descriptor: S:ARAI(AU;SAFA;0x1f0116;;;WD)
Security	Audit Success	13568	2015-04-22	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: LTRANPHD$ Account Domain: WORKGROUP Logon ID: 0x3e7 Object: Object Server: Security Object Type: File Object Name: C:\Windows\WinSxS\FileMaps\$$_system32_21f9a9c4a2f8b514.cdf-ms Handle ID: 0x688 Process Information: Process ID: 0xf34 Process Name: C:\Windows\WinSxS\amd64_microsoft-windows-

			19:03:57		servicingstack_31bf3856ad364e35_6.3.9600.17477_none_fa2b7d3b9b36c7b4\TiWorker.exe Auditing Settings: Original Security Descriptor: New Security Descriptor: S:ARAI(AU;SAFA;0x1f0116;;;WD)
Security	Audit Success	13568	2015-04-22 19:03:58	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: LTRANPHD$ Account Domain: WORKGROUP Logon ID: 0x3e7 Object: Object Server: Security Object Type: File Object Name: C:\Windows\WinSxS\FileMaps_0000000000000000.cdf-ms Handle ID: 0x7a0 Process Information: Process ID: 0xf34 Process Name: C:\Windows\WinSxS\amd64_microsoft-windows-servicingstack_31bf3856ad364e35_6.3.9600.17477_none_fa2b7d3b9b36c7b4\TiWorker.exe Auditing Settings: Original Security Descriptor: New Security Descriptor: S:ARAI(AU;SAFA;0x1f0116;;;WD)
Security	Audit Success	13568	2015-04-22 19:03:58	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: LTRANPHD$ Account Domain: WORKGROUP Logon ID: 0x3e7 Object: Object Server: Security Object Type: File Object Name: C:\Windows\WinSxS\FileMaps\$$.cdf-ms Handle ID: 0x520 Process Information: Process ID: 0xf34 Process Name: C:\Windows\WinSxS\amd64_microsoft-windows-servicingstack_31bf3856ad364e35_6.3.9600.17477_none_fa2b7d3b9b36c7b4\TiWorker.exe Auditing Settings: Original Security Descriptor: New Security Descriptor: S:ARAI(AU;SAFA;0x1f0116;;;WD)
Security	Audit Success	13568	2015-04-22 19:03:58	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: LTRANPHD$ Account Domain: WORKGROUP Logon ID: 0x3e7 Object: Object Server: Security Object Type: File Object Name: C:\Windows\WinSxS\FileMaps\$$_syswow64_21ffbdd2a2dd92e0.cdf-ms Handle ID: 0x520 Process Information: Process ID: 0xf34 Process Name: C:\Windows\WinSxS\amd64_microsoft-windows-servicingstack_31bf3856ad364e35_6.3.9600.17477_none_fa2b7d3b9b36c7b4\TiWorker.exe Auditing Settings: Original Security Descriptor: New Security Descriptor: S:ARAI(AU;SAFA;0x1f0116;;;WD)
Security	Audit Success	13568	2015-04-22 19:03:58	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: LTRANPHD$ Account Domain: WORKGROUP Logon ID: 0x3e7 Object: Object Server: Security Object Type: File Object Name: C:\Windows\WinSxS\FileMaps\$$_system32_21f9a9c4a2f8b514.cdf-ms Handle ID: 0x520 Process Information: Process ID: 0xf34 Process Name: C:\Windows\WinSxS\amd64_microsoft-windows-servicingstack_31bf3856ad364e35_6.3.9600.17477_none_fa2b7d3b9b36c7b4\TiWorker.exe Auditing Settings: Original Security Descriptor: New Security Descriptor: S:ARAI(AU;SAFA;0x1f0116;;;WD)
Security	Audit Success	13568	2015-04-22 19:04:12	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: LTRANPHD$ Account Domain: WORKGROUP Logon ID: 0x3e7 Object: Object Server: Security Object Type: File Object Name: C:\Windows\WinSxS\FileMaps_0000000000000000.cdf-ms Handle ID: 0x764 Process Information: Process ID: 0xf34 Process Name: C:\Windows\WinSxS\amd64_microsoft-windows-servicingstack_31bf3856ad364e35_6.3.9600.17477_none_fa2b7d3b9b36c7b4\TiWorker.exe Auditing Settings: Original Security Descriptor: New Security Descriptor: S:ARAI(AU;SAFA;0x1f0116;;;WD)
Security	Audit Success	13568	2015-04-22 19:04:12	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: LTRANPHD$ Account Domain: WORKGROUP Logon ID: 0x3e7 Object: Object Server: Security Object Type: File Object Name: C:\Windows\WinSxS\FileMaps\$$.cdf-ms Handle ID: 0x700 Process Information: Process ID: 0xf34 Process Name: C:\Windows\WinSxS\amd64_microsoft-windows-servicingstack_31bf3856ad364e35_6.3.9600.17477_none_fa2b7d3b9b36c7b4\TiWorker.exe Auditing Settings: Original Security Descriptor: New Security Descriptor: S:ARAI(AU;SAFA;0x1f0116;;;WD)
Security	Audit Success	13568	2015-04-22 19:04:12	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: LTRANPHD$ Account Domain: WORKGROUP Logon ID: 0x3e7 Object: Object Server: Security Object Type: File Object Name: C:\Windows\WinSxS\FileMaps\$$_syswow64_21ffbdd2a2dd92e0.cdf-ms Handle ID: 0x4bc Process Information: Process ID: 0xf34 Process Name: C:\Windows\WinSxS\amd64_microsoft-windows-servicingstack_31bf3856ad364e35_6.3.9600.17477_none_fa2b7d3b9b36c7b4\TiWorker.exe Auditing Settings: Original Security Descriptor: New Security Descriptor: S:ARAI(AU;SAFA;0x1f0116;;;WD)
Security	Audit Success	13568	2015-04-22 19:04:12	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: LTRANPHD$ Account Domain: WORKGROUP Logon ID: 0x3e7 Object: Object Server: Security Object Type: File Object Name: C:\Windows\WinSxS\FileMaps\$$_system32_21f9a9c4a2f8b514.cdf-ms Handle ID: 0x7d0 Process Information: Process ID: 0xf34 Process Name: C:\Windows\WinSxS\amd64_microsoft-windows-servicingstack_31bf3856ad364e35_6.3.9600.17477_none_fa2b7d3b9b36c7b4\TiWorker.exe Auditing Settings: Original Security Descriptor: New Security Descriptor: S:ARAI(AU;SAFA;0x1f0116;;;WD)
Security	Audit Success	13568	2015-04-22 19:04:12	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: LTRANPHD$ Account Domain: WORKGROUP Logon ID: 0x3e7 Object: Object Server: Security Object Type: File Object Name: C:\Windows\System32\SRH.dll Handle ID: 0x558 Process Information: Process ID: 0xf34 Process Name: C:\Windows\WinSxS\amd64_microsoft-windows-servicingstack_31bf3856ad364e35_6.3.9600.17477_none_fa2b7d3b9b36c7b4\TiWorker.exe Auditing Settings: Original Security Descriptor: S:AI New Security Descriptor: S:ARAI(AU;SAFA;DCLCRPCRSDWDWO;;;WD)
Security	Audit Success	13568	2015-04-22 19:04:12	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: LTRANPHD$ Account Domain: WORKGROUP Logon ID: 0x3e7 Object: Object Server: Security Object Type: File Object Name: C:\Windows\SysWOW64\SRH.dll Handle ID: 0x5f0 Process Information: Process ID: 0xf34 Process Name: C:\Windows\WinSxS\amd64_microsoft-windows-servicingstack_31bf3856ad364e35_6.3.9600.17477_none_fa2b7d3b9b36c7b4\TiWorker.exe Auditing Settings: Original Security Descriptor: S:AI New Security Descriptor: S:ARAI(AU;SAFA;DCLCRPCRSDWDWO;;;WD)
			2015-04-		4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: LTRANPHD$ Account Domain: WORKGROUP Logon ID: 0x3e7 Object: Object Server: Security Object Type: File Object

Security	Audit Success	13568	22 19:04:17	Microsoft-Windows-Security-Auditing	Name: C:\Windows\WinSxS\FileMaps_0000000000000000.cdf-ms Handle ID: 0x504 Process Information: Process ID: 0xf34 Process Name: C:\Windows\WinSxS\amd64_microsoft-windows-servicingstack_31bf3856ad364e35_6.3.9600.17477_none_fa2b7d3b9b36c7b4\TiWorker.exe Auditing Settings: Original Security Descriptor: New Security Descriptor: S:ARAI(AU;SAFA;0x1f0116;;;WD)
Security	Audit Success	13568	2015-04-22 19:04:17	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: LTRANPHD$ Account Domain: WORKGROUP Logon ID: 0x3e7 Object: Object Server: Security Object Type: File Object Name: C:\Windows\WinSxS\FileMaps\$$.cdf-ms Handle ID: 0x61c Process Information: Process ID: 0xf34 Process Name: C:\Windows\WinSxS\amd64_microsoft-windows-servicingstack_31bf3856ad364e35_6.3.9600.17477_none_fa2b7d3b9b36c7b4\TiWorker.exe Auditing Settings: Original Security Descriptor: New Security Descriptor: S:ARAI(AU;SAFA;0x1f0116;;;WD)
Security	Audit Success	13568	2015-04-22 19:04:17	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: LTRANPHD$ Account Domain: WORKGROUP Logon ID: 0x3e7 Object: Object Server: Security Object Type: File Object Name: C:\Windows\WinSxS\FileMaps\$$_fonts_40104ba9a1d20dac.cdf-ms Handle ID: 0x4ec Process Information: Process ID: 0xf34 Process Name: C:\Windows\WinSxS\amd64_microsoft-windows-servicingstack_31bf3856ad364e35_6.3.9600.17477_none_fa2b7d3b9b36c7b4\TiWorker.exe Auditing Settings: Original Security Descriptor: New Security Descriptor: S:ARAI(AU;SAFA;0x1f0116;;;WD)
Security	Audit Success	13568	2015-04-22 19:04:17	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: LTRANPHD$ Account Domain: WORKGROUP Logon ID: 0x3e7 Object: Object Server: Security Object Type: File Object Name: C:\Windows\WinSxS\FileMaps_0000000000000000.cdf-ms Handle ID: 0x508 Process Information: Process ID: 0xf34 Process Name: C:\Windows\WinSxS\amd64_microsoft-windows-servicingstack_31bf3856ad364e35_6.3.9600.17477_none_fa2b7d3b9b36c7b4\TiWorker.exe Auditing Settings: Original Security Descriptor: New Security Descriptor: S:ARAI(AU;SAFA;0x1f0116;;;WD)
Security	Audit Success	13568	2015-04-22 19:04:17	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: LTRANPHD$ Account Domain: WORKGROUP Logon ID: 0x3e7 Object: Object Server: Security Object Type: File Object Name: C:\Windows\WinSxS\FileMaps\$$.cdf-ms Handle ID: 0x3a4 Process Information: Process ID: 0xf34 Process Name: C:\Windows\WinSxS\amd64_microsoft-windows-servicingstack_31bf3856ad364e35_6.3.9600.17477_none_fa2b7d3b9b36c7b4\TiWorker.exe Auditing Settings: Original Security Descriptor: New Security Descriptor: S:ARAI(AU;SAFA;0x1f0116;;;WD)
Security	Audit Success	13568	2015-04-22 19:04:17	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: LTRANPHD$ Account Domain: WORKGROUP Logon ID: 0x3e7 Object: Object Server: Security Object Type: File Object Name: C:\Windows\WinSxS\FileMaps\$$_system32_21f9a9c4a2f8b514.cdf-ms Handle ID: 0x710 Process Information: Process ID: 0xf34 Process Name: C:\Windows\WinSxS\amd64_microsoft-windows-servicingstack_31bf3856ad364e35_6.3.9600.17477_none_fa2b7d3b9b36c7b4\TiWorker.exe Auditing Settings: Original Security Descriptor: New Security Descriptor: S:ARAI(AU;SAFA;0x1f0116;;;WD)
Security	Audit Success	13568	2015-04-22 19:04:17	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: LTRANPHD$ Account Domain: WORKGROUP Logon ID: 0x3e7 Object: Object Server: Security Object Type: File Object Name: C:\Windows\WinSxS\FileMaps\$$_system32_advancedinstallers_dfe2cf200b391371.cdf-ms Handle ID: 0x710 Process Information: Process ID: 0xf34 Process Name: C:\Windows\WinSxS\amd64_microsoft-windows-servicingstack_31bf3856ad364e35_6.3.9600.17477_none_fa2b7d3b9b36c7b4\TiWorker.exe Auditing Settings: Original Security Descriptor: New Security Descriptor: S:ARAI(AU;SAFA;0x1f0116;;;WD)
Security	Audit Success	13568	2015-04-22 19:04:17	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: LTRANPHD$ Account Domain: WORKGROUP Logon ID: 0x3e7 Object: Object Server: Security Object Type: File Object Name: C:\Windows\System32\AdvancedInstallers\cmitrust.dll Handle ID: 0x710 Process Information: Process ID: 0xf34 Process Name: C:\Windows\WinSxS\amd64_microsoft-windows-servicingstack_31bf3856ad364e35_6.3.9600.17477_none_fa2b7d3b9b36c7b4\TiWorker.exe Auditing Settings: Original Security Descriptor: S:AI New Security Descriptor: S:ARAI(AU;SAFA;DCLCRPCRSDWDWO;;;WD)
Security	Audit Success	13568	2015-04-22 19:04:22	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: LTRANPHD$ Account Domain: WORKGROUP Logon ID: 0x3e7 Object: Object Server: Security Object Type: File Object Name: C:\Windows\WinSxS\FileMaps_0000000000000000.cdf-ms Handle ID: 0x358 Process Information: Process ID: 0xf34 Process Name: C:\Windows\WinSxS\amd64_microsoft-windows-servicingstack_31bf3856ad364e35_6.3.9600.17477_none_fa2b7d3b9b36c7b4\TiWorker.exe Auditing Settings: Original Security Descriptor: New Security Descriptor: S:ARAI(AU;SAFA;0x1f0116;;;WD)
Security	Audit Success	13568	2015-04-22 19:04:22	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: LTRANPHD$ Account Domain: WORKGROUP Logon ID: 0x3e7 Object: Object Server: Security Object Type: File Object Name: C:\Windows\WinSxS\FileMaps\$$.cdf-ms Handle ID: 0x588 Process Information: Process ID: 0xf34 Process Name: C:\Windows\WinSxS\amd64_microsoft-windows-servicingstack_31bf3856ad364e35_6.3.9600.17477_none_fa2b7d3b9b36c7b4\TiWorker.exe Auditing Settings: Original Security Descriptor: New Security Descriptor: S:ARAI(AU;SAFA;0x1f0116;;;WD)
Security	Audit Success	13568	2015-04-22 19:04:22	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: LTRANPHD$ Account Domain: WORKGROUP Logon ID: 0x3e7 Object: Object Server: Security Object Type: File Object Name: C:\Windows\WinSxS\FileMaps\$$_immersivecontrolpanel_1e6ccf0e6a91b570.cdf-ms Handle ID: 0x220 Process Information: Process ID: 0xf34 Process Name: C:\Windows\WinSxS\amd64_microsoft-windows-servicingstack_31bf3856ad364e35_6.3.9600.17477_none_fa2b7d3b9b36c7b4\TiWorker.exe Auditing Settings: Original Security Descriptor: New Security Descriptor: S:ARAI(AU;SAFA;0x1f0116;;;WD)
					4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: LTRANPHD$

Security	Audit Success	13568	2015-04-22 19:04:22	Microsoft-Windows-Security-Auditing	Account Domain: WORKGROUP Logon ID: 0x3e7 Object: Object Server: Security Object Type: File Object Name: C:\Windows\WinSxS\FileMaps\$$_system32_21f9a9c4a2f8b514.cdf-ms Handle ID: 0x358 Process Information: Process ID: 0xf34 Process Name: C:\Windows\WinSxS\amd64_microsoft-windows-servicingstack_31bf3856ad364e35_6.3.9600.17477_none_fa2b7d3b9b36c7b4\TiWorker.exe Auditing Settings: Original Security Descriptor: New Security Descriptor: S:ARAI(AU;SAFA;0x1f0116;;;WD)
Security	Audit Success	13568	2015-04-22 19:04:22	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: LTRANPHD$ Account Domain: WORKGROUP Logon ID: 0x3e7 Object: Object Server: Security Object Type: File Object Name: C:\Windows\System32\SettingsHandlers.dll Handle ID: 0x588 Process Information: Process ID: 0xf34 Process Name: C:\Windows\WinSxS\amd64_microsoft-windows-servicingstack_31bf3856ad364e35_6.3.9600.17477_none_fa2b7d3b9b36c7b4\TiWorker.exe Auditing Settings: Original Security Descriptor: S:AI New Security Descriptor: S:ARAI(AU;SAFA;DCLCRPCRSDWDWO;;;WD)
Security	Audit Success	13568	2015-04-22 19:04:22	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: LTRANPHD$ Account Domain: WORKGROUP Logon ID: 0x3e7 Object: Object Server: Security Object Type: File Object Name: C:\Windows\ImmersiveControlPanel\SystemSettings.dll Handle ID: 0x5a0 Process Information: Process ID: 0xf34 Process Name: C:\Windows\WinSxS\amd64_microsoft-windows-servicingstack_31bf3856ad364e35_6.3.9600.17477_none_fa2b7d3b9b36c7b4\TiWorker.exe Auditing Settings: Original Security Descriptor: S:AI New Security Descriptor: S:ARAI(AU;SAFA;DCLCRPCRSDWDWO;;;WD)
Security	Audit Success	13568	2015-04-22 19:04:27	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: LTRANPHD$ Account Domain: WORKGROUP Logon ID: 0x3e7 Object: Object Server: Security Object Type: File Object Name: C:\Windows\WinSxS\FileMaps_0000000000000000.cdf-ms Handle ID: 0x4a8 Process Information: Process ID: 0xf34 Process Name: C:\Windows\WinSxS\amd64_microsoft-windows-servicingstack_31bf3856ad364e35_6.3.9600.17477_none_fa2b7d3b9b36c7b4\TiWorker.exe Auditing Settings: Original Security Descriptor: New Security Descriptor: S:ARAI(AU;SAFA;0x1f0116;;;WD)
Security	Audit Success	13568	2015-04-22 19:04:27	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: LTRANPHD$ Account Domain: WORKGROUP Logon ID: 0x3e7 Object: Object Server: Security Object Type: File Object Name: C:\Windows\WinSxS\FileMaps\$$.cdf-ms Handle ID: 0x448 Process Information: Process ID: 0xf34 Process Name: C:\Windows\WinSxS\amd64_microsoft-windows-servicingstack_31bf3856ad364e35_6.3.9600.17477_none_fa2b7d3b9b36c7b4\TiWorker.exe Auditing Settings: Original Security Descriptor: New Security Descriptor: S:ARAI(AU;SAFA;0x1f0116;;;WD)
Security	Audit Success	13568	2015-04-22 19:04:27	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: LTRANPHD$ Account Domain: WORKGROUP Logon ID: 0x3e7 Object: Object Server: Security Object Type: File Object Name: C:\Windows\WinSxS\FileMaps\$$_syswow64_21ffbdd2a2dd92e0.cdf-ms Handle ID: 0x764 Process Information: Process ID: 0xf34 Process Name: C:\Windows\WinSxS\amd64_microsoft-windows-servicingstack_31bf3856ad364e35_6.3.9600.17477_none_fa2b7d3b9b36c7b4\TiWorker.exe Auditing Settings: Original Security Descriptor: New Security Descriptor: S:ARAI(AU;SAFA;0x1f0116;;;WD)
Security	Audit Success	13568	2015-04-22 19:04:27	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: LTRANPHD$ Account Domain: WORKGROUP Logon ID: 0x3e7 Object: Object Server: Security Object Type: File Object Name: C:\Windows\WinSxS\FileMaps\$$_system32_21f9a9c4a2f8b514.cdf-ms Handle ID: 0x4a8 Process Information: Process ID: 0xf34 Process Name: C:\Windows\WinSxS\amd64_microsoft-windows-servicingstack_31bf3856ad364e35_6.3.9600.17477_none_fa2b7d3b9b36c7b4\TiWorker.exe Auditing Settings: Original Security Descriptor: New Security Descriptor: S:ARAI(AU;SAFA;0x1f0116;;;WD)
Security	Audit Success	13568	2015-04-22 19:04:27	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: LTRANPHD$ Account Domain: WORKGROUP Logon ID: 0x3e7 Object: Object Server: Security Object Type: File Object Name: C:\Windows\System32\Windows.UI.Input.Inking.dll Handle ID: 0x448 Process Information: Process ID: 0xf34 Process Name: C:\Windows\WinSxS\amd64_microsoft-windows-servicingstack_31bf3856ad364e35_6.3.9600.17477_none_fa2b7d3b9b36c7b4\TiWorker.exe Auditing Settings: Original Security Descriptor: S:AI New Security Descriptor: S:ARAI(AU;SAFA;DCLCRPCRSDWDWO;;;WD)
Security	Audit Success	13568	2015-04-22 19:04:27	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: LTRANPHD$ Account Domain: WORKGROUP Logon ID: 0x3e7 Object: Object Server: Security Object Type: File Object Name: C:\Windows\SysWOW64\Windows.UI.Input.Inking.dll Handle ID: 0x5c4 Process Information: Process ID: 0xf34 Process Name: C:\Windows\WinSxS\amd64_microsoft-windows-servicingstack_31bf3856ad364e35_6.3.9600.17477_none_fa2b7d3b9b36c7b4\TiWorker.exe Auditing Settings: Original Security Descriptor: S:AI New Security Descriptor: S:ARAI(AU;SAFA;DCLCRPCRSDWDWO;;;WD)
Security	Audit Success	13568	2015-04-22 19:04:30	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: LTRANPHD$ Account Domain: WORKGROUP Logon ID: 0x3e7 Object: Object Server: Security Object Type: File Object Name: C:\Windows\WinSxS\FileMaps_0000000000000000.cdf-ms Handle ID: 0x4e0 Process Information: Process ID: 0xf34 Process Name: C:\Windows\WinSxS\amd64_microsoft-windows-servicingstack_31bf3856ad364e35_6.3.9600.17477_none_fa2b7d3b9b36c7b4\TiWorker.exe Auditing Settings: Original Security Descriptor: New Security Descriptor: S:ARAI(AU;SAFA;0x1f0116;;;WD)
Security	Audit Success	13568	2015-04-22 19:04:30	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: LTRANPHD$ Account Domain: WORKGROUP Logon ID: 0x3e7 Object: Object Server: Security Object Type: File Object Name: C:\Windows\WinSxS\FileMaps\program_files_ffd0cbfc813cc4f1.cdf-ms Handle ID: 0x7d4 Process Information: Process ID: 0xf34 Process Name: C:\Windows\WinSxS\amd64_microsoft-windows-servicingstack_31bf3856ad364e35_6.3.9600.17477_none_fa2b7d3b9b36c7b4\TiWorker.exe Auditing Settings: Original Security Descriptor: New Security Descriptor: S:ARAI(AU;SAFA;0x1f0116;;;WD)

Security	Audit Success	13568	2015-04-22 19:04:30	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: LTRANPHD$ Account Domain: WORKGROUP Logon ID: 0x3e7 Object: Object Server: Security Object Type: File Object Name: C:\Windows\WinSxS\FileMaps\program_files_common_files_d7a65bb2f0e854e7.cdf-ms Handle ID: 0x7ac Process Information: Process ID: 0xf34 Process Name: C:\Windows\WinSxS\amd64_microsoft-windows-servicingstack_31bf3856ad364e35_6.3.9600.17477_none_fa2b7d3b9b36c7b4\TiWorker.exe Auditing Settings: Original Security Descriptor: New Security Descriptor: S:ARAI(AU;SAFA;0x1f0116;;;WD)
Security	Audit Success	13568	2015-04-22 19:04:30	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: LTRANPHD$ Account Domain: WORKGROUP Logon ID: 0x3e7 Object: Object Server: Security Object Type: File Object Name: C:\Windows\WinSxS\FileMaps\program_files_common_files_microsoft_shared_818c5a0e45020fba.cdf-ms Handle ID: 0x504 Process Information: Process ID: 0xf34 Process Name: C:\Windows\WinSxS\amd64_microsoft-windows-servicingstack_31bf3856ad364e35_6.3.9600.17477_none_fa2b7d3b9b36c7b4\TiWorker.exe Auditing Settings: Original Security Descriptor: New Security Descriptor: S:ARAI(AU;SAFA;0x1f0116;;;WD)
Security	Audit Success	13568	2015-04-22 19:04:30	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: LTRANPHD$ Account Domain: WORKGROUP Logon ID: 0x3e7 Object: Object Server: Security Object Type: File Object Name: C:\Windows\WinSxS\FileMaps\program_files_common_files_microsoft_shared_ink_3c86e3db0b3b254c.cdf-ms Handle ID: 0x504 Process Information: Process ID: 0xf34 Process Name: C:\Windows\WinSxS\amd64_microsoft-windows-servicingstack_31bf3856ad364e35_6.3.9600.17477_none_fa2b7d3b9b36c7b4\TiWorker.exe Auditing Settings: Original Security Descriptor: New Security Descriptor: S:ARAI(AU;SAFA;0x1f0116;;;WD)
Security	Audit Success	13568	2015-04-22 19:04:30	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: LTRANPHD$ Account Domain: WORKGROUP Logon ID: 0x3e7 Object: Object Server: Security Object Type: File Object Name: C:\Windows\WinSxS\FileMaps\$$.cdf-ms Handle ID: 0x58c Process Information: Process ID: 0xf34 Process Name: C:\Windows\WinSxS\amd64_microsoft-windows-servicingstack_31bf3856ad364e35_6.3.9600.17477_none_fa2b7d3b9b36c7b4\TiWorker.exe Auditing Settings: Original Security Descriptor: New Security Descriptor: S:ARAI(AU;SAFA;0x1f0116;;;WD)
Security	Audit Success	13568	2015-04-22 19:04:30	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: LTRANPHD$ Account Domain: WORKGROUP Logon ID: 0x3e7 Object: Object Server: Security Object Type: File Object Name: C:\Windows\WinSxS\FileMaps\$$_system32_21f9a9c4a2f8b514.cdf-ms Handle ID: 0x7c0 Process Information: Process ID: 0xf34 Process Name: C:\Windows\WinSxS\amd64_microsoft-windows-servicingstack_31bf3856ad364e35_6.3.9600.17477_none_fa2b7d3b9b36c7b4\TiWorker.exe Auditing Settings: Original Security Descriptor: New Security Descriptor: S:ARAI(AU;SAFA;0x1f0116;;;WD)
Security	Audit Success	13568	2015-04-22 19:04:30	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: LTRANPHD$ Account Domain: WORKGROUP Logon ID: 0x3e7 Object: Object Server: Security Object Type: File Object Name: C:\Windows\WinSxS\FileMaps\$$_system32_spp_tokens_ppdlic_0f09ba294211a24b.cdf-ms Handle ID: 0x504 Process Information: Process ID: 0xf34 Process Name: C:\Windows\WinSxS\amd64_microsoft-windows-servicingstack_31bf3856ad364e35_6.3.9600.17477_none_fa2b7d3b9b36c7b4\TiWorker.exe Auditing Settings: Original Security Descriptor: New Security Descriptor: S:ARAI(AU;SAFA;0x1f0116;;;WD)
Security	Audit Success	13568	2015-04-22 19:04:30	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: LTRANPHD$ Account Domain: WORKGROUP Logon ID: 0x3e7 Object: Object Server: Security Object Type: File Object Name: C:\Windows\System32\spp\tokens\ppdlic\TabletPCInputPersonalization-ppdlic.xrm-ms Handle ID: 0x504 Process Information: Process ID: 0xf34 Process Name: C:\Windows\WinSxS\amd64_microsoft-windows-servicingstack_31bf3856ad364e35_6.3.9600.17477_none_fa2b7d3b9b36c7b4\TiWorker.exe Auditing Settings: Original Security Descriptor: S:AI New Security Descriptor: S:ARAI(AU;SAFA;DCLCRPCRSDWDWO;;;WD)
Security	Audit Success	13568	2015-04-22 19:04:30	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: LTRANPHD$ Account Domain: WORKGROUP Logon ID: 0x3e7 Object: Object Server: Security Object Type: File Object Name: C:\Program Files\Common Files\microsoft shared\ink\InputPersonalization.exe Handle ID: 0x710 Process Information: Process ID: 0xf34 Process Name: C:\Windows\WinSxS\amd64_microsoft-windows-servicingstack_31bf3856ad364e35_6.3.9600.17477_none_fa2b7d3b9b36c7b4\TiWorker.exe Auditing Settings: Original Security Descriptor: S:AI New Security Descriptor: S:ARAI(AU;SAFA;DCLCRPCRSDWDWO;;;WD)
Security	Audit Success	12545	2015-04-22 19:04:41	Microsoft-Windows-Security-Auditing	4647: User initiated logoff: Subject: Security ID: S-1-5-21-1888849264-3803429180-4108621888-1001 Account Name: Liem Account Domain: LTRANPHD Logon ID: 0x18453 This event is generated when a logoff is initiated. No further user-initiated activity can occur. This event can be interpreted as a logoff event.
Security	Audit Success	13568	2015-04-22 19:04:56	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: LTRANPHD$ Account Domain: WORKGROUP Logon ID: 0x3e7 Object: Object Server: Security Object Type: File Object Name: C:\Windows\System32\rascfg.dll Handle ID: 0x20 Process Information: Process ID: 0x1244 Process Name: C:\Windows\System32\poqexec.exe Auditing Settings: Original Security Descriptor: S:AI New Security Descriptor: S:ARAI(AU;SAFA;DCLCRPCRSDWDWO;;;WD)
Security	Audit Success	13568	2015-04-22 19:04:56	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: LTRANPHD$ Account Domain: WORKGROUP Logon ID: 0x3e7 Object: Object Server: Security Object Type: File Object Name: C:\Windows\System32\drivers\ndproxy.sys Handle ID: 0x38 Process Information: Process ID: 0x1244 Process Name: C:\Windows\System32\poqexec.exe Auditing Settings: Original Security Descriptor: S:AI New Security Descriptor: S:ARAI(AU;SAFA;DCLCRPCRSDWDWO;;;WD)
					4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: LTRANPHD$

Security	Audit Success	13568	2015-04-22 19:04:56	Microsoft-Windows-Security-Auditing	Account Domain: WORKGROUP Logon ID: 0x3e7 Object: Object Server: Security Object Type: File Object Name: C:\Windows\System32\drivers\wanarp.sys Handle ID: 0x38 Process Information: Process ID: 0x1244 Process Name: C:\Windows\System32\poqexec.exe Auditing Settings: Original Security Descriptor: S:AI New Security Descriptor: S:ARAI(AU;SAFA;DCLCRPCRSDWDWO;;;WD)
Security	Audit Success	13568	2015-04-22 19:04:56	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: LTRANPHD$ Account Domain: WORKGROUP Logon ID: 0x3e7 Object: Object Server: Security Object Type: File Object Name: C:\Windows\System32\spp\tokens\ppdlic\RasBase-ppdlic.xrm-ms Handle ID: 0x38 Process Information: Process ID: 0x1244 Process Name: C:\Windows\System32\poqexec.exe Auditing Settings: Original Security Descriptor: S:AI New Security Descriptor: S:ARAI(AU;SAFA;DCLCRPCRSDWDWO;;;WD)
Security	Audit Success	13568	2015-04-22 19:04:56	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: LTRANPHD$ Account Domain: WORKGROUP Logon ID: 0x3e7 Object: Object Server: Security Object Type: File Object Name: C:\Windows\SysWOW64\rascfg.dll Handle ID: 0x20 Process Information: Process ID: 0x1244 Process Name: C:\Windows\System32\poqexec.exe Auditing Settings: Original Security Descriptor: S:AI New Security Descriptor: S:ARAI(AU;SAFA;DCLCRPCRSDWDWO;;;WD)
Security	Audit Success	13568	2015-04-22 19:04:56	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: LTRANPHD$ Account Domain: WORKGROUP Logon ID: 0x3e7 Object: Object Server: Security Object Type: File Object Name: C:\Windows\WinSxS\FileMaps_0000000000000000.cdf-ms Handle ID: 0x38 Process Information: Process ID: 0x1244 Process Name: C:\Windows\System32\poqexec.exe Auditing Settings: Original Security Descriptor: New Security Descriptor: S:ARAI(AU;SAFA;0x1f0116;;;WD)
Security	Audit Success	13568	2015-04-22 19:04:56	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: LTRANPHD$ Account Domain: WORKGROUP Logon ID: 0x3e7 Object: Object Server: Security Object Type: File Object Name: C:\Windows\WinSxS\FileMaps\$$.cdf-ms Handle ID: 0x38 Process Information: Process ID: 0x1244 Process Name: C:\Windows\System32\poqexec.exe Auditing Settings: Original Security Descriptor: New Security Descriptor: S:ARAI(AU;SAFA;0x1f0116;;;WD)
Security	Audit Success	13568	2015-04-22 19:04:56	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: LTRANPHD$ Account Domain: WORKGROUP Logon ID: 0x3e7 Object: Object Server: Security Object Type: File Object Name: C:\Windows\WinSxS\FileMaps\$$_syswow64_21ffbdd2a2dd92e0.cdf-ms Handle ID: 0x38 Process Information: Process ID: 0x1244 Process Name: C:\Windows\System32\poqexec.exe Auditing Settings: Original Security Descriptor: New Security Descriptor: S:ARAI(AU;SAFA;0x1f0116;;;WD)
Security	Audit Success	13568	2015-04-22 19:04:56	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: LTRANPHD$ Account Domain: WORKGROUP Logon ID: 0x3e7 Object: Object Server: Security Object Type: File Object Name: C:\Windows\WinSxS\FileMaps\$$_system32_21f9a9c4a2f8b514.cdf-ms Handle ID: 0x2c Process Information: Process ID: 0x1244 Process Name: C:\Windows\System32\poqexec.exe Auditing Settings: Original Security Descriptor: New Security Descriptor: S:ARAI(AU;SAFA;0x1f0116;;;WD)
Security	Audit Success	13568	2015-04-22 19:04:56	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: LTRANPHD$ Account Domain: WORKGROUP Logon ID: 0x3e7 Object: Object Server: Security Object Type: File Object Name: C:\Windows\WinSxS\FileMaps\$$_system32_spp_tokens_ppdlic_0f09ba294211a24b.cdf-ms Handle ID: 0x38 Process Information: Process ID: 0x1244 Process Name: C:\Windows\System32\poqexec.exe Auditing Settings: Original Security Descriptor: New Security Descriptor: S:ARAI(AU;SAFA;0x1f0116;;;WD)
Security	Audit Success	13568	2015-04-22 19:04:56	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: LTRANPHD$ Account Domain: WORKGROUP Logon ID: 0x3e7 Object: Object Server: Security Object Type: File Object Name: C:\Windows\WinSxS\FileMaps\$$_system32_drivers_dc1b782427b5ee1b.cdf-ms Handle ID: 0x14 Process Information: Process ID: 0x1244 Process Name: C:\Windows\System32\poqexec.exe Auditing Settings: Original Security Descriptor: New Security Descriptor: S:ARAI(AU;SAFA;0x1f0116;;;WD)
Security	Audit Success	13568	2015-04-22 19:04:56	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: LTRANPHD$ Account Domain: WORKGROUP Logon ID: 0x3e7 Object: Object Server: Security Object Type: File Object Name: C:\Windows\WinSxS\FileMaps_0000000000000000.cdf-ms Handle ID: 0x38 Process Information: Process ID: 0x1244 Process Name: C:\Windows\System32\poqexec.exe Auditing Settings: Original Security Descriptor: New Security Descriptor: S:ARAI(AU;SAFA;0x1f0116;;;WD)
Security	Audit Success	13568	2015-04-22 19:04:56	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: LTRANPHD$ Account Domain: WORKGROUP Logon ID: 0x3e7 Object: Object Server: Security Object Type: File Object Name: C:\Windows\WinSxS\FileMaps\$$.cdf-ms Handle ID: 0x38 Process Information: Process ID: 0x1244 Process Name: C:\Windows\System32\poqexec.exe Auditing Settings: Original Security Descriptor: New Security Descriptor: S:ARAI(AU;SAFA;0x1f0116;;;WD)
Security	Audit Success	13568	2015-04-22 19:04:56	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: LTRANPHD$ Account Domain: WORKGROUP Logon ID: 0x3e7 Object: Object Server: Security Object Type: File Object Name: C:\Windows\WinSxS\FileMaps\$$_syswow64_21ffbdd2a2dd92e0.cdf-ms Handle ID: 0x38 Process Information: Process ID: 0x1244 Process Name: C:\Windows\System32\poqexec.exe Auditing Settings: Original Security Descriptor: New Security Descriptor: S:ARAI(AU;SAFA;0x1f0116;;;WD)
Security	Audit Success	13568	2015-04-22 19:04:56	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: LTRANPHD$ Account Domain: WORKGROUP Logon ID: 0x3e7 Object: Object Server: Security Object Type: File Object Name: C:\Windows\WinSxS\FileMaps\$$_system32_21f9a9c4a2f8b514.cdf-ms Handle ID: 0x38 Process Information: Process ID: 0x1244 Process Name: C:\Windows\System32\poqexec.exe Auditing Settings: Original Security Descriptor: New Security Descriptor: S:ARAI(AU;SAFA;0x1f0116;;;WD)

Security	Audit Success	13568	2015-04-22 19:04:56	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: LTRANPHD$ Account Domain: WORKGROUP Logon ID: 0x3e7 Object: Object Server: Security Object Type: File Object Name: C:\Windows\System32\schannel.dll Handle ID: 0x20 Process Information: Process ID: 0x1244 Process Name: C:\Windows\System32\poqexec.exe Auditing Settings: Original Security Descriptor: S:AI New Security Descriptor: S:ARAI(AU;SAFA;DCLCRPCRSDWDWO;;;WD)
Security	Audit Success	13568	2015-04-22 19:04:56	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: LTRANPHD$ Account Domain: WORKGROUP Logon ID: 0x3e7 Object: Object Server: Security Object Type: File Object Name: C:\Windows\SysWOW64\schannel.dll Handle ID: 0x14 Process Information: Process ID: 0x1244 Process Name: C:\Windows\System32\poqexec.exe Auditing Settings: Original Security Descriptor: S:AI New Security Descriptor: S:ARAI(AU;SAFA;DCLCRPCRSDWDWO;;;WD)
Security	Audit Success	13568	2015-04-22 19:04:56	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: LTRANPHD$ Account Domain: WORKGROUP Logon ID: 0x3e7 Object: Object Server: Security Object Type: File Object Name: C:\Windows\WinSxS\FileMaps_00000000000000000.cdf-ms Handle ID: 0x38 Process Information: Process ID: 0x1244 Process Name: C:\Windows\System32\poqexec.exe Auditing Settings: Original Security Descriptor: New Security Descriptor: S:ARAI(AU;SAFA;0x1f0116;;;WD)
Security	Audit Success	13568	2015-04-22 19:04:56	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: LTRANPHD$ Account Domain: WORKGROUP Logon ID: 0x3e7 Object: Object Server: Security Object Type: File Object Name: C:\Windows\WinSxS\FileMaps\$$.cdf-ms Handle ID: 0x38 Process Information: Process ID: 0x1244 Process Name: C:\Windows\System32\poqexec.exe Auditing Settings: Original Security Descriptor: New Security Descriptor: S:ARAI(AU;SAFA;0x1f0116;;;WD)
Security	Audit Success	13568	2015-04-22 19:04:56	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: LTRANPHD$ Account Domain: WORKGROUP Logon ID: 0x3e7 Object: Object Server: Security Object Type: File Object Name: C:\Windows\WinSxS\FileMaps\$$_syswow64_21ffbdd2a2dd92e0.cdf-ms Handle ID: 0x38 Process Information: Process ID: 0x1244 Process Name: C:\Windows\System32\poqexec.exe Auditing Settings: Original Security Descriptor: New Security Descriptor: S:ARAI(AU;SAFA;0x1f0116;;;WD)
Security	Audit Success	13568	2015-04-22 19:04:56	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: LTRANPHD$ Account Domain: WORKGROUP Logon ID: 0x3e7 Object: Object Server: Security Object Type: File Object Name: C:\Windows\WinSxS\FileMaps\$$_system32_21f9a9c4a2f8b514.cdf-ms Handle ID: 0x38 Process Information: Process ID: 0x1244 Process Name: C:\Windows\System32\poqexec.exe Auditing Settings: Original Security Descriptor: New Security Descriptor: S:ARAI(AU;SAFA;0x1f0116;;;WD)
Security	Audit Success	13568	2015-04-22 19:04:56	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: LTRANPHD$ Account Domain: WORKGROUP Logon ID: 0x3e7 Object: Object Server: Security Object Type: File Object Name: C:\Windows\System32\certcli.dll Handle ID: 0x14 Process Information: Process ID: 0x1244 Process Name: C:\Windows\System32\poqexec.exe Auditing Settings: Original Security Descriptor: S:AI New Security Descriptor: S:ARAI(AU;SAFA;DCLCRPCRSDWDWO;;;WD)
Security	Audit Success	13568	2015-04-22 19:04:56	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: LTRANPHD$ Account Domain: WORKGROUP Logon ID: 0x3e7 Object: Object Server: Security Object Type: File Object Name: C:\Windows\System32\dpapisrv.dll Handle ID: 0x2c Process Information: Process ID: 0x1244 Process Name: C:\Windows\System32\poqexec.exe Auditing Settings: Original Security Descriptor: S:AI New Security Descriptor: S:ARAI(AU;SAFA;DCLCRPCRSDWDWO;;;WD)
Security	Audit Success	13568	2015-04-22 19:04:56	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: LTRANPHD$ Account Domain: WORKGROUP Logon ID: 0x3e7 Object: Object Server: Security Object Type: File Object Name: C:\Windows\SysWOW64\certcli.dll Handle ID: 0x2c Process Information: Process ID: 0x1244 Process Name: C:\Windows\System32\poqexec.exe Auditing Settings: Original Security Descriptor: S:AI New Security Descriptor: S:ARAI(AU;SAFA;DCLCRPCRSDWDWO;;;WD)
Security	Audit Success	13568	2015-04-22 19:04:57	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: LTRANPHD$ Account Domain: WORKGROUP Logon ID: 0x3e7 Object: Object Server: Security Object Type: File Object Name: C:\Windows\WinSxS\FileMaps_0000000000000000.cdf-ms Handle ID: 0x38 Process Information: Process ID: 0x1244 Process Name: C:\Windows\System32\poqexec.exe Auditing Settings: Original Security Descriptor: New Security Descriptor: S:ARAI(AU;SAFA;0x1f0116;;;WD)
Security	Audit Success	13568	2015-04-22 19:04:57	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: LTRANPHD$ Account Domain: WORKGROUP Logon ID: 0x3e7 Object: Object Server: Security Object Type: File Object Name: C:\Windows\WinSxS\FileMaps\$$.cdf-ms Handle ID: 0x38 Process Information: Process ID: 0x1244 Process Name: C:\Windows\System32\poqexec.exe Auditing Settings: Original Security Descriptor: New Security Descriptor: S:ARAI(AU;SAFA;0x1f0116;;;WD)
Security	Audit Success	13568	2015-04-22 19:04:57	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: LTRANPHD$ Account Domain: WORKGROUP Logon ID: 0x3e7 Object: Object Server: Security Object Type: File Object Name: C:\Windows\WinSxS\FileMaps\$$_system32_21f9a9c4a2f8b514.cdf-ms Handle ID: 0x38 Process Information: Process ID: 0x1244 Process Name: C:\Windows\System32\poqexec.exe Auditing Settings: Original Security Descriptor: New Security Descriptor: S:ARAI(AU;SAFA;0x1f0116;;;WD)
Security	Audit Success	13568	2015-04-22 19:04:57	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: LTRANPHD$ Account Domain: WORKGROUP Logon ID: 0x3e7 Object: Object Server: Security Object Type: File Object Name: C:\Windows\System32\wevtsvc.dll Handle ID: 0x14 Process Information: Process ID: 0x1244 Process Name: C:\Windows\System32\poqexec.exe Auditing Settings: Original Security Descriptor: S:AI New Security Descriptor: S:ARAI(AU;SAFA;DCLCRPCRSDWDWO;;;WD)

Security	Audit Success	13568	2015-04-22 19:04:57	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: LTRANPHD$ Account Domain: WORKGROUP Logon ID: 0x3e7 Object: Object Server: Security Object Type: File Object Name: C:\Windows\System32\drivers\udfs.sys Handle ID: 0x38 Process Information: Process ID: 0x1244 Process Name: C:\Windows\System32\poqexec.exe Auditing Settings: Original Security Descriptor: S:AI New Security Descriptor: S:ARAI(AU;SAFA;DCLCRPCRSDWDWO;;;WD)
Security	Audit Success	13568	2015-04-22 19:04:57	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: LTRANPHD$ Account Domain: WORKGROUP Logon ID: 0x3e7 Object: Object Server: Security Object Type: File Object Name: C:\Windows\WinSxS\FileMaps_0000000000000000.cdf-ms Handle ID: 0x38 Process Information: Process ID: 0x1244 Process Name: C:\Windows\System32\poqexec.exe Auditing Settings: Original Security Descriptor: New Security Descriptor: S:ARAI(AU;SAFA;0x1f0116;;;WD)
Security	Audit Success	13568	2015-04-22 19:04:57	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: LTRANPHD$ Account Domain: WORKGROUP Logon ID: 0x3e7 Object: Object Server: Security Object Type: File Object Name: C:\Windows\WinSxS\FileMaps\$$.cdf-ms Handle ID: 0x38 Process Information: Process ID: 0x1244 Process Name: C:\Windows\System32\poqexec.exe Auditing Settings: Original Security Descriptor: New Security Descriptor: S:ARAI(AU;SAFA;0x1f0116;;;WD)
Security	Audit Success	13568	2015-04-22 19:04:57	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: LTRANPHD$ Account Domain: WORKGROUP Logon ID: 0x3e7 Object: Object Server: Security Object Type: File Object Name: C:\Windows\WinSxS\FileMaps\$$_system32_21f9a9c4a2f8b514.cdf-ms Handle ID: 0x20 Process Information: Process ID: 0x1244 Process Name: C:\Windows\System32\poqexec.exe Auditing Settings: Original Security Descriptor: New Security Descriptor: S:ARAI(AU;SAFA;0x1f0116;;;WD)
Security	Audit Success	13568	2015-04-22 19:04:57	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: LTRANPHD$ Account Domain: WORKGROUP Logon ID: 0x3e7 Object: Object Server: Security Object Type: File Object Name: C:\Windows\WinSxS\FileMaps\$$_system32_drivers_dc1b782427b5ee1b.cdf-ms Handle ID: 0x38 Process Information: Process ID: 0x1244 Process Name: C:\Windows\System32\poqexec.exe Auditing Settings: Original Security Descriptor: New Security Descriptor: S:ARAI(AU;SAFA;0x1f0116;;;WD)
Security	Audit Success	13568	2015-04-22 19:04:57	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: LTRANPHD$ Account Domain: WORKGROUP Logon ID: 0x3e7 Object: Object Server: Security Object Type: File Object Name: C:\Windows\WinSxS\FileMaps_0000000000000000.cdf-ms Handle ID: 0x20 Process Information: Process ID: 0x1244 Process Name: C:\Windows\System32\poqexec.exe Auditing Settings: Original Security Descriptor: New Security Descriptor: S:ARAI(AU;SAFA;0x1f0116;;;WD)
Security	Audit Success	13568	2015-04-22 19:04:57	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: LTRANPHD$ Account Domain: WORKGROUP Logon ID: 0x3e7 Object: Object Server: Security Object Type: File Object Name: C:\Windows\WinSxS\FileMaps\$$.cdf-ms Handle ID: 0x38 Process Information: Process ID: 0x1244 Process Name: C:\Windows\System32\poqexec.exe Auditing Settings: Original Security Descriptor: New Security Descriptor: S:ARAI(AU;SAFA;0x1f0116;;;WD)
Security	Audit Success	13568	2015-04-22 19:04:57	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: LTRANPHD$ Account Domain: WORKGROUP Logon ID: 0x3e7 Object: Object Server: Security Object Type: File Object Name: C:\Windows\WinSxS\FileMaps\$$_syswow64_21ffbdd2a2dd92e0.cdf-ms Handle ID: 0x38 Process Information: Process ID: 0x1244 Process Name: C:\Windows\System32\poqexec.exe Auditing Settings: Original Security Descriptor: New Security Descriptor: S:ARAI(AU;SAFA;0x1f0116;;;WD)
Security	Audit Success	13568	2015-04-22 19:04:57	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: LTRANPHD$ Account Domain: WORKGROUP Logon ID: 0x3e7 Object: Object Server: Security Object Type: File Object Name: C:\Windows\WinSxS\FileMaps\$$_system32_21f9a9c4a2f8b514.cdf-ms Handle ID: 0x38 Process Information: Process ID: 0x1244 Process Name: C:\Windows\System32\poqexec.exe Auditing Settings: Original Security Descriptor: New Security Descriptor: S:ARAI(AU;SAFA;0x1f0116;;;WD)
Security	Audit Success	13568	2015-04-22 19:04:57	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: LTRANPHD$ Account Domain: WORKGROUP Logon ID: 0x3e7 Object: Object Server: Security Object Type: File Object Name: C:\Windows\System32\PhotoMetadataHandler.dll Handle ID: 0x20 Process Information: Process ID: 0x1244 Process Name: C:\Windows\System32\poqexec.exe Auditing Settings: Original Security Descriptor: S:AI New Security Descriptor: S:ARAI(AU;SAFA;DCLCRPCRSDWDWO;;;WD)
Security	Audit Success	13568	2015-04-22 19:04:57	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: LTRANPHD$ Account Domain: WORKGROUP Logon ID: 0x3e7 Object: Object Server: Security Object Type: File Object Name: C:\Windows\SysWOW64\PhotoMetadataHandler.dll Handle ID: 0x20 Process Information: Process ID: 0x1244 Process Name: C:\Windows\System32\poqexec.exe Auditing Settings: Original Security Descriptor: S:AI New Security Descriptor: S:ARAI(AU;SAFA;DCLCRPCRSDWDWO;;;WD)
Security	Audit Success	13568	2015-04-22 19:04:57	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: LTRANPHD$ Account Domain: WORKGROUP Logon ID: 0x3e7 Object: Object Server: Security Object Type: File Object Name: C:\Windows\WinSxS\FileMaps_0000000000000000.cdf-ms Handle ID: 0x38 Process Information: Process ID: 0x1244 Process Name: C:\Windows\System32\poqexec.exe Auditing Settings: Original Security Descriptor: New Security Descriptor: S:ARAI(AU;SAFA;0x1f0116;;;WD)
Security	Audit Success	13568	2015-04-22 19:04:57	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: LTRANPHD$ Account Domain: WORKGROUP Logon ID: 0x3e7 Object: Object Server: Security Object Type: File Object Name: C:\Windows\WinSxS\FileMaps\$$.cdf-ms Handle ID: 0x38 Process Information: Process ID: 0x1244 Process Name: C:\Windows\System32\poqexec.exe Auditing Settings: Original Security Descriptor: New Security Descriptor: S:ARAI(AU;SAFA;0x1f0116;;;WD)

Security	Audit Success	13568	2015-04-22 19:04:57	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: LTRANPHD$ Account Domain: WORKGROUP Logon ID: 0x3e7 Object: Object Server: Security Object Type: File Object Name: C:\Windows\WinSxS\FileMaps\$$_system32_21f9a9c4a2f8b514.cdf-ms Handle ID: 0x40 Process Information: Process ID: 0x1244 Process Name: C:\Windows\System32\poqexec.exe Auditing Settings: Original Security Descriptor: New Security Descriptor: S:ARAI(AU;SAFA;0x1f0116;;;WD)
Security	Audit Success	13568	2015-04-22 19:04:57	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-18 Account Name: LTRANPHD$ Account Domain: WORKGROUP Logon ID: 0x3e7 Object: Object Server: Security Object Type: File Object Name: C:\Windows\System32\win32k.sys Handle ID: 0x38 Process Information: Process ID: 0x1244 Process Name: C:\Windows\System32\poqexec.exe Auditing Settings: Original Security Descriptor: S:AI New Security Descriptor: S:ARAI(AU;SAFA;DCLCRPCRSDWDWO;;;WD)
Security	Audit Success	103	2015-04-22 19:04:58	Microsoft-Windows-Eventlog	1100: The event logging service has shut down.
Security	Audit Success	12288	2015-04-22 19:05:18	Microsoft-Windows-Security-Auditing	4608: Windows is starting up. This event is logged when LSASS.EXE starts and the auditing subsystem is initialized.
Security	Audit Success	12544	2015-04-22 19:05:18	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-0-0 Account Name: - Account Domain: - Logon ID: 0x0 Logon Type: 0 Impersonation Level: - New Logon: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Logon ID: 0x3e7 Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x4 Process Name: Network Information: Workstation Name: - Source Network Address: - Source Port: - Detailed Authentication Information: Logon Process: - Authentication Package: - Transited Services: - Package Name (NTLM only): - Key Length: 0 This event is generated when a logon session is created. It is generated on the computer that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service such as the Server service, or a local process such as Winlogon.exe or Services.exe. The logon type field indicates the kind of logon that occurred. The most common types are 2 (interactive) and 3 (network). The New Logon fields indicate the account for whom the new logon was created, i.e. the account that was logged on. The network fields indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impersonation level field indicates the extent to which a process in the logon session can impersonate. The authentication information fields provide detailed information about this specific logon request. - Logon GUID is a unique identifier that can be used to correlate this event with a KDC event. - Transited services indicate which intermediate services have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indicates the length of the generated session key. This will be 0 if no session key was requested.
Security	Audit Success	12544	2015-04-22 19:05:18	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: LTRANPHD$ Account Domain: WORKGROUP Logon ID: 0x3e7 Logon Type: 5 Impersonation Level: %%1833 New Logon: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Logon ID: 0x3e7 Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x238 Process Name: C:\Windows\System32\services.exe Network Information: Workstation Name: Source Network Address: - Source Port: - Detailed Authentication Information: Logon Process: Advapi Authentication Package: Negotiate Transited Services: - Package Name (NTLM only): - Key Length: 0 This event is generated when a logon session is created. It is generated on the computer that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service such as the Server service, or a local process such as Winlogon.exe or Services.exe. The logon type field indicates the kind of logon that occurred. The most common types are 2 (interactive) and 3 (network). The New Logon fields indicate the account for whom the new logon was created, i.e. the account that was logged on. The network fields indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impersonation level field indicates the extent to which a process in the logon session can impersonate. The authentication information fields provide detailed information about this specific logon request. - Logon GUID is a unique identifier that can be used to correlate this event with a KDC event. - Transited services indicate which intermediate services have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indicates the length of the generated session key. This will be 0 if no session key was requested.
Security	Audit Success	12544	2015-04-22 19:05:18	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: LTRANPHD$ Account Domain: WORKGROUP Logon ID: 0x3e7 Logon Type: 5 Impersonation Level: %%1833 New Logon: Security ID: S-1-5-20 Account Name: NETWORK SERVICE Account Domain: NT AUTHORITY Logon ID: 0x3e4 Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x238 Process Name: C:\Windows\System32\services.exe Network Information: Workstation Name: Source Network Address: - Source Port: - Detailed Authentication Information: Logon Process: Advapi Authentication Package: Negotiate Transited Services: - Package Name (NTLM only): - Key Length: 0 This event is generated when a logon session is created. It is generated on the computer that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service such as the Server service, or a local process such as Winlogon.exe or Services.exe. The logon type field indicates the kind of logon that occurred. The most common types are 2 (interactive) and 3 (network). The New Logon fields indicate the account for whom the new logon was created, i.e. the account that was logged on. The network fields indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some

					cases. The impersonation level field indicates the extent to which a process in the logon session can impersonate. The authentication information fields provide detailed information about this specific logon request. - Logon GUID is a unique identifier that can be used to correlate this event with a KDC event. - Transited services indicate which intermediate services have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indicates the length of the generated session key. This will be 0 if no session key was requested.
Security	Audit Success	12548	2015-04-22 19:05:18	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Logon ID: 0x3e7 Privileges: SeAssignPrimaryTokenPrivilege SeTcbPrivilege SeSecurityPrivilege SeTakeOwnershipPrivilege SeLoadDriverPrivilege SeBackupPrivilege SeRestorePrivilege SeDebugPrivilege SeAuditPrivilege SeSystemEnvironmentPrivilege SeImpersonatePrivilege
Security	Audit Success	12548	2015-04-22 19:05:18	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-20 Account Name: NETWORK SERVICE Account Domain: NT AUTHORITY Logon ID: 0x3e4 Privileges: SeAssignPrimaryTokenPrivilege SeAuditPrivilege SeImpersonatePrivilege
Security	Audit Success	13568	2015-04-22 19:05:18	Microsoft-Windows-Security-Auditing	4902: The Per-user audit policy table was created. Number of Elements: 0 Policy ID: 0x8b4e
Security	Audit Success	12544	2015-04-22 19:05:19	Microsoft-Windows-Security-Auditing	4648: A logon was attempted using explicit credentials. Subject: Security ID: S-1-5-18 Account Name: LTRANPHD$ Account Domain: WORKGROUP Logon ID: 0x3e7 Logon GUID: {00000000-0000-0000-0000-000000000000} Account Whose Credentials Were Used: Account Name: DWM-1 Account Domain: Window Manager Logon GUID: {00000000-0000-0000-0000-000000000000} Target Server: Target Server Name: localhost Additional Information: localhost Process Information: Process ID: 0x210 Process Name: C:\Windows\System32\winlogon.exe Network Information: Network Address: - Port: - This event is generated when a process attempts to log on an account by explicitly specifying that account's credentials. This most commonly occurs in batch-type configurations such as scheduled tasks, or when using the RUNAS command.
Security	Audit Success	12544	2015-04-22 19:05:19	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: LTRANPHD$ Account Domain: WORKGROUP Logon ID: 0x3e7 Logon Type: 2 Impersonation Level: %%1833 New Logon: Security ID: S-1-5-90-1 Account Name: DWM-1 Account Domain: Window Manager Logon ID: 0xdd65 Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x210 Process Name: C:\Windows\System32\winlogon.exe Network Information: Workstation Name: Source Network Address: - Source Port: - Detailed Authentication Information: Logon Process: Advapi Authentication Package: Negotiate Transited Services: - Package Name (NTLM only): - Key Length: 0 This event is generated when a logon session is created. It is generated on the computer that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service such as the Server service, or a local process such as Winlogon.exe or Services.exe. The logon type field indicates the kind of logon that occurred. The most common types are 2 (interactive) and 3 (network). The New Logon fields indicate the account for whom the new logon was created, i.e. the account that was logged on. The network fields indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impersonation level field indicates the extent to which a process in the logon session can impersonate. The authentication information fields provide detailed information about this specific logon request. - Logon GUID is a unique identifier that can be used to correlate this event with a KDC event. - Transited services indicate which intermediate services have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indicates the length of the generated session key. This will be 0 if no session key was requested.
Security	Audit Success	12544	2015-04-22 19:05:19	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: LTRANPHD$ Account Domain: WORKGROUP Logon ID: 0x3e7 Logon Type: 2 Impersonation Level: %%1833 New Logon: Security ID: S-1-5-90-1 Account Name: DWM-1 Account Domain: Window Manager Logon ID: 0xdd7f Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x210 Process Name: C:\Windows\System32\winlogon.exe Network Information: Workstation Name: Source Network Address: - Source Port: - Detailed Authentication Information: Logon Process: Advapi Authentication Package: Negotiate Transited Services: - Package Name (NTLM only): - Key Length: 0 This event is generated when a logon session is created. It is generated on the computer that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service such as the Server service, or a local process such as Winlogon.exe or Services.exe. The logon type field indicates the kind of logon that occurred. The most common types are 2 (interactive) and 3 (network). The New Logon fields indicate the account for whom the new logon was created, i.e. the account that was logged on. The network fields indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impersonation level field indicates the extent to which a process in the logon session can impersonate. The authentication information fields provide detailed information about this specific logon request. - Logon GUID is a unique identifier that can be used to correlate this event with a KDC event. - Transited services indicate which intermediate services have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indicates the length of the generated session key. This will be 0 if no session key was requested.
					4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: LTRANPHD$ Account Domain: WORKGROUP Logon ID: 0x3e7 Logon Type: 5 Impersonation Level: %%1833 New Logon: Security ID: S-1-5-19 Account Name: LOCAL SERVICE Account Domain: NT AUTHORITY Logon ID: 0x3e5 Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x238 Process Name:

Security	Audit Success	12544	2015-04-22 19:05:19		Microsoft-Windows-Security-Auditing	C:\Windows\System32\services.exe Network Information: Workstation Name: Source Network Address: - Source Port: - Detailed Authentication Information: Logon Process: Advapi Authentication Package: Negotiate Transited Services: - Package Name (NTLM only): - Key Length: 0 This event is generated when a logon session is created. It is generated on the computer that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service such as the Server service, or a local process such as Winlogon.exe or Services.exe. The logon type field indicates the kind of logon that occurred. The most common types are 2 (interactive) and 3 (network). The New Logon fields indicate the account for whom the new logon was created, i.e. the account that was logged on. The network fields indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impersonation level field indicates the extent to which a process in the logon session can impersonate. The authentication information fields provide detailed information about this specific logon request. - Logon GUID is a unique identifier that can be used to correlate this event with a KDC event. - Transited services indicate which intermediate services have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indicates the length of the generated session key. This will be 0 if no session key was requested.
Security	Audit Success	12544	2015-04-22 19:05:19		Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: LTRANPHD$ Account Domain: WORKGROUP Logon ID: 0x3e7 Logon Type: 5 Impersonation Level: %%1833 New Logon: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Logon ID: 0x3e7 Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x238 Process Name: C:\Windows\System32\services.exe Network Information: Workstation Name: Source Network Address: - Source Port: - Detailed Authentication Information: Logon Process: Advapi Authentication Package: Negotiate Transited Services: - Package Name (NTLM only): - Key Length: 0 This event is generated when a logon session is created. It is generated on the computer that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service such as the Server service, or a local process such as Winlogon.exe or Services.exe. The logon type field indicates the kind of logon that occurred. The most common types are 2 (interactive) and 3 (network). The New Logon fields indicate the account for whom the new logon was created, i.e. the account that was logged on. The network fields indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impersonation level field indicates the extent to which a process in the logon session can impersonate. The authentication information fields provide detailed information about this specific logon request. - Logon GUID is a unique identifier that can be used to correlate this event with a KDC event. - Transited services indicate which intermediate services have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indicates the length of the generated session key. This will be 0 if no session key was requested.
Security	Audit Success	12544	2015-04-22 19:05:19		Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: LTRANPHD$ Account Domain: WORKGROUP Logon ID: 0x3e7 Logon Type: 5 Impersonation Level: %%1833 New Logon: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Logon ID: 0x3e7 Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x238 Process Name: C:\Windows\System32\services.exe Network Information: Workstation Name: Source Network Address: - Source Port: - Detailed Authentication Information: Logon Process: Advapi Authentication Package: Negotiate Transited Services: - Package Name (NTLM only): - Key Length: 0 This event is generated when a logon session is created. It is generated on the computer that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service such as the Server service, or a local process such as Winlogon.exe or Services.exe. The logon type field indicates the kind of logon that occurred. The most common types are 2 (interactive) and 3 (network). The New Logon fields indicate the account for whom the new logon was created, i.e. the account that was logged on. The network fields indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impersonation level field indicates the extent to which a process in the logon session can impersonate. The authentication information fields provide detailed information about this specific logon request. - Logon GUID is a unique identifier that can be used to correlate this event with a KDC event. - Transited services indicate which intermediate services have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indicates the length of the generated session key. This will be 0 if no session key was requested.
Security	Audit Success	12544	2015-04-22 19:05:19		Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: LTRANPHD$ Account Domain: WORKGROUP Logon ID: 0x3e7 Logon Type: 5 Impersonation Level: %%1833 New Logon: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Logon ID: 0x3e7 Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x238 Process Name: C:\Windows\System32\services.exe Network Information: Workstation Name: Source Network Address: - Source Port: - Detailed Authentication Information: Logon Process: Advapi Authentication Package: Negotiate Transited Services: - Package Name (NTLM only): - Key Length: 0 This event is generated when a logon session is created. It is generated on the computer that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service such as the Server service, or a local process such as Winlogon.exe or Services.exe. The logon type field indicates the kind of logon that occurred. The most common types are 2 (interactive) and 3 (network). The New Logon fields indicate the account for whom the new logon was created, i.e. the account that was logged on. The network fields indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impersonation level field indicates the extent to which a process in the logon session can

					impersonate. The authentication information fields provide detailed information about this specific logon request. - Logon GUID is a unique identifier that can be used to correlate this event with a KDC event. - Transited services indicate which intermediate services have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indicates the length of the generated session key. This will be 0 if no session key was requested.
Security	Audit Success	12548	2015-04-22 19:05:19	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-90-1 Account Name: DWM-1 Account Domain: Window Manager Logon ID: 0xdd65 Privileges: SeAssignPrimaryTokenPrivilege SeAuditPrivilege SeImpersonatePrivilege
Security	Audit Success	12548	2015-04-22 19:05:19	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-90-1 Account Name: DWM-1 Account Domain: Window Manager Logon ID: 0xdd7f Privileges: SeAssignPrimaryTokenPrivilege SeAuditPrivilege
Security	Audit Success	12548	2015-04-22 19:05:19	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-19 Account Name: LOCAL SERVICE Account Domain: NT AUTHORITY Logon ID: 0x3e5 Privileges: SeAssignPrimaryTokenPrivilege SeAuditPrivilege SeImpersonatePrivilege
Security	Audit Success	12548	2015-04-22 19:05:19	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Logon ID: 0x3e7 Privileges: SeAssignPrimaryTokenPrivilege SeTcbPrivilege SeSecurityPrivilege SeTakeOwnershipPrivilege SeLoadDriverPrivilege SeBackupPrivilege SeRestorePrivilege SeDebugPrivilege SeAuditPrivilege SeSystemEnvironmentPrivilege SeImpersonatePrivilege
Security	Audit Success	12548	2015-04-22 19:05:19	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Logon ID: 0x3e7 Privileges: SeAssignPrimaryTokenPrivilege SeTcbPrivilege SeSecurityPrivilege SeTakeOwnershipPrivilege SeLoadDriverPrivilege SeBackupPrivilege SeRestorePrivilege SeDebugPrivilege SeAuditPrivilege SeSystemEnvironmentPrivilege SeImpersonatePrivilege
Security	Audit Success	12548	2015-04-22 19:05:19	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Logon ID: 0x3e7 Privileges: SeAssignPrimaryTokenPrivilege SeTcbPrivilege SeSecurityPrivilege SeTakeOwnershipPrivilege SeLoadDriverPrivilege SeBackupPrivilege SeRestorePrivilege SeDebugPrivilege SeAuditPrivilege SeSystemEnvironmentPrivilege SeImpersonatePrivilege
Security	Audit Success	12292	2015-04-22 19:05:20	Microsoft-Windows-Security-Auditing	5033: The Windows Firewall Driver started successfully.
Security	Audit Success	12292	2015-04-22 19:05:20	Microsoft-Windows-Security-Auditing	5024: The Windows Firewall service started successfully.
Security	Audit Success	12544	2015-04-22 19:05:20	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: LTRANPHD$ Account Domain: WORKGROUP Logon ID: 0x3e7 Logon Type: 5 Impersonation Level: %%1833 New Logon: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Logon ID: 0x3e7 Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x238 Process Name: C:\Windows\System32\services.exe Network Information: Workstation Name: Source Network Address: - Source Port: - Detailed Authentication Information: Logon Process: Advapi Authentication Package: Negotiate Transited Services: - Package Name (NTLM only): - Key Length: 0 This event is generated when a logon session is created. It is generated on the computer that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service such as the Server service, or a local process such as Winlogon.exe or Services.exe. The logon type field indicates the kind of logon that occurred. The most common types are 2 (interactive) and 3 (network). The New Logon fields indicate the account for whom the new logon was created, i.e. the account that was logged on. The network fields indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impersonation level field indicates the extent to which a process in the logon session can impersonate. The authentication information fields provide detailed information about this specific logon request. - Logon GUID is a unique identifier that can be used to correlate this event with a KDC event. - Transited services indicate which intermediate services have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indicates the length of the generated session key. This will be 0 if no session key was requested.
Security	Audit Success	12544	2015-04-22 19:05:20	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: LTRANPHD$ Account Domain: WORKGROUP Logon ID: 0x3e7 Logon Type: 5 Impersonation Level: %%1833 New Logon: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Logon ID: 0x3e7 Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x238 Process Name: C:\Windows\System32\services.exe Network Information: Workstation Name: Source Network Address: - Source Port: - Detailed Authentication Information: Logon Process: Advapi Authentication Package: Negotiate Transited Services: - Package Name (NTLM only): - Key Length: 0 This event is generated when a logon session is created. It is generated on the computer that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service such as the Server service, or a local process such as Winlogon.exe or Services.exe. The logon type field indicates the kind of logon that occurred. The most common types are 2 (interactive) and 3 (network). The New Logon fields indicate the account for whom the new logon was created, i.e. the account that was logged on. The network fields indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impersonation level field indicates the extent to which a process in the logon session can

						impersonate. The authentication information fields provide detailed information about this specific logon request. - Logon GUID is a unique identifier that can be used to correlate this event with a KDC event. - Transited services indicate which intermediate services have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indicates the length of the generated session key. This will be 0 if no session key was requested.
Security	Audit Success	12544	2015-04-22 19:05:20		Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: LTRANPHD$ Account Domain: WORKGROUP Logon ID: 0x3e7 Logon Type: 5 Impersonation Level: %%1833 New Logon: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Logon ID: 0x3e7 Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x238 Process Name: C:\Windows\System32\services.exe Network Information: Workstation Name: Source Network Address: - Source Port: - Detailed Authentication Information: Logon Process: Advapi Authentication Package: Negotiate Transited Services: - Package Name (NTLM only): - Key Length: 0 This event is generated when a logon session is created. It is generated on the computer that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service such as the Server service, or a local process such as Winlogon.exe or Services.exe. The logon type field indicates the kind of logon that occurred. The most common types are 2 (interactive) and 3 (network). The New Logon fields indicate the account for whom the new logon was created, i.e. the account that was logged on. The network fields indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impersonation level field indicates the extent to which a process in the logon session can impersonate. The authentication information fields provide detailed information about this specific logon request. - Logon GUID is a unique identifier that can be used to correlate this event with a KDC event. - Transited services indicate which intermediate services have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indicates the length of the generated session key. This will be 0 if no session key was requested.
Security	Audit Success	12544	2015-04-22 19:05:20		Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-0-0 Account Name: - Account Domain: - Logon ID: 0x0 Logon Type: 3 Impersonation Level: %%1833 New Logon: Security ID: S-1-5-7 Account Name: ANONYMOUS LOGON Account Domain: NT AUTHORITY Logon ID: 0x175ae Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x0 Process Name: - Network Information: Workstation Name: Source Network Address: - Source Port: - Detailed Authentication Information: Logon Process: NtLmSsp Authentication Package: NTLM Transited Services: - Package Name (NTLM only): NTLM V1 Key Length: 0 This event is generated when a logon session is created. It is generated on the computer that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service such as the Server service, or a local process such as Winlogon.exe or Services.exe. The logon type field indicates the kind of logon that occurred. The most common types are 2 (interactive) and 3 (network). The New Logon fields indicate the account for whom the new logon was created, i.e. the account that was logged on. The network fields indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impersonation level field indicates the extent to which a process in the logon session can impersonate. The authentication information fields provide detailed information about this specific logon request. - Logon GUID is a unique identifier that can be used to correlate this event with a KDC event. - Transited services indicate which intermediate services have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indicates the length of the generated session key. This will be 0 if no session key was requested.
Security	Audit Success	12548	2015-04-22 19:05:20		Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Logon ID: 0x3e7 Privileges: SeAssignPrimaryTokenPrivilege SeTcbPrivilege SeSecurityPrivilege SeTakeOwnershipPrivilege SeLoadDriverPrivilege SeBackupPrivilege SeRestorePrivilege SeDebugPrivilege SeAuditPrivilege SeSystemEnvironmentPrivilege SeImpersonatePrivilege
Security	Audit Success	12548	2015-04-22 19:05:20		Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Logon ID: 0x3e7 Privileges: SeAssignPrimaryTokenPrivilege SeTcbPrivilege SeSecurityPrivilege SeTakeOwnershipPrivilege SeLoadDriverPrivilege SeBackupPrivilege SeRestorePrivilege SeDebugPrivilege SeAuditPrivilege SeSystemEnvironmentPrivilege SeImpersonatePrivilege
Security	Audit Success	12548	2015-04-22 19:05:20		Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Logon ID: 0x3e7 Privileges: SeAssignPrimaryTokenPrivilege SeTcbPrivilege SeSecurityPrivilege SeTakeOwnershipPrivilege SeLoadDriverPrivilege SeBackupPrivilege SeRestorePrivilege SeDebugPrivilege SeAuditPrivilege SeSystemEnvironmentPrivilege SeImpersonatePrivilege
Security	Audit Success	12544	2015-04-22 19:05:30		Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: LTRANPHD$ Account Domain: WORKGROUP Logon ID: 0x3e7 Logon Type: 5 Impersonation Level: %%1833 New Logon: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Logon ID: 0x3e7 Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x238 Process Name: C:\Windows\System32\services.exe Network Information: Workstation Name: Source Network Address: - Source Port: - Detailed Authentication Information: Logon Process: Advapi Authentication Package: Negotiate Transited Services: - Package Name (NTLM only): - Key Length: 0 This event is generated when a logon session is created. It is generated on the computer that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service such as the Server service, or a local process such as Winlogon.exe or Services.exe. The logon type field indicates the kind of logon that occurred. The most common types are 2 (interactive) and 3 (network). The New Logon fields indicate the account for whom the new logon was created, i.e. the account that was logged on. The network fields indicate where a

					remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impersonation level field indicates the extent to which a process in the logon session can impersonate. The authentication information fields provide detailed information about this specific logon request. - Logon GUID is a unique identifier that can be used to correlate this event with a KDC event. - Transited services indicate which intermediate services have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indicates the length of the generated session key. This will be 0 if no session key was requested.
	Security	Audit Success	12548	2015-04-22 19:05:30	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Logon ID: 0x3e7 Privileges: SeAssignPrimaryTokenPrivilege SeTcbPrivilege SeSecurityPrivilege SeTakeOwnershipPrivilege SeLoadDriverPrivilege SeBackupPrivilege SeRestorePrivilege SeDebugPrivilege SeAuditPrivilege SeSystemEnvironmentPrivilege SeImpersonatePrivilege
	Security	Audit Success	12544	2015-04-22 19:07:22	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: LTRANPHD$ Account Domain: WORKGROUP Logon ID: 0x3e7 Logon Type: 5 Impersonation Level: %%1833 New Logon: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Logon ID: 0x3e7 Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x238 Process Name: C:\Windows\System32\services.exe Network Information: Workstation Name: Source Network Address: - Source Port: - Detailed Authentication Information: Logon Process: Advapi Authentication Package: Negotiate Transited Services: - Package Name (NTLM only): - Key Length: 0 This event is generated when a logon session is created. It is generated on the computer that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service such as the Server service, or a local process such as Winlogon.exe or Services.exe. The logon type field indicates the kind of logon that occurred. The most common types are 2 (interactive) and 3 (network). The New Logon fields indicate the account for whom the new logon was created, i.e. the account that was logged on. The network fields indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impersonation level field indicates the extent to which a process in the logon session can impersonate. The authentication information fields provide detailed information about this specific logon request. - Logon GUID is a unique identifier that can be used to correlate this event with a KDC event. - Transited services indicate which intermediate services have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indicates the length of the generated session key. This will be 0 if no session key was requested.
	Security	Audit Success	12544	2015-04-22 19:07:22	Microsoft-Windows-Security-Auditing	4648: A logon was attempted using explicit credentials. Subject: Security ID: S-1-5-18 Account Name: LTRANPHD$ Account Domain: WORKGROUP Logon ID: 0x3e7 Logon GUID: {00000000-0000-0000-0000-000000000000} Account Whose Credentials Were Used: Account Name: Liem Account Domain: LTRANPHD Logon GUID: {00000000-0000-0000-0000-000000000000} Target Server: Target Server Name: localhost Additional Information: localhost Process Information: Process ID: 0x210 Process Name: C:\Windows\System32\winlogon.exe Network Information: Network Address: 127.0.0.1 Port: 0 This event is generated when a process attempts to log on an account by explicitly specifying that account's credentials. This most commonly occurs in batch-type configurations such as scheduled tasks, or when using the RUNAS command.
	Security	Audit Success	12544	2015-04-22 19:07:22	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: LTRANPHD$ Account Domain: WORKGROUP Logon ID: 0x3e7 Logon Type: 2 Impersonation Level: %%1833 New Logon: Security ID: S-1-5-21-1888849264-3803429180-4108621888-1001 Account Name: Liem Account Domain: LTRANPHD Logon ID: 0x136a41 Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x210 Process Name: C:\Windows\System32\winlogon.exe Network Information: Workstation Name: LTRANPHD Source Network Address: 127.0.0.1 Source Port: 0 Detailed Authentication Information: Logon Process: User32 Authentication Package: Negotiate Transited Services: - Package Name (NTLM only): - Key Length: 0 This event is generated when a logon session is created. It is generated on the computer that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service such as the Server service, or a local process such as Winlogon.exe or Services.exe. The logon type field indicates the kind of logon that occurred. The most common types are 2 (interactive) and 3 (network). The New Logon fields indicate the account for whom the new logon was created, i.e. the account that was logged on. The network fields indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impersonation level field indicates the extent to which a process in the logon session can impersonate. The authentication information fields provide detailed information about this specific logon request. - Logon GUID is a unique identifier that can be used to correlate this event with a KDC event. - Transited services indicate which intermediate services have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indicates the length of the generated session key. This will be 0 if no session key was requested.
						4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: LTRANPHD$ Account Domain: WORKGROUP Logon ID: 0x3e7 Logon Type: 2 Impersonation Level: %%1833 New Logon: Security ID: S-1-5-21-1888849264-3803429180-4108621888-1001 Account Name: Liem Account Domain: LTRANPHD Logon ID: 0x136a63 Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x210 Process Name: C:\Windows\System32\winlogon.exe Network Information: Workstation Name: LTRANPHD Source Network Address: 127.0.0.1 Source Port: 0 Detailed Authentication Information: Logon Process: User32 Authentication Package: Negotiate Transited Services: - Package Name

Security	Audit Success	12544	2015-04-22 19:07:22	Microsoft-Windows-Security-Auditing	(NTLM only): - Key Length: 0 This event is generated when a logon session is created. It is generated on the computer that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service such as the Server service, or a local process such as Winlogon.exe or Services.exe. The logon type field indicates the kind of logon that occurred. The most common types are 2 (interactive) and 3 (network). The New Logon fields indicate the account for whom the new logon was created, i.e. the account that was logged on. The network fields indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impersonation level field indicates the extent to which a process in the logon session can impersonate. The authentication information fields provide detailed information about this specific logon request. - Logon GUID is a unique identifier that can be used to correlate this event with a KDC event. - Transited services indicate which intermediate services have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indicates the length of the generated session key. This will be 0 if no session key was requested.
Security	Audit Success	12548	2015-04-22 19:07:22	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Logon ID: 0x3e7 Privileges: SeAssignPrimaryTokenPrivilege SeTcbPrivilege SeSecurityPrivilege SeTakeOwnershipPrivilege SeLoadDriverPrivilege SeBackupPrivilege SeRestorePrivilege SeDebugPrivilege SeAuditPrivilege SeSystemEnvironmentPrivilege SeImpersonatePrivilege
Security	Audit Success	12548	2015-04-22 19:07:22	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-21-1888849264-3803429180-4108621888-1001 Account Name: Liem Account Domain: LTRANPHD Logon ID: 0x136a41 Privileges: SeSecurityPrivilege SeTakeOwnershipPrivilege SeLoadDriverPrivilege SeBackupPrivilege SeRestorePrivilege SeDebugPrivilege SeSystemEnvironmentPrivilege SeImpersonatePrivilege
Security	Audit Success	13824	2015-04-22 19:07:24	Microsoft-Windows-Security-Auditing	4797: An attempt was made to query the existence of a blank password for an account. Subject: Security ID: S-1-5-19 Account Name: LOCAL SERVICE Account Domain: NT AUTHORITY Logon ID: 0x3e5 Additional Information: Caller Workstation: LTRANPHD Target Account Name: Administrator Target Account Domain: LTRANPHD
Security	Audit Success	13824	2015-04-22 19:07:24	Microsoft-Windows-Security-Auditing	4797: An attempt was made to query the existence of a blank password for an account. Subject: Security ID: S-1-5-19 Account Name: LOCAL SERVICE Account Domain: NT AUTHORITY Logon ID: 0x3e5 Additional Information: Caller Workstation: LTRANPHD Target Account Name: Guest Target Account Domain: LTRANPHD
Security	Audit Success	13824	2015-04-22 19:07:24	Microsoft-Windows-Security-Auditing	4797: An attempt was made to query the existence of a blank password for an account. Subject: Security ID: S-1-5-19 Account Name: LOCAL SERVICE Account Domain: NT AUTHORITY Logon ID: 0x3e5 Additional Information: Caller Workstation: LTRANPHD Target Account Name: Liem Target Account Domain: LTRANPHD
Security	Audit Success	13824	2015-04-22 19:07:24	Microsoft-Windows-Security-Auditing	4797: An attempt was made to query the existence of a blank password for an account. Subject: Security ID: S-1-5-19 Account Name: LOCAL SERVICE Account Domain: NT AUTHORITY Logon ID: 0x3e5 Additional Information: Caller Workstation: LTRANPHD Target Account Name: Liem Target Account Domain: LTRANPHD
Security	Audit Success	13824	2015-04-22 19:07:24	Microsoft-Windows-Security-Auditing	4797: An attempt was made to query the existence of a blank password for an account. Subject: Security ID: S-1-5-19 Account Name: LOCAL SERVICE Account Domain: NT AUTHORITY Logon ID: 0x3e5 Additional Information: Caller Workstation: LTRANPHD Target Account Name: Administrator Target Account Domain: LTRANPHD
Security	Audit Success	13824	2015-04-22 19:07:24	Microsoft-Windows-Security-Auditing	4797: An attempt was made to query the existence of a blank password for an account. Subject: Security ID: S-1-5-19 Account Name: LOCAL SERVICE Account Domain: NT AUTHORITY Logon ID: 0x3e5 Additional Information: Caller Workstation: LTRANPHD Target Account Name: Guest Target Account Domain: LTRANPHD
Security	Audit Success	13824	2015-04-22 19:07:24	Microsoft-Windows-Security-Auditing	4797: An attempt was made to query the existence of a blank password for an account. Subject: Security ID: S-1-5-19 Account Name: LOCAL SERVICE Account Domain: NT AUTHORITY Logon ID: 0x3e5 Additional Information: Caller Workstation: LTRANPHD Target Account Name: Liem Target Account Domain: LTRANPHD
Security	Audit Success	13824	2015-04-22 19:07:24	Microsoft-Windows-Security-Auditing	4797: An attempt was made to query the existence of a blank password for an account. Subject: Security ID: S-1-5-19 Account Name: LOCAL SERVICE Account Domain: NT AUTHORITY Logon ID: 0x3e5 Additional Information: Caller Workstation: LTRANPHD Target Account Name: Administrator Target Account Domain: LTRANPHD
Security	Audit Success	13824	2015-04-22 19:07:24	Microsoft-Windows-Security-Auditing	4797: An attempt was made to query the existence of a blank password for an account. Subject: Security ID: S-1-5-19 Account Name: LOCAL SERVICE Account Domain: NT AUTHORITY Logon ID: 0x3e5 Additional Information: Caller Workstation: LTRANPHD Target Account Name: Liem Target Account Domain: LTRANPHD
Security	Audit Success	13824	2015-04-22 19:07:25	Microsoft-Windows-Security-Auditing	4797: An attempt was made to query the existence of a blank password for an account. Subject: Security ID: S-1-5-19 Account Name: LOCAL SERVICE Account Domain: NT AUTHORITY Logon ID: 0x3e5 Additional Information: Caller Workstation: LTRANPHD Target Account Name: Administrator Target Account Domain: LTRANPHD
Security	Audit Success	13824	2015-04-22 19:07:25	Microsoft-Windows-Security-Auditing	4797: An attempt was made to query the existence of a blank password for an account. Subject: Security ID: S-1-5-19 Account Name: LOCAL SERVICE Account Domain: NT AUTHORITY Logon ID: 0x3e5 Additional Information: Caller Workstation: LTRANPHD Target Account Name: Guest Target Account Domain: LTRANPHD
Security	Audit Success	13824	2015-04-22 19:07:25	Microsoft-Windows-Security-Auditing	4797: An attempt was made to query the existence of a blank password for an account. Subject: Security ID: S-1-5-19 Account Name: LOCAL SERVICE Account Domain: NT AUTHORITY Logon ID: 0x3e5 Additional Information: Caller Workstation: LTRANPHD Target Account Name: Liem Target Account Domain: LTRANPHD
Security	Audit Success	13824	2015-04-22 19:07:25	Microsoft-Windows-Security-Auditing	4797: An attempt was made to query the existence of a blank password for an account. Subject: Security ID: S-1-5-19 Account Name: LOCAL SERVICE Account Domain: NT AUTHORITY Logon ID: 0x3e5 Additional Information: Caller Workstation: LTRANPHD Target Account Name: Liem Target Account Domain: LTRANPHD

Security	Audit Success	13824	2015-04-22 19:07:25	Microsoft-Windows-Security-Auditing	4797: An attempt was made to query the existence of a blank password for an account. Subject: Security ID: S-1-5-19 Account Name: LOCAL SERVICE Account Domain: NT AUTHORITY Logon ID: 0x3e5 Additional Information: Caller Workstation: LTRANPHD Target Account Name: Administrator Target Account Domain: LTRANPHD
Security	Audit Success	13824	2015-04-22 19:07:25	Microsoft-Windows-Security-Auditing	4797: An attempt was made to query the existence of a blank password for an account. Subject: Security ID: S-1-5-19 Account Name: LOCAL SERVICE Account Domain: NT AUTHORITY Logon ID: 0x3e5 Additional Information: Caller Workstation: LTRANPHD Target Account Name: Guest Target Account Domain: LTRANPHD
Security	Audit Success	13824	2015-04-22 19:07:25	Microsoft-Windows-Security-Auditing	4797: An attempt was made to query the existence of a blank password for an account. Subject: Security ID: S-1-5-19 Account Name: LOCAL SERVICE Account Domain: NT AUTHORITY Logon ID: 0x3e5 Additional Information: Caller Workstation: LTRANPHD Target Account Name: Liem Target Account Domain: LTRANPHD
Security	Audit Success	13824	2015-04-22 19:07:25	Microsoft-Windows-Security-Auditing	4797: An attempt was made to query the existence of a blank password for an account. Subject: Security ID: S-1-5-19 Account Name: LOCAL SERVICE Account Domain: NT AUTHORITY Logon ID: 0x3e5 Additional Information: Caller Workstation: LTRANPHD Target Account Name: Liem Target Account Domain: LTRANPHD
Security	Audit Success	13824	2015-04-22 19:07:25	Microsoft-Windows-Security-Auditing	4797: An attempt was made to query the existence of a blank password for an account. Subject: Security ID: S-1-5-21-1888849264-3803429180-4108621888-1001 Account Name: Liem Account Domain: LTRANPHD Logon ID: 0x136a63 Additional Information: Caller Workstation: LTRANPHD Target Account Name: Administrator Target Account Domain: LTRANPHD
Security	Audit Success	13824	2015-04-22 19:07:25	Microsoft-Windows-Security-Auditing	4797: An attempt was made to query the existence of a blank password for an account. Subject: Security ID: S-1-5-21-1888849264-3803429180-4108621888-1001 Account Name: Liem Account Domain: LTRANPHD Logon ID: 0x136a63 Additional Information: Caller Workstation: LTRANPHD Target Account Name: Guest Target Account Domain: LTRANPHD
Security	Audit Success	13824	2015-04-22 19:07:25	Microsoft-Windows-Security-Auditing	4797: An attempt was made to query the existence of a blank password for an account. Subject: Security ID: S-1-5-21-1888849264-3803429180-4108621888-1001 Account Name: Liem Account Domain: LTRANPHD Logon ID: 0x136a63 Additional Information: Caller Workstation: LTRANPHD Target Account Name: Administrator Target Account Domain: LTRANPHD
Security	Audit Success	13824	2015-04-22 19:07:25	Microsoft-Windows-Security-Auditing	4797: An attempt was made to query the existence of a blank password for an account. Subject: Security ID: S-1-5-21-1888849264-3803429180-4108621888-1001 Account Name: Liem Account Domain: LTRANPHD Logon ID: 0x136a63 Additional Information: Caller Workstation: LTRANPHD Target Account Name: Guest Target Account Domain: LTRANPHD
Security	Audit Success	12544	2015-04-22 19:08:33	Microsoft-Windows-Security-Auditing	4648: A logon was attempted using explicit credentials. Subject: Security ID: S-1-5-21-1888849264-3803429180-4108621888-1001 Account Name: Liem Account Domain: LTRANPHD Logon ID: 0x136a63 Logon GUID: {00000000-0000-0000-0000-000000000000} Account Whose Credentials Were Used: Account Name: admin Account Domain: LTRANPHD Logon GUID: {00000000-0000-0000-0000-000000000000} Target Server: Target Server Name: Community Additional Information: Community Process Information: Process ID: 0x4 Process Name: Network Information: Network Address: - Port: - This event is generated when a process attempts to log on an account by explicitly specifying that account's credentials. This most commonly occurs in batch-type configurations such as scheduled tasks, or when using the RUNAS command.
Security	Audit Success	12544	2015-04-22 19:13:23	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: LTRANPHD$ Account Domain: WORKGROUP Logon ID: 0x3e7 Logon Type: 5 Impersonation Level: %%1833 New Logon: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Logon ID: 0x3e7 Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x238 Process Name: C:\Windows\System32\services.exe Network Information: Workstation Name: Source Network Address: - Source Port: - Detailed Authentication Information: Logon Process: Advapi Authentication Package: Negotiate Transited Services: - Package Name (NTLM only): - Key Length: 0 This event is generated when a logon session is created. It is generated on the computer that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service such as the Server service, or a local process such as Winlogon.exe or Services.exe. The logon type field indicates the kind of logon that occurred. The most common types are 2 (interactive) and 3 (network). The New Logon fields indicate the account for whom the new logon was created, i.e. the account that was logged on. The network fields indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impersonation level field indicates the extent to which a process in the logon session can impersonate. The authentication information fields provide detailed information about this specific logon request. - Logon GUID is a unique identifier that can be used to correlate this event with a KDC event. - Transited services indicate which intermediate services have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indicates the length of the generated session key. This will be 0 if no session key was requested.
	Audit		2015-04-	Microsoft-Windows-Security-	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: LTRANPHD$ Account Domain: WORKGROUP Logon ID: 0x3e7 Logon Type: 5 Impersonation Level: %%1833 New Logon: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Logon ID: 0x3e7 Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x238 Process Name: C:\Windows\System32\services.exe Network Information: Workstation Name: Source Network Address: - Source Port: - Detailed Authentication Information: Logon Process: Advapi Authentication Package: Negotiate Transited Services: - Package Name (NTLM only): - Key Length: 0 This event is generated when a logon session is created. It is generated on the computer that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service such as the Server service, or a local

Security	Success	12544	22 19:13:23	Auditing	process such as Winlogon.exe or Services.exe. The logon type field indicates the kind of logon that occurred. The most common types are 2 (interactive) and 3 (network). The New Logon fields indicate the account for whom the new logon was created, i.e. the account that was logged on. The network fields indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impersonation level field indicates the extent to which a process in the logon session can impersonate. The authentication information fields provide detailed information about this specific logon request. - Logon GUID is a unique identifier that can be used to correlate this event with a KDC event. - Transited services indicate which intermediate services have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indicates the length of the generated session key. This will be 0 if no session key was requested.
Security	Audit Success	12548	2015-04-22 19:13:23	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Logon ID: 0x3e7 Privileges: SeAssignPrimaryTokenPrivilege SeTcbPrivilege SeSecurityPrivilege SeTakeOwnershipPrivilege SeLoadDriverPrivilege SeBackupPrivilege SeRestorePrivilege SeDebugPrivilege SeAuditPrivilege SeSystemEnvironmentPrivilege SeImpersonatePrivilege
Security	Audit Success	12548	2015-04-22 19:13:23	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Logon ID: 0x3e7 Privileges: SeAssignPrimaryTokenPrivilege SeTcbPrivilege SeSecurityPrivilege SeTakeOwnershipPrivilege SeLoadDriverPrivilege SeBackupPrivilege SeRestorePrivilege SeDebugPrivilege SeAuditPrivilege SeSystemEnvironmentPrivilege SeImpersonatePrivilege
Security	Audit Success	13824	2015-04-22 19:18:20	Microsoft-Windows-Security-Auditing	4797: An attempt was made to query the existence of a blank password for an account. Subject: Security ID: S-1-5-21-1888849264-3803429180-4108621888-1001 Account Name: Liem Account Domain: LTRANPHD Logon ID: 0x136a63 Additional Information: Caller Workstation: LTRANPHD Target Account Name: Administrator Target Account Domain: LTRANPHD
Security	Audit Success	12544	2015-04-22 19:21:53	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: LTRANPHD$ Account Domain: WORKGROUP Logon ID: 0x3e7 Logon Type: 5 Impersonation Level: %%1833 New Logon: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Logon ID: 0x3e7 Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x238 Process Name: C:\Windows\System32\services.exe Network Information: Workstation Name: Source Network Address: - Source Port: - Detailed Authentication Information: Logon Process: Advapi Authentication Package: Negotiate Transited Services: - Package Name (NTLM only): - Key Length: 0 This event is generated when a logon session is created. It is generated on the computer that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service such as the Server service, or a local process such as Winlogon.exe or Services.exe. The logon type field indicates the kind of logon that occurred. The most common types are 2 (interactive) and 3 (network). The New Logon fields indicate the account for whom the new logon was created, i.e. the account that was logged on. The network fields indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impersonation level field indicates the extent to which a process in the logon session can impersonate. The authentication information fields provide detailed information about this specific logon request. - Logon GUID is a unique identifier that can be used to correlate this event with a KDC event. - Transited services indicate which intermediate services have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indicates the length of the generated session key. This will be 0 if no session key was requested.
Security	Audit Success	12548	2015-04-22 19:21:53	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Logon ID: 0x3e7 Privileges: SeAssignPrimaryTokenPrivilege SeTcbPrivilege SeSecurityPrivilege SeTakeOwnershipPrivilege SeLoadDriverPrivilege SeBackupPrivilege SeRestorePrivilege SeDebugPrivilege SeAuditPrivilege SeSystemEnvironmentPrivilege SeImpersonatePrivilege
Security	Audit Success	12544	2015-04-22 19:21:57	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: LTRANPHD$ Account Domain: WORKGROUP Logon ID: 0x3e7 Logon Type: 5 Impersonation Level: %%1833 New Logon: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Logon ID: 0x3e7 Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x238 Process Name: C:\Windows\System32\services.exe Network Information: Workstation Name: Source Network Address: - Source Port: - Detailed Authentication Information: Logon Process: Advapi Authentication Package: Negotiate Transited Services: - Package Name (NTLM only): - Key Length: 0 This event is generated when a logon session is created. It is generated on the computer that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service such as the Server service, or a local process such as Winlogon.exe or Services.exe. The logon type field indicates the kind of logon that occurred. The most common types are 2 (interactive) and 3 (network). The New Logon fields indicate the account for whom the new logon was created, i.e. the account that was logged on. The network fields indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impersonation level field indicates the extent to which a process in the logon session can impersonate. The authentication information fields provide detailed information about this specific logon request. - Logon GUID is a unique identifier that can be used to correlate this event with a KDC event. - Transited services indicate which intermediate services have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indicates the length of the generated session key. This will be 0 if no session key was requested.
					4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: LTRANPHD$ Account Domain: WORKGROUP Logon ID: 0x3e7 Logon Type: 5 Impersonation Level: %%1833 New Logon:

Security	Audit Success	12544	2015-04-22 19:21:57	Microsoft-Windows-Security-Auditing	Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Logon ID: 0x3e7 Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x238 Process Name: C:\Windows\System32\services.exe Network Information: Workstation Name: Source Network Address: - Source Port: - Detailed Authentication Information: Logon Process: Advapi Authentication Package: Negotiate Transited Services: - Package Name (NTLM only): - Key Length: 0 This event is generated when a logon session is created. It is generated on the computer that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service such as the Server service, or a local process such as Winlogon.exe or Services.exe. The logon type field indicates the kind of logon that occurred. The most common types are 2 (interactive) and 3 (network). The New Logon fields indicate the account for whom the new logon was created, i.e. the account that was logged on. The network fields indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impersonation level field indicates the extent to which a process in the logon session can impersonate. The authentication information fields provide detailed information about this specific logon request. - Logon GUID is a unique identifier that can be used to correlate this event with a KDC event. - Transited services indicate which intermediate services have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indicates the length of the generated session key. This will be 0 if no session key was requested.
Security	Audit Success	12548	2015-04-22 19:21:57	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Logon ID: 0x3e7 Privileges: SeAssignPrimaryTokenPrivilege SeTcbPrivilege SeSecurityPrivilege SeTakeOwnershipPrivilege SeLoadDriverPrivilege SeBackupPrivilege SeRestorePrivilege SeDebugPrivilege SeAuditPrivilege SeSystemEnvironmentPrivilege SeImpersonatePrivilege
Security	Audit Success	12548	2015-04-22 19:21:57	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Logon ID: 0x3e7 Privileges: SeAssignPrimaryTokenPrivilege SeTcbPrivilege SeSecurityPrivilege SeTakeOwnershipPrivilege SeLoadDriverPrivilege SeBackupPrivilege SeRestorePrivilege SeDebugPrivilege SeAuditPrivilege SeSystemEnvironmentPrivilege SeImpersonatePrivilege
Security	Audit Success	103	2015-04-22 19:30:54	Microsoft-Windows-Eventlog	1100: The event logging service has shut down.
Security	Audit Success	12545	2015-04-22 19:30:54	Microsoft-Windows-Security-Auditing	4647: User initiated logoff: Subject: Security ID: S-1-5-21-1888849264-3803429180-4108621888-1001 Account Name: Liem Account Domain: LTRANPHD Logon ID: 0x136a63 This event is generated when a logoff is initiated. No further user-initiated activity can occur. This event can be interpreted as a logoff event.
Security	Audit Success	12288	2015-04-22 19:47:35	Microsoft-Windows-Security-Auditing	4608: Windows is starting up. This event is logged when LSASS.EXE starts and the auditing subsystem is initialized.
Security	Audit Success	12544	2015-04-22 19:47:35	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-0-0 Account Name: - Account Domain: - Logon ID: 0x0 Logon Type: 0 Impersonation Level: - New Logon: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Logon ID: 0x3e7 Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x4 Process Name: Network Information: Workstation Name: - Source Network Address: - Source Port: - Detailed Authentication Information: Logon Process: - Authentication Package: - Transited Services: - Package Name (NTLM only): - Key Length: 0 This event is generated when a logon session is created. It is generated on the computer that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service such as the Server service, or a local process such as Winlogon.exe or Services.exe. The logon type field indicates the kind of logon that occurred. The most common types are 2 (interactive) and 3 (network). The New Logon fields indicate the account for whom the new logon was created, i.e. the account that was logged on. The network fields indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impersonation level field indicates the extent to which a process in the logon session can impersonate. The authentication information fields provide detailed information about this specific logon request. - Logon GUID is a unique identifier that can be used to correlate this event with a KDC event. - Transited services indicate which intermediate services have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indicates the length of the generated session key. This will be 0 if no session key was requested.
Security	Audit Success	13568	2015-04-22 19:47:36	Microsoft-Windows-Security-Auditing	4902: The Per-user audit policy table was created. Number of Elements: 0 Policy ID: 0x7415
Security	Audit Success	12544	2015-04-22 19:47:38	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: LTRANPHD$ Account Domain: WORKGROUP Logon ID: 0x3e7 Logon Type: 5 Impersonation Level: %%1833 New Logon: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Logon ID: 0x3e7 Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x22c Process Name: C:\Windows\System32\services.exe Network Information: Workstation Name: Source Network Address: - Source Port: - Detailed Authentication Information: Logon Process: Advapi Authentication Package: Negotiate Transited Services: - Package Name (NTLM only): - Key Length: 0 This event is generated when a logon session is created. It is generated on the computer that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service such as the Server service, or a local process such as Winlogon.exe or Services.exe. The logon type field indicates the kind of logon that occurred. The most common types are 2 (interactive) and 3 (network). The New Logon fields indicate the account for

					whom the new logon was created, i.e. the account that was logged on. The network fields indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impersonation level field indicates the extent to which a process in the logon session can impersonate. The authentication information fields provide detailed information about this specific logon request. - Logon GUID is a unique identifier that can be used to correlate this event with a KDC event. - Transited services indicate which intermediate services have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indicates the length of the generated session key. This will be 0 if no session key was requested.
Security	Audit Success	12544	2015-04-22 19:47:38	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: LTRANPHD$ Account Domain: WORKGROUP Logon ID: 0x3e7 Logon Type: 5 Impersonation Level: %%1833 New Logon: Security ID: S-1-5-20 Account Name: NETWORK SERVICE Account Domain: NT AUTHORITY Logon ID: 0x3e4 Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x22c Process Name: C:\Windows\System32\services.exe Network Information: Workstation Name: Source Network Address: - Source Port: - Detailed Authentication Information: Logon Process: Advapi Authentication Package: Negotiate Transited Services: - Package Name (NTLM only): - Key Length: 0 This event is generated when a logon session is created. It is generated on the computer that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service such as the Server service, or a local process such as Winlogon.exe or Services.exe. The logon type field indicates the kind of logon that occurred. The most common types are 2 (interactive) and 3 (network). The New Logon fields indicate the account for whom the new logon was created, i.e. the account that was logged on. The network fields indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impersonation level field indicates the extent to which a process in the logon session can impersonate. The authentication information fields provide detailed information about this specific logon request. - Logon GUID is a unique identifier that can be used to correlate this event with a KDC event. - Transited services indicate which intermediate services have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indicates the length of the generated session key. This will be 0 if no session key was requested.
Security	Audit Success	12544	2015-04-22 19:47:38	Microsoft-Windows-Security-Auditing	4648: A logon was attempted using explicit credentials. Subject: Security ID: S-1-5-18 Account Name: LTRANPHD$ Account Domain: WORKGROUP Logon ID: 0x3e7 Logon GUID: {00000000-0000-0000-0000-000000000000} Account Whose Credentials Were Used: Account Name: DWM-1 Account Domain: Window Manager Logon GUID: {00000000-0000-0000-0000-000000000000} Target Server: Target Server Name: localhost Additional Information: localhost Process Information: Process ID: 0x1fc Process Name: C:\Windows\System32\winlogon.exe Network Information: Network Address: - Port: - This event is generated when a process attempts to log on an account by explicitly specifying that account's credentials. This most commonly occurs in batch-type configurations such as scheduled tasks, or when using the RUNAS command.
Security	Audit Success	12544	2015-04-22 19:47:38	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: LTRANPHD$ Account Domain: WORKGROUP Logon ID: 0x3e7 Logon Type: 2 Impersonation Level: %%1833 New Logon: Security ID: S-1-5-90-1 Account Name: DWM-1 Account Domain: Window Manager Logon ID: 0xcc3d Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x1fc Process Name: C:\Windows\System32\winlogon.exe Network Information: Workstation Name: Source Network Address: - Source Port: - Detailed Authentication Information: Logon Process: Advapi Authentication Package: Negotiate Transited Services: - Package Name (NTLM only): - Key Length: 0 This event is generated when a logon session is created. It is generated on the computer that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service such as the Server service, or a local process such as Winlogon.exe or Services.exe. The logon type field indicates the kind of logon that occurred. The most common types are 2 (interactive) and 3 (network). The New Logon fields indicate the account for whom the new logon was created, i.e. the account that was logged on. The network fields indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impersonation level field indicates the extent to which a process in the logon session can impersonate. The authentication information fields provide detailed information about this specific logon request. - Logon GUID is a unique identifier that can be used to correlate this event with a KDC event. - Transited services indicate which intermediate services have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indicates the length of the generated session key. This will be 0 if no session key was requested.
Security	Audit Success	12544	2015-04-22 19:47:38	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: LTRANPHD$ Account Domain: WORKGROUP Logon ID: 0x3e7 Logon Type: 2 Impersonation Level: %%1833 New Logon: Security ID: S-1-5-90-1 Account Name: DWM-1 Account Domain: Window Manager Logon ID: 0xcc61 Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x1fc Process Name: C:\Windows\System32\winlogon.exe Network Information: Workstation Name: Source Network Address: - Source Port: - Detailed Authentication Information: Logon Process: Advapi Authentication Package: Negotiate Transited Services: - Package Name (NTLM only): - Key Length: 0 This event is generated when a logon session is created. It is generated on the computer that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service such as the Server service, or a local process such as Winlogon.exe or Services.exe. The logon type field indicates the kind of logon that occurred. The most common types are 2 (interactive) and 3 (network). The New Logon fields indicate the account for whom the new logon was created, i.e. the account that was logged on. The network fields indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some

					cases. The impersonation level field indicates the extent to which a process in the logon session can impersonate. The authentication information fields provide detailed information about this specific logon request. - Logon GUID is a unique identifier that can be used to correlate this event with a KDC event. - Transited services indicate which intermediate services have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indicates the length of the generated session key. This will be 0 if no session key was requested.
Security	Audit Success	12548	2015-04-22 19:47:38	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Logon ID: 0x3e7 Privileges: SeAssignPrimaryTokenPrivilege SeTcbPrivilege SeSecurityPrivilege SeTakeOwnershipPrivilege SeLoadDriverPrivilege SeBackupPrivilege SeRestorePrivilege SeDebugPrivilege SeAuditPrivilege SeSystemEnvironmentPrivilege SeImpersonatePrivilege
Security	Audit Success	12548	2015-04-22 19:47:38	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-20 Account Name: NETWORK SERVICE Account Domain: NT AUTHORITY Logon ID: 0x3e4 Privileges: SeAssignPrimaryTokenPrivilege SeAuditPrivilege SeImpersonatePrivilege
Security	Audit Success	12548	2015-04-22 19:47:38	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-90-1 Account Name: DWM-1 Account Domain: Window Manager Logon ID: 0xcc3d Privileges: SeAssignPrimaryTokenPrivilege SeAuditPrivilege SeImpersonatePrivilege
Security	Audit Success	12548	2015-04-22 19:47:38	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-90-1 Account Name: DWM-1 Account Domain: Window Manager Logon ID: 0xcc61 Privileges: SeAssignPrimaryTokenPrivilege SeAuditPrivilege
Security	Audit Success	12292	2015-04-22 19:47:39	Microsoft-Windows-Security-Auditing	5033: The Windows Firewall Driver started successfully.
Security	Audit Success	12292	2015-04-22 19:47:39	Microsoft-Windows-Security-Auditing	5024: The Windows Firewall service started successfully.
Security	Audit Success	12544	2015-04-22 19:47:39	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: LTRANPHD$ Account Domain: WORKGROUP Logon ID: 0x3e7 Logon Type: 5 Impersonation Level: %%1833 New Logon: Security ID: S-1-5-19 Account Name: LOCAL SERVICE Account Domain: NT AUTHORITY Logon ID: 0x3e5 Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x22c Process Name: C:\Windows\System32\services.exe Network Information: Workstation Name: Source Network Address: - Source Port: - Detailed Authentication Information: Logon Process: Advapi Authentication Package: Negotiate Transited Services: - Package Name (NTLM only): - Key Length: 0 This event is generated when a logon session is created. It is generated on the computer that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service such as the Server service, or a local process such as Winlogon.exe or Services.exe. The logon type field indicates the kind of logon that occurred. The most common types are 2 (interactive) and 3 (network). The New Logon fields indicate the account for whom the new logon was created, i.e. the account that was logged on. The network fields indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impersonation level field indicates the extent to which a process in the logon session can impersonate. The authentication information fields provide detailed information about this specific logon request. - Logon GUID is a unique identifier that can be used to correlate this event with a KDC event. - Transited services indicate which intermediate services have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indicates the length of the generated session key. This will be 0 if no session key was requested.
Security	Audit Success	12544	2015-04-22 19:47:39	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: LTRANPHD$ Account Domain: WORKGROUP Logon ID: 0x3e7 Logon Type: 5 Impersonation Level: %%1833 New Logon: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Logon ID: 0x3e7 Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x22c Process Name: C:\Windows\System32\services.exe Network Information: Workstation Name: Source Network Address: - Source Port: - Detailed Authentication Information: Logon Process: Advapi Authentication Package: Negotiate Transited Services: - Package Name (NTLM only): - Key Length: 0 This event is generated when a logon session is created. It is generated on the computer that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service such as the Server service, or a local process such as Winlogon.exe or Services.exe. The logon type field indicates the kind of logon that occurred. The most common types are 2 (interactive) and 3 (network). The New Logon fields indicate the account for whom the new logon was created, i.e. the account that was logged on. The network fields indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impersonation level field indicates the extent to which a process in the logon session can impersonate. The authentication information fields provide detailed information about this specific logon request. - Logon GUID is a unique identifier that can be used to correlate this event with a KDC event. - Transited services indicate which intermediate services have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indicates the length of the generated session key. This will be 0 if no session key was requested.
					4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: LTRANPHD$ Account Domain: WORKGROUP Logon ID: 0x3e7 Logon Type: 5 Impersonation Level: %%1833 New Logon:

Security	Audit Success	12544	2015-04-22 19:47:39		Microsoft-Windows-Security-Auditing	Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Logon ID: 0x3e7 Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x22c Process Name: C:\Windows\System32\services.exe Network Information: Workstation Name: Source Network Address: - Source Port: - Detailed Authentication Information: Logon Process: Advapi Authentication Package: Negotiate Transited Services: - Package Name (NTLM only): - Key Length: 0 This event is generated when a logon session is created. It is generated on the computer that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service such as the Server service, or a local process such as Winlogon.exe or Services.exe. The logon type field indicates the kind of logon that occurred. The most common types are 2 (interactive) and 3 (network). The New Logon fields indicate the account for whom the new logon was created, i.e. the account that was logged on. The network fields indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impersonation level field indicates the extent to which a process in the logon session can impersonate. The authentication information fields provide detailed information about this specific logon request. - Logon GUID is a unique identifier that can be used to correlate this event with a KDC event. - Transited services indicate which intermediate services have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indicates the length of the generated session key. This will be 0 if no session key was requested.
Security	Audit Success	12544	2015-04-22 19:47:39		Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: LTRANPHD$ Account Domain: WORKGROUP Logon ID: 0x3e7 Logon Type: 5 Impersonation Level: %%1833 New Logon: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Logon ID: 0x3e7 Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x22c Process Name: C:\Windows\System32\services.exe Network Information: Workstation Name: Source Network Address: - Source Port: - Detailed Authentication Information: Logon Process: Advapi Authentication Package: Negotiate Transited Services: - Package Name (NTLM only): - Key Length: 0 This event is generated when a logon session is created. It is generated on the computer that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service such as the Server service, or a local process such as Winlogon.exe or Services.exe. The logon type field indicates the kind of logon that occurred. The most common types are 2 (interactive) and 3 (network). The New Logon fields indicate the account for whom the new logon was created, i.e. the account that was logged on. The network fields indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impersonation level field indicates the extent to which a process in the logon session can impersonate. The authentication information fields provide detailed information about this specific logon request. - Logon GUID is a unique identifier that can be used to correlate this event with a KDC event. - Transited services indicate which intermediate services have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indicates the length of the generated session key. This will be 0 if no session key was requested.
Security	Audit Success	12544	2015-04-22 19:47:39		Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: LTRANPHD$ Account Domain: WORKGROUP Logon ID: 0x3e7 Logon Type: 5 Impersonation Level: %%1833 New Logon: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Logon ID: 0x3e7 Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x22c Process Name: C:\Windows\System32\services.exe Network Information: Workstation Name: Source Network Address: - Source Port: - Detailed Authentication Information: Logon Process: Advapi Authentication Package: Negotiate Transited Services: - Package Name (NTLM only): - Key Length: 0 This event is generated when a logon session is created. It is generated on the computer that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service such as the Server service, or a local process such as Winlogon.exe or Services.exe. The logon type field indicates the kind of logon that occurred. The most common types are 2 (interactive) and 3 (network). The New Logon fields indicate the account for whom the new logon was created, i.e. the account that was logged on. The network fields indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impersonation level field indicates the extent to which a process in the logon session can impersonate. The authentication information fields provide detailed information about this specific logon request. - Logon GUID is a unique identifier that can be used to correlate this event with a KDC event. - Transited services indicate which intermediate services have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indicates the length of the generated session key. This will be 0 if no session key was requested.
Security	Audit Success	12544	2015-04-22 19:47:39		Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: LTRANPHD$ Account Domain: WORKGROUP Logon ID: 0x3e7 Logon Type: 5 Impersonation Level: %%1833 New Logon: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Logon ID: 0x3e7 Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x22c Process Name: C:\Windows\System32\services.exe Network Information: Workstation Name: Source Network Address: - Source Port: - Detailed Authentication Information: Logon Process: Advapi Authentication Package: Negotiate Transited Services: - Package Name (NTLM only): - Key Length: 0 This event is generated when a logon session is created. It is generated on the computer that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service such as the Server service, or a local process such as Winlogon.exe or Services.exe. The logon type field indicates the kind of logon that occurred. The most common types are 2 (interactive) and 3 (network). The New Logon fields indicate the account for whom the new logon was created, i.e. the account that was logged on. The network fields indicate where a

						remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impersonation level field indicates the extent to which a process in the logon session can impersonate. The authentication information fields provide detailed information about this specific logon request. - Logon GUID is a unique identifier that can be used to correlate this event with a KDC event. - Transited services indicate which intermediate services have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indicates the length of the generated session key. This will be 0 if no session key was requested.
Security	Audit Success	12544	2015-04-22 19:47:39		Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-0-0 Account Name: - Account Domain: - Logon ID: 0x0 Logon Type: 3 Impersonation Level: %%1833 New Logon: Security ID: S-1-5-7 Account Name: ANONYMOUS LOGON Account Domain: NT AUTHORITY Logon ID: 0x1692b Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x0 Process Name: - Network Information: Workstation Name: Source Network Address: - Source Port: - Detailed Authentication Information: Logon Process: NtLmSsp Authentication Package: NTLM Transited Services: - Package Name (NTLM only): NTLM V1 Key Length: 0 This event is generated when a logon session is created. It is generated on the computer that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service such as the Server service, or a local process such as Winlogon.exe or Services.exe. The logon type field indicates the kind of logon that occurred. The most common types are 2 (interactive) and 3 (network). The New Logon fields indicate the account for whom the new logon was created, i.e. the account that was logged on. The network fields indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impersonation level field indicates the extent to which a process in the logon session can impersonate. The authentication information fields provide detailed information about this specific logon request. - Logon GUID is a unique identifier that can be used to correlate this event with a KDC event. - Transited services indicate which intermediate services have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indicates the length of the generated session key. This will be 0 if no session key was requested.
Security	Audit Success	12548	2015-04-22 19:47:39		Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-19 Account Name: LOCAL SERVICE Account Domain: NT AUTHORITY Logon ID: 0x3e5 Privileges: SeAssignPrimaryTokenPrivilege SeAuditPrivilege SeImpersonatePrivilege
Security	Audit Success	12548	2015-04-22 19:47:39		Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Logon ID: 0x3e7 Privileges: SeAssignPrimaryTokenPrivilege SeTcbPrivilege SeSecurityPrivilege SeTakeOwnershipPrivilege SeLoadDriverPrivilege SeBackupPrivilege SeRestorePrivilege SeDebugPrivilege SeAuditPrivilege SeSystemEnvironmentPrivilege SeImpersonatePrivilege
Security	Audit Success	12548	2015-04-22 19:47:39		Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Logon ID: 0x3e7 Privileges: SeAssignPrimaryTokenPrivilege SeTcbPrivilege SeSecurityPrivilege SeTakeOwnershipPrivilege SeLoadDriverPrivilege SeBackupPrivilege SeRestorePrivilege SeDebugPrivilege SeAuditPrivilege SeSystemEnvironmentPrivilege SeImpersonatePrivilege
Security	Audit Success	12548	2015-04-22 19:47:39		Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Logon ID: 0x3e7 Privileges: SeAssignPrimaryTokenPrivilege SeTcbPrivilege SeSecurityPrivilege SeTakeOwnershipPrivilege SeLoadDriverPrivilege SeBackupPrivilege SeRestorePrivilege SeDebugPrivilege SeAuditPrivilege SeSystemEnvironmentPrivilege SeImpersonatePrivilege
Security	Audit Success	12548	2015-04-22 19:47:39		Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Logon ID: 0x3e7 Privileges: SeAssignPrimaryTokenPrivilege SeTcbPrivilege SeSecurityPrivilege SeTakeOwnershipPrivilege SeLoadDriverPrivilege SeBackupPrivilege SeRestorePrivilege SeDebugPrivilege SeAuditPrivilege SeSystemEnvironmentPrivilege SeImpersonatePrivilege
Security	Audit Success	12548	2015-04-22 19:47:39		Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Logon ID: 0x3e7 Privileges: SeAssignPrimaryTokenPrivilege SeTcbPrivilege SeSecurityPrivilege SeTakeOwnershipPrivilege SeLoadDriverPrivilege SeBackupPrivilege SeRestorePrivilege SeDebugPrivilege SeAuditPrivilege SeSystemEnvironmentPrivilege SeImpersonatePrivilege
Security	Audit Success	12544	2015-04-22 19:47:44		Microsoft-Windows-Security-Auditing	4648: A logon was attempted using explicit credentials. Subject: Security ID: S-1-5-18 Account Name: LTRANPHD$ Account Domain: WORKGROUP Logon ID: 0x3e7 Logon GUID: {00000000-0000-0000-0000-000000000000} Account Whose Credentials Were Used: Account Name: Liem Account Domain: LTRANPHD Logon GUID: {00000000-0000-0000-0000-000000000000} Target Server: Target Server Name: localhost Additional Information: localhost Process Information: Process ID: 0x1fc Process Name: C:\Windows\System32\winlogon.exe Network Information: Network Address: 127.0.0.1 Port: 0 This event is generated when a process attempts to log on an account by explicitly specifying that account’s credentials. This most commonly occurs in batch-type configurations such as scheduled tasks, or when using the RUNAS command.
						4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: LTRANPHD$ Account Domain: WORKGROUP Logon ID: 0x3e7 Logon Type: 2 Impersonation Level: %%1833 New Logon: Security ID: S-1-5-21-1888849264-3803429180-4108621888-1001 Account Name: Liem Account Domain: LTRANPHD Logon ID: 0x1a88d Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x1fc Process Name: C:\Windows\System32\winlogon.exe Network Information: Workstation Name: LTRANPHD Source Network Address: 127.0.0.1 Source Port: 0 Detailed Authentication Information: Logon Process: User32 Authentication Package: Negotiate Transited Services: - Package Name (NTLM only): - Key Length: 0 This event is generated when a logon session is created. It is generated on the computer that was

Security	Audit Success	12544	2015-04-22 19:47:44	Microsoft-Windows-Security-Auditing	accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service such as the Server service, or a local process such as Winlogon.exe or Services.exe. The logon type field indicates the kind of logon that occurred. The most common types are 2 (interactive) and 3 (network). The New Logon fields indicate the account for whom the new logon was created, i.e. the account that was logged on. The network fields indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impersonation level field indicates the extent to which a process in the logon session can impersonate. The authentication information fields provide detailed information about this specific logon request. - Logon GUID is a unique identifier that can be used to correlate this event with a KDC event. - Transited services indicate which intermediate services have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indicates the length of the generated session key. This will be 0 if no session key was requested.
Security	Audit Success	12544	2015-04-22 19:47:44	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: LTRANPHD$ Account Domain: WORKGROUP Logon ID: 0x3e7 Logon Type: 2 Impersonation Level: %%1833 New Logon: Security ID: S-1-5-21-1888849264-3803429180-4108621888-1001 Account Name: Liem Account Domain: LTRANPHD Logon ID: 0x1a8e6 Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x1fc Process Name: C:\Windows\System32\winlogon.exe Network Information: Workstation Name: LTRANPHD Source Network Address: 127.0.0.1 Source Port: 0 Detailed Authentication Information: Logon Process: User32 Authentication Package: Negotiate Transited Services: - Package Name (NTLM only): - Key Length: 0 This event is generated when a logon session is created. It is generated on the computer that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service such as the Server service, or a local process such as Winlogon.exe or Services.exe. The logon type field indicates the kind of logon that occurred. The most common types are 2 (interactive) and 3 (network). The New Logon fields indicate the account for whom the new logon was created, i.e. the account that was logged on. The network fields indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impersonation level field indicates the extent to which a process in the logon session can impersonate. The authentication information fields provide detailed information about this specific logon request. - Logon GUID is a unique identifier that can be used to correlate this event with a KDC event. - Transited services indicate which intermediate services have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indicates the length of the generated session key. This will be 0 if no session key was requested.
Security	Audit Success	12548	2015-04-22 19:47:44	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-21-1888849264-3803429180-4108621888-1001 Account Name: Liem Account Domain: LTRANPHD Logon ID: 0x1a88d Privileges: SeSecurityPrivilege SeTakeOwnershipPrivilege SeLoadDriverPrivilege SeBackupPrivilege SeRestorePrivilege SeDebugPrivilege SeSystemEnvironmentPrivilege SeImpersonatePrivilege
Security	Audit Success	12544	2015-04-22 19:47:45	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: LTRANPHD$ Account Domain: WORKGROUP Logon ID: 0x3e7 Logon Type: 5 Impersonation Level: %%1833 New Logon: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Logon ID: 0x3e7 Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x22c Process Name: C:\Windows\System32\services.exe Network Information: Workstation Name: Source Network Address: - Source Port: - Detailed Authentication Information: Logon Process: Advapi Authentication Package: Negotiate Transited Services: - Package Name (NTLM only): - Key Length: 0 This event is generated when a logon session is created. It is generated on the computer that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service such as the Server service, or a local process such as Winlogon.exe or Services.exe. The logon type field indicates the kind of logon that occurred. The most common types are 2 (interactive) and 3 (network). The New Logon fields indicate the account for whom the new logon was created, i.e. the account that was logged on. The network fields indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impersonation level field indicates the extent to which a process in the logon session can impersonate. The authentication information fields provide detailed information about this specific logon request. - Logon GUID is a unique identifier that can be used to correlate this event with a KDC event. - Transited services indicate which intermediate services have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indicates the length of the generated session key. This will be 0 if no session key was requested.
Security	Audit Success	12548	2015-04-22 19:47:45	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Logon ID: 0x3e7 Privileges: SeAssignPrimaryTokenPrivilege SeTcbPrivilege SeSecurityPrivilege SeTakeOwnershipPrivilege SeLoadDriverPrivilege SeBackupPrivilege SeRestorePrivilege SeDebugPrivilege SeAuditPrivilege SeSystemEnvironmentPrivilege SeImpersonatePrivilege
Security	Audit Success	13824	2015-04-22 19:47:47	Microsoft-Windows-Security-Auditing	4797: An attempt was made to query the existence of a blank password for an account. Subject: Security ID: S-1-5-21-1888849264-3803429180-4108621888-1001 Account Name: Liem Account Domain: LTRANPHD Logon ID: 0x1a8e6 Additional Information: Caller Workstation: LTRANPHD Target Account Name: Administrator Target Account Domain: LTRANPHD
Security	Audit Success	13824	2015-04-22 19:47:47	Microsoft-Windows-Security-Auditing	4797: An attempt was made to query the existence of a blank password for an account. Subject: Security ID: S-1-5-21-1888849264-3803429180-4108621888-1001 Account Name: Liem Account Domain: LTRANPHD Logon ID: 0x1a8e6 Additional Information: Caller Workstation: LTRANPHD Target Account Name: Guest Target Account Domain: LTRANPHD
					4797: An attempt was made to query the existence of a blank password for an account. Subject: Security ID:

Security	Audit Success	13824	2015-04-22 19:47:47	Microsoft-Windows-Security-Auditing	S-1-5-21-1888849264-3803429180-4108621888-1001 Account Name: Liem Account Domain: LTRANPHD Logon ID: 0x1a8e6 Additional Information: Caller Workstation: LTRANPHD Target Account Name: Administrator Target Account Domain: LTRANPHD
Security	Audit Success	13824	2015-04-22 19:47:47	Microsoft-Windows-Security-Auditing	4797: An attempt was made to query the existence of a blank password for an account. Subject: Security ID: S-1-5-21-1888849264-3803429180-4108621888-1001 Account Name: Liem Account Domain: LTRANPHD Logon ID: 0x1a8e6 Additional Information: Caller Workstation: LTRANPHD Target Account Name: Guest Target Account Domain: LTRANPHD
Security	Audit Success	13824	2015-04-22 19:47:48	Microsoft-Windows-Security-Auditing	4797: An attempt was made to query the existence of a blank password for an account. Subject: Security ID: S-1-5-19 Account Name: LOCAL SERVICE Account Domain: NT AUTHORITY Logon ID: 0x3e5 Additional Information: Caller Workstation: LTRANPHD Target Account Name: Administrator Target Account Domain: LTRANPHD
Security	Audit Success	13824	2015-04-22 19:47:48	Microsoft-Windows-Security-Auditing	4797: An attempt was made to query the existence of a blank password for an account. Subject: Security ID: S-1-5-19 Account Name: LOCAL SERVICE Account Domain: NT AUTHORITY Logon ID: 0x3e5 Additional Information: Caller Workstation: LTRANPHD Target Account Name: Administrator Target Account Domain: LTRANPHD
Security	Audit Success	13824	2015-04-22 19:47:48	Microsoft-Windows-Security-Auditing	4797: An attempt was made to query the existence of a blank password for an account. Subject: Security ID: S-1-5-19 Account Name: LOCAL SERVICE Account Domain: NT AUTHORITY Logon ID: 0x3e5 Additional Information: Caller Workstation: LTRANPHD Target Account Name: Guest Target Account Domain: LTRANPHD
Security	Audit Success	13824	2015-04-22 19:47:48	Microsoft-Windows-Security-Auditing	4797: An attempt was made to query the existence of a blank password for an account. Subject: Security ID: S-1-5-19 Account Name: LOCAL SERVICE Account Domain: NT AUTHORITY Logon ID: 0x3e5 Additional Information: Caller Workstation: LTRANPHD Target Account Name: Guest Target Account Domain: LTRANPHD
Security	Audit Success	13824	2015-04-22 19:47:48	Microsoft-Windows-Security-Auditing	4797: An attempt was made to query the existence of a blank password for an account. Subject: Security ID: S-1-5-19 Account Name: LOCAL SERVICE Account Domain: NT AUTHORITY Logon ID: 0x3e5 Additional Information: Caller Workstation: LTRANPHD Target Account Name: Liem Target Account Domain: LTRANPHD
Security	Audit Success	13824	2015-04-22 19:47:48	Microsoft-Windows-Security-Auditing	4797: An attempt was made to query the existence of a blank password for an account. Subject: Security ID: S-1-5-19 Account Name: LOCAL SERVICE Account Domain: NT AUTHORITY Logon ID: 0x3e5 Additional Information: Caller Workstation: LTRANPHD Target Account Name: Liem Target Account Domain: LTRANPHD
Security	Audit Success	13824	2015-04-22 19:47:48	Microsoft-Windows-Security-Auditing	4797: An attempt was made to query the existence of a blank password for an account. Subject: Security ID: S-1-5-19 Account Name: LOCAL SERVICE Account Domain: NT AUTHORITY Logon ID: 0x3e5 Additional Information: Caller Workstation: LTRANPHD Target Account Name: Liem Target Account Domain: LTRANPHD
Security	Audit Success	13824	2015-04-22 19:47:48	Microsoft-Windows-Security-Auditing	4797: An attempt was made to query the existence of a blank password for an account. Subject: Security ID: S-1-5-19 Account Name: LOCAL SERVICE Account Domain: NT AUTHORITY Logon ID: 0x3e5 Additional Information: Caller Workstation: LTRANPHD Target Account Name: Liem Target Account Domain: LTRANPHD
Security	Audit Success	12544	2015-04-22 19:48:31	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: LTRANPHD$ Account Domain: WORKGROUP Logon ID: 0x3e7 Logon Type: 5 Impersonation Level: %%1833 New Logon: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Logon ID: 0x3e7 Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x22c Process Name: C:\Windows\System32\services.exe Network Information: Workstation Name: Source Network Address: - Source Port: - Detailed Authentication Information: Logon Process: Advapi Authentication Package: Negotiate Transited Services: - Package Name (NTLM only): - Key Length: 0 This event is generated when a logon session is created. It is generated on the computer that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service such as the Server service, or a local process such as Winlogon.exe or Services.exe. The logon type field indicates the kind of logon that occurred. The most common types are 2 (interactive) and 3 (network). The New Logon fields indicate the account for whom the new logon was created, i.e. the account that was logged on. The network fields indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impersonation level field indicates the extent to which a process in the logon session can impersonate. The authentication information fields provide detailed information about this specific logon request. - Logon GUID is a unique identifier that can be used to correlate this event with a KDC event. - Transited services indicate which intermediate services have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indicates the length of the generated session key. This will be 0 if no session key was requested.
Security	Audit Success	12548	2015-04-22 19:48:31	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Logon ID: 0x3e7 Privileges: SeAssignPrimaryTokenPrivilege SeTcbPrivilege SeSecurityPrivilege SeTakeOwnershipPrivilege SeLoadDriverPrivilege SeBackupPrivilege SeRestorePrivilege SeDebugPrivilege SeAuditPrivilege SeSystemEnvironmentPrivilege SeImpersonatePrivilege
Security	Audit Success	103	2015-04-22 19:49:19	Microsoft-Windows-Eventlog	1100: The event logging service has shut down.
Security	Audit Success	12545	2015-04-22 19:49:19	Microsoft-Windows-Security-Auditing	4647: User initiated logoff: Subject: Security ID: S-1-5-21-1888849264-3803429180-4108621888-1001 Account Name: Liem Account Domain: LTRANPHD Logon ID: 0x1a8e6 This event is generated when a logoff is initiated. No further user-initiated activity can occur. This event can be interpreted as a logoff event.
Security	Audit	12288	2015-04-22	Microsoft-Windows-Security-	4608: Windows is starting up. This event is logged when LSASS.EXE starts and the auditing subsystem is

	Success		19:49:32	Auditing	initialized.
Security	Audit Success	12544	2015-04-22 19:49:32	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-0-0 Account Name: - Account Domain: - Logon ID: 0x0 Logon Type: 0 Impersonation Level: - New Logon: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Logon ID: 0x3e7 Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x4 Process Name: Network Information: Workstation Name: - Source Network Address: - Source Port: - Detailed Authentication Information: Logon Process: - Authentication Package: - Transited Services: - Package Name (NTLM only): - Key Length: 0 This event is generated when a logon session is created. It is generated on the computer that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service such as the Server service, or a local process such as Winlogon.exe or Services.exe. The logon type field indicates the kind of logon that occurred. The most common types are 2 (interactive) and 3 (network). The New Logon fields indicate the account for whom the new logon was created, i.e. the account that was logged on. The network fields indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impersonation level field indicates the extent to which a process in the logon session can impersonate. The authentication information fields provide detailed information about this specific logon request. - Logon GUID is a unique identifier that can be used to correlate this event with a KDC event. - Transited services indicate which intermediate services have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indicates the length of the generated session key. This will be 0 if no session key was requested.
Security	Audit Success	13568	2015-04-22 19:49:32	Microsoft-Windows-Security-Auditing	4902: The Per-user audit policy table was created. Number of Elements: 0 Policy ID: 0x7287
Security	Audit Success	12544	2015-04-22 19:49:34	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: LTRANPHD$ Account Domain: WORKGROUP Logon ID: 0x3e7 Logon Type: 5 Impersonation Level: %%1833 New Logon: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Logon ID: 0x3e7 Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x230 Process Name: C:\Windows\System32\services.exe Network Information: Workstation Name: Source Network Address: - Source Port: - Detailed Authentication Information: Logon Process: Advapi Authentication Package: Negotiate Transited Services: - Package Name (NTLM only): - Key Length: 0 This event is generated when a logon session is created. It is generated on the computer that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service such as the Server service, or a local process such as Winlogon.exe or Services.exe. The logon type field indicates the kind of logon that occurred. The most common types are 2 (interactive) and 3 (network). The New Logon fields indicate the account for whom the new logon was created, i.e. the account that was logged on. The network fields indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impersonation level field indicates the extent to which a process in the logon session can impersonate. The authentication information fields provide detailed information about this specific logon request. - Logon GUID is a unique identifier that can be used to correlate this event with a KDC event. - Transited services indicate which intermediate services have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indicates the length of the generated session key. This will be 0 if no session key was requested.
Security	Audit Success	12544	2015-04-22 19:49:34	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: LTRANPHD$ Account Domain: WORKGROUP Logon ID: 0x3e7 Logon Type: 5 Impersonation Level: %%1833 New Logon: Security ID: S-1-5-20 Account Name: NETWORK SERVICE Account Domain: NT AUTHORITY Logon ID: 0x3e4 Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x230 Process Name: C:\Windows\System32\services.exe Network Information: Workstation Name: Source Network Address: - Source Port: - Detailed Authentication Information: Logon Process: Advapi Authentication Package: Negotiate Transited Services: - Package Name (NTLM only): - Key Length: 0 This event is generated when a logon session is created. It is generated on the computer that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service such as the Server service, or a local process such as Winlogon.exe or Services.exe. The logon type field indicates the kind of logon that occurred. The most common types are 2 (interactive) and 3 (network). The New Logon fields indicate the account for whom the new logon was created, i.e. the account that was logged on. The network fields indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impersonation level field indicates the extent to which a process in the logon session can impersonate. The authentication information fields provide detailed information about this specific logon request. - Logon GUID is a unique identifier that can be used to correlate this event with a KDC event. - Transited services indicate which intermediate services have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indicates the length of the generated session key. This will be 0 if no session key was requested.
Security	Audit Success	12544	2015-04-22 19:49:34	Microsoft-Windows-Security-Auditing	4648: A logon was attempted using explicit credentials. Subject: Security ID: S-1-5-18 Account Name: LTRANPHD$ Account Domain: WORKGROUP Logon ID: 0x3e7 Logon GUID: {00000000-0000-0000-0000-000000000000} Account Whose Credentials Were Used: Account Name: DWM-1 Account Domain: Window Manager Logon GUID: {00000000-0000-0000-0000-000000000000} Target Server: Target Server Name: localhost Additional Information: localhost Process Information: Process ID: 0x200 Process Name: C:\Windows\System32\winlogon.exe Network Information: Network Address: - Port: - This event is generated

					when a process attempts to log on an account by explicitly specifying that account's credentials. This most commonly occurs in batch-type configurations such as scheduled tasks, or when using the RUNAS command.
Security	Audit Success	12544	2015-04-22 19:49:34	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: LTRANPHD$ Account Domain: WORKGROUP Logon ID: 0x3e7 Logon Type: 2 Impersonation Level: %%1833 New Logon: Security ID: S-1-5-90-1 Account Name: DWM-1 Account Domain: Window Manager Logon ID: 0xccd9 Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x200 Process Name: C:\Windows\System32\winlogon.exe Network Information: Workstation Name: Source Network Address: - Source Port: - Detailed Authentication Information: Logon Process: Advapi Authentication Package: Negotiate Transited Services: - Package Name (NTLM only): - Key Length: 0 This event is generated when a logon session is created. It is generated on the computer that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service such as the Server service, or a local process such as Winlogon.exe or Services.exe. The logon type field indicates the kind of logon that occurred. The most common types are 2 (interactive) and 3 (network). The New Logon fields indicate the account for whom the new logon was created, i.e. the account that was logged on. The network fields indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impersonation level field indicates the extent to which a process in the logon session can impersonate. The authentication information fields provide detailed information about this specific logon request. - Logon GUID is a unique identifier that can be used to correlate this event with a KDC event. - Transited services indicate which intermediate services have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indicates the length of the generated session key. This will be 0 if no session key was requested.
Security	Audit Success	12544	2015-04-22 19:49:34	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: LTRANPHD$ Account Domain: WORKGROUP Logon ID: 0x3e7 Logon Type: 2 Impersonation Level: %%1833 New Logon: Security ID: S-1-5-90-1 Account Name: DWM-1 Account Domain: Window Manager Logon ID: 0xccee Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x200 Process Name: C:\Windows\System32\winlogon.exe Network Information: Workstation Name: Source Network Address: - Source Port: - Detailed Authentication Information: Logon Process: Advapi Authentication Package: Negotiate Transited Services: - Package Name (NTLM only): - Key Length: 0 This event is generated when a logon session is created. It is generated on the computer that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service such as the Server service, or a local process such as Winlogon.exe or Services.exe. The logon type field indicates the kind of logon that occurred. The most common types are 2 (interactive) and 3 (network). The New Logon fields indicate the account for whom the new logon was created, i.e. the account that was logged on. The network fields indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impersonation level field indicates the extent to which a process in the logon session can impersonate. The authentication information fields provide detailed information about this specific logon request. - Logon GUID is a unique identifier that can be used to correlate this event with a KDC event. - Transited services indicate which intermediate services have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indicates the length of the generated session key. This will be 0 if no session key was requested.
Security	Audit Success	12548	2015-04-22 19:49:34	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Logon ID: 0x3e7 Privileges: SeAssignPrimaryTokenPrivilege SeTcbPrivilege SeSecurityPrivilege SeTakeOwnershipPrivilege SeLoadDriverPrivilege SeBackupPrivilege SeRestorePrivilege SeDebugPrivilege SeAuditPrivilege SeSystemEnvironmentPrivilege SeImpersonatePrivilege
Security	Audit Success	12548	2015-04-22 19:49:34	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-20 Account Name: NETWORK SERVICE Account Domain: NT AUTHORITY Logon ID: 0x3e4 Privileges: SeAssignPrimaryTokenPrivilege SeAuditPrivilege SeImpersonatePrivilege
Security	Audit Success	12548	2015-04-22 19:49:34	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-90-1 Account Name: DWM-1 Account Domain: Window Manager Logon ID: 0xccd9 Privileges: SeAssignPrimaryTokenPrivilege SeAuditPrivilege SeImpersonatePrivilege
Security	Audit Success	12548	2015-04-22 19:49:34	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-90-1 Account Name: DWM-1 Account Domain: Window Manager Logon ID: 0xccee Privileges: SeAssignPrimaryTokenPrivilege SeAuditPrivilege
Security	Audit Success	12292	2015-04-22 19:49:35	Microsoft-Windows-Security-Auditing	5033: The Windows Firewall Driver started successfully.
Security	Audit	12544	2015-04-22	Microsoft-Windows-Security-	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: LTRANPHD$ Account Domain: WORKGROUP Logon ID: 0x3e7 Logon Type: 5 Impersonation Level: %%1833 New Logon: Security ID: S-1-5-19 Account Name: LOCAL SERVICE Account Domain: NT AUTHORITY Logon ID: 0x3e5 Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x230 Process Name: C:\Windows\System32\services.exe Network Information: Workstation Name: Source Network Address: - Source Port: - Detailed Authentication Information: Logon Process: Advapi Authentication Package: Negotiate Transited Services: - Package Name (NTLM only): - Key Length: 0 This event is generated when a logon session is created. It is generated on the computer that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service such as the Server service, or a local process such as Winlogon.exe or Services.exe. The logon type field indicates the kind of logon that occurred.

	Success		19:49:35	Auditing	The most common types are 2 (interactive) and 3 (network). The New Logon fields indicate the account for whom the new logon was created, i.e. the account that was logged on. The network fields indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impersonation level field indicates the extent to which a process in the logon session can impersonate. The authentication information fields provide detailed information about this specific logon request. - Logon GUID is a unique identifier that can be used to correlate this event with a KDC event. - Transited services indicate which intermediate services have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indicates the length of the generated session key. This will be 0 if no session key was requested.
Security	Audit Success	12544	2015-04-22 19:49:35	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: LTRANPHD$ Account Domain: WORKGROUP Logon ID: 0x3e7 Logon Type: 5 Impersonation Level: %%1833 New Logon: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Logon ID: 0x3e7 Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x230 Process Name: C:\Windows\System32\services.exe Network Information: Workstation Name: Source Network Address: - Source Port: - Detailed Authentication Information: Logon Process: Advapi Authentication Package: Negotiate Transited Services: - Package Name (NTLM only): - Key Length: 0 This event is generated when a logon session is created. It is generated on the computer that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service such as the Server service, or a local process such as Winlogon.exe or Services.exe. The logon type field indicates the kind of logon that occurred. The most common types are 2 (interactive) and 3 (network). The New Logon fields indicate the account for whom the new logon was created, i.e. the account that was logged on. The network fields indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impersonation level field indicates the extent to which a process in the logon session can impersonate. The authentication information fields provide detailed information about this specific logon request. - Logon GUID is a unique identifier that can be used to correlate this event with a KDC event. - Transited services indicate which intermediate services have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indicates the length of the generated session key. This will be 0 if no session key was requested.
Security	Audit Success	12544	2015-04-22 19:49:35	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: LTRANPHD$ Account Domain: WORKGROUP Logon ID: 0x3e7 Logon Type: 5 Impersonation Level: %%1833 New Logon: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Logon ID: 0x3e7 Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x230 Process Name: C:\Windows\System32\services.exe Network Information: Workstation Name: Source Network Address: - Source Port: - Detailed Authentication Information: Logon Process: Advapi Authentication Package: Negotiate Transited Services: - Package Name (NTLM only): - Key Length: 0 This event is generated when a logon session is created. It is generated on the computer that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service such as the Server service, or a local process such as Winlogon.exe or Services.exe. The logon type field indicates the kind of logon that occurred. The most common types are 2 (interactive) and 3 (network). The New Logon fields indicate the account for whom the new logon was created, i.e. the account that was logged on. The network fields indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impersonation level field indicates the extent to which a process in the logon session can impersonate. The authentication information fields provide detailed information about this specific logon request. - Logon GUID is a unique identifier that can be used to correlate this event with a KDC event. - Transited services indicate which intermediate services have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indicates the length of the generated session key. This will be 0 if no session key was requested.
Security	Audit Success	12544	2015-04-22 19:49:35	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: LTRANPHD$ Account Domain: WORKGROUP Logon ID: 0x3e7 Logon Type: 5 Impersonation Level: %%1833 New Logon: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Logon ID: 0x3e7 Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x230 Process Name: C:\Windows\System32\services.exe Network Information: Workstation Name: Source Network Address: - Source Port: - Detailed Authentication Information: Logon Process: Advapi Authentication Package: Negotiate Transited Services: - Package Name (NTLM only): - Key Length: 0 This event is generated when a logon session is created. It is generated on the computer that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service such as the Server service, or a local process such as Winlogon.exe or Services.exe. The logon type field indicates the kind of logon that occurred. The most common types are 2 (interactive) and 3 (network). The New Logon fields indicate the account for whom the new logon was created, i.e. the account that was logged on. The network fields indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impersonation level field indicates the extent to which a process in the logon session can impersonate. The authentication information fields provide detailed information about this specific logon request. - Logon GUID is a unique identifier that can be used to correlate this event with a KDC event. - Transited services indicate which intermediate services have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indicates the length of the generated session key. This will be 0 if no session key was requested.

Security	Audit Success	12544	2015-04-22 19:49:35	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: LTRANPHD$ Account Domain: WORKGROUP Logon ID: 0x3e7 Logon Type: 5 Impersonation Level: %%1833 New Logon: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Logon ID: 0x3e7 Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x230 Process Name: C:\Windows\System32\services.exe Network Information: Workstation Name: Source Network Address: - Source Port: - Detailed Authentication Information: Logon Process: Advapi Authentication Package: Negotiate Transited Services: - Package Name (NTLM only): - Key Length: 0 This event is generated when a logon session is created. It is generated on the computer that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service such as the Server service, or a local process such as Winlogon.exe or Services.exe. The logon type field indicates the kind of logon that occurred. The most common types are 2 (interactive) and 3 (network). The New Logon fields indicate the account for whom the new logon was created, i.e. the account that was logged on. The network fields indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impersonation level field indicates the extent to which a process in the logon session can impersonate. The authentication information fields provide detailed information about this specific logon request. - Logon GUID is a unique identifier that can be used to correlate this event with a KDC event. - Transited services indicate which intermediate services have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indicates the length of the generated session key. This will be 0 if no session key was requested.
Security	Audit Success	12548	2015-04-22 19:49:35	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-19 Account Name: LOCAL SERVICE Account Domain: NT AUTHORITY Logon ID: 0x3e5 Privileges: SeAssignPrimaryTokenPrivilege SeAuditPrivilege SeImpersonatePrivilege
Security	Audit Success	12548	2015-04-22 19:49:35	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Logon ID: 0x3e7 Privileges: SeAssignPrimaryTokenPrivilege SeTcbPrivilege SeSecurityPrivilege SeTakeOwnershipPrivilege SeLoadDriverPrivilege SeBackupPrivilege SeRestorePrivilege SeDebugPrivilege SeAuditPrivilege SeSystemEnvironmentPrivilege SeImpersonatePrivilege
Security	Audit Success	12548	2015-04-22 19:49:35	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Logon ID: 0x3e7 Privileges: SeAssignPrimaryTokenPrivilege SeTcbPrivilege SeSecurityPrivilege SeTakeOwnershipPrivilege SeLoadDriverPrivilege SeBackupPrivilege SeRestorePrivilege SeDebugPrivilege SeAuditPrivilege SeSystemEnvironmentPrivilege SeImpersonatePrivilege
Security	Audit Success	12548	2015-04-22 19:49:35	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Logon ID: 0x3e7 Privileges: SeAssignPrimaryTokenPrivilege SeTcbPrivilege SeSecurityPrivilege SeTakeOwnershipPrivilege SeLoadDriverPrivilege SeBackupPrivilege SeRestorePrivilege SeDebugPrivilege SeAuditPrivilege SeSystemEnvironmentPrivilege SeImpersonatePrivilege
Security	Audit Success	12548	2015-04-22 19:49:35	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Logon ID: 0x3e7 Privileges: SeAssignPrimaryTokenPrivilege SeTcbPrivilege SeSecurityPrivilege SeTakeOwnershipPrivilege SeLoadDriverPrivilege SeBackupPrivilege SeRestorePrivilege SeDebugPrivilege SeAuditPrivilege SeSystemEnvironmentPrivilege SeImpersonatePrivilege
Security	Audit Success	12292	2015-04-22 19:49:36	Microsoft-Windows-Security-Auditing	5024: The Windows Firewall service started successfully.
Security	Audit Success	12544	2015-04-22 19:49:36	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: LTRANPHD$ Account Domain: WORKGROUP Logon ID: 0x3e7 Logon Type: 5 Impersonation Level: %%1833 New Logon: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Logon ID: 0x3e7 Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x230 Process Name: C:\Windows\System32\services.exe Network Information: Workstation Name: Source Network Address: - Source Port: - Detailed Authentication Information: Logon Process: Advapi Authentication Package: Negotiate Transited Services: - Package Name (NTLM only): - Key Length: 0 This event is generated when a logon session is created. It is generated on the computer that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service such as the Server service, or a local process such as Winlogon.exe or Services.exe. The logon type field indicates the kind of logon that occurred. The most common types are 2 (interactive) and 3 (network). The New Logon fields indicate the account for whom the new logon was created, i.e. the account that was logged on. The network fields indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impersonation level field indicates the extent to which a process in the logon session can impersonate. The authentication information fields provide detailed information about this specific logon request. - Logon GUID is a unique identifier that can be used to correlate this event with a KDC event. - Transited services indicate which intermediate services have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indicates the length of the generated session key. This will be 0 if no session key was requested.
					4624: An account was successfully logged on. Subject: Security ID: S-1-0-0 Account Name: - Account Domain: - Logon ID: 0x0 Logon Type: 3 Impersonation Level: %%1833 New Logon: Security ID: S-1-5-7 Account Name: ANONYMOUS LOGON Account Domain: NT AUTHORITY Logon ID: 0x1670c Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x0 Process Name: - Network Information: Workstation Name: Source Network Address: - Source Port: - Detailed Authentication Information: Logon Process: NtLmSsp Authentication Package: NTLM Transited Services: - Package Name (NTLM only): NTLM V1

Security	Audit Success	12544	2015-04-22 19:49:36	Microsoft-Windows-Security-Auditing	Key Length: 0 This event is generated when a logon session is created. It is generated on the computer that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service such as the Server service, or a local process such as Winlogon.exe or Services.exe. The logon type field indicates the kind of logon that occurred. The most common types are 2 (interactive) and 3 (network). The New Logon fields indicate the account for whom the new logon was created, i.e. the account that was logged on. The network fields indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impersonation level field indicates the extent to which a process in the logon session can impersonate. The authentication information fields provide detailed information about this specific logon request. - Logon GUID is a unique identifier that can be used to correlate this event with a KDC event. - Transited services indicate which intermediate services have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indicates the length of the generated session key. This will be 0 if no session key was requested.
Security	Audit Success	12548	2015-04-22 19:49:36	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Logon ID: 0x3e7 Privileges: SeAssignPrimaryTokenPrivilege SeTcbPrivilege SeSecurityPrivilege SeTakeOwnershipPrivilege SeLoadDriverPrivilege SeBackupPrivilege SeRestorePrivilege SeDebugPrivilege SeAuditPrivilege SeSystemEnvironmentPrivilege SeImpersonatePrivilege
Security	Audit Success	12544	2015-04-22 19:49:37	Microsoft-Windows-Security-Auditing	4648: A logon was attempted using explicit credentials. Subject: Security ID: S-1-5-18 Account Name: LTRANPHD$ Account Domain: WORKGROUP Logon ID: 0x3e7 Logon GUID: {00000000-0000-0000-0000-000000000000} Account Whose Credentials Were Used: Account Name: Liem Account Domain: LTRANPHD Logon GUID: {00000000-0000-0000-0000-000000000000} Target Server: Target Server Name: localhost Additional Information: localhost Process Information: Process ID: 0x200 Process Name: C:\Windows\System32\winlogon.exe Network Information: Network Address: 127.0.0.1 Port: 0 This event is generated when a process attempts to log on an account by explicitly specifying that account's credentials. This most commonly occurs in batch-type configurations such as scheduled tasks, or when using the RUNAS command.
Security	Audit Success	12544	2015-04-22 19:49:37	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: LTRANPHD$ Account Domain: WORKGROUP Logon ID: 0x3e7 Logon Type: 2 Impersonation Level: %%1833 New Logon: Security ID: S-1-5-21-1888849264-3803429180-4108621888-1001 Account Name: Liem Account Domain: LTRANPHD Logon ID: 0x17fb6 Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x200 Process Name: C:\Windows\System32\winlogon.exe Network Information: Workstation Name: LTRANPHD Source Network Address: 127.0.0.1 Source Port: 0 Detailed Authentication Information: Logon Process: User32 Authentication Package: Negotiate Transited Services: - Package Name (NTLM only): - Key Length: 0 This event is generated when a logon session is created. It is generated on the computer that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service such as the Server service, or a local process such as Winlogon.exe or Services.exe. The logon type field indicates the kind of logon that occurred. The most common types are 2 (interactive) and 3 (network). The New Logon fields indicate the account for whom the new logon was created, i.e. the account that was logged on. The network fields indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impersonation level field indicates the extent to which a process in the logon session can impersonate. The authentication information fields provide detailed information about this specific logon request. - Logon GUID is a unique identifier that can be used to correlate this event with a KDC event. - Transited services indicate which intermediate services have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indicates the length of the generated session key. This will be 0 if no session key was requested.
Security	Audit Success	12544	2015-04-22 19:49:37	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: LTRANPHD$ Account Domain: WORKGROUP Logon ID: 0x3e7 Logon Type: 2 Impersonation Level: %%1833 New Logon: Security ID: S-1-5-21-1888849264-3803429180-4108621888-1001 Account Name: Liem Account Domain: LTRANPHD Logon ID: 0x17fe6 Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x200 Process Name: C:\Windows\System32\winlogon.exe Network Information: Workstation Name: LTRANPHD Source Network Address: 127.0.0.1 Source Port: 0 Detailed Authentication Information: Logon Process: User32 Authentication Package: Negotiate Transited Services: - Package Name (NTLM only): - Key Length: 0 This event is generated when a logon session is created. It is generated on the computer that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service such as the Server service, or a local process such as Winlogon.exe or Services.exe. The logon type field indicates the kind of logon that occurred. The most common types are 2 (interactive) and 3 (network). The New Logon fields indicate the account for whom the new logon was created, i.e. the account that was logged on. The network fields indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impersonation level field indicates the extent to which a process in the logon session can impersonate. The authentication information fields provide detailed information about this specific logon request. - Logon GUID is a unique identifier that can be used to correlate this event with a KDC event. - Transited services indicate which intermediate services have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indicates the length of the generated session key. This will be 0 if no session key was requested.
Security	Audit Success	12548	2015-04-22 19:49:37	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-21-1888849264-3803429180-4108621888-1001 Account Name: Liem Account Domain: LTRANPHD Logon ID: 0x17fb6 Privileges: SeSecurityPrivilege SeTakeOwnershipPrivilege SeLoadDriverPrivilege SeBackupPrivilege SeRestorePrivilege

					SeDebugPrivilege SeSystemEnvironmentPrivilege SeImpersonatePrivilege
Security	Audit Success	12544	2015-04-22 19:49:38	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: LTRANPHD$ Account Domain: WORKGROUP Logon ID: 0x3e7 Logon Type: 5 Impersonation Level: %%1833 New Logon: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Logon ID: 0x3e7 Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x230 Process Name: C:\Windows\System32\services.exe Network Information: Workstation Name: Source Network Address: - Source Port: - Detailed Authentication Information: Logon Process: Advapi Authentication Package: Negotiate Transited Services: - Package Name (NTLM only): - Key Length: 0 This event is generated when a logon session is created. It is generated on the computer that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service such as the Server service, or a local process such as Winlogon.exe or Services.exe. The logon type field indicates the kind of logon that occurred. The most common types are 2 (interactive) and 3 (network). The New Logon fields indicate the account for whom the new logon was created, i.e. the account that was logged on. The network fields indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impersonation level field indicates the extent to which a process in the logon session can impersonate. The authentication information fields provide detailed information about this specific logon request. - Logon GUID is a unique identifier that can be used to correlate this event with a KDC event. - Transited services indicate which intermediate services have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indicates the length of the generated session key. This will be 0 if no session key was requested.
Security	Audit Success	12548	2015-04-22 19:49:38	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Logon ID: 0x3e7 Privileges: SeAssignPrimaryTokenPrivilege SeTcbPrivilege SeSecurityPrivilege SeTakeOwnershipPrivilege SeLoadDriverPrivilege SeBackupPrivilege SeRestorePrivilege SeDebugPrivilege SeAuditPrivilege SeSystemEnvironmentPrivilege SeImpersonatePrivilege
Security	Audit Success	13824	2015-04-22 19:49:41	Microsoft-Windows-Security-Auditing	4797: An attempt was made to query the existence of a blank password for an account. Subject: Security ID: S-1-5-21-1888849264-3803429180-4108621888-1001 Account Name: Liem Account Domain: LTRANPHD Logon ID: 0x17fe6 Additional Information: Caller Workstation: LTRANPHD Target Account Name: Administrator Target Account Domain: LTRANPHD
Security	Audit Success	13824	2015-04-22 19:49:41	Microsoft-Windows-Security-Auditing	4797: An attempt was made to query the existence of a blank password for an account. Subject: Security ID: S-1-5-21-1888849264-3803429180-4108621888-1001 Account Name: Liem Account Domain: LTRANPHD Logon ID: 0x17fe6 Additional Information: Caller Workstation: LTRANPHD Target Account Name: Guest Target Account Domain: LTRANPHD
Security	Audit Success	13824	2015-04-22 19:49:41	Microsoft-Windows-Security-Auditing	4797: An attempt was made to query the existence of a blank password for an account. Subject: Security ID: S-1-5-21-1888849264-3803429180-4108621888-1001 Account Name: Liem Account Domain: LTRANPHD Logon ID: 0x17fe6 Additional Information: Caller Workstation: LTRANPHD Target Account Name: Administrator Target Account Domain: LTRANPHD
Security	Audit Success	13824	2015-04-22 19:49:41	Microsoft-Windows-Security-Auditing	4797: An attempt was made to query the existence of a blank password for an account. Subject: Security ID: S-1-5-21-1888849264-3803429180-4108621888-1001 Account Name: Liem Account Domain: LTRANPHD Logon ID: 0x17fe6 Additional Information: Caller Workstation: LTRANPHD Target Account Name: Guest Target Account Domain: LTRANPHD
Security	Audit Success	13824	2015-04-22 19:49:44	Microsoft-Windows-Security-Auditing	4797: An attempt was made to query the existence of a blank password for an account. Subject: Security ID: S-1-5-19 Account Name: LOCAL SERVICE Account Domain: NT AUTHORITY Logon ID: 0x3e5 Additional Information: Caller Workstation: LTRANPHD Target Account Name: Administrator Target Account Domain: LTRANPHD
Security	Audit Success	13824	2015-04-22 19:49:44	Microsoft-Windows-Security-Auditing	4797: An attempt was made to query the existence of a blank password for an account. Subject: Security ID: S-1-5-19 Account Name: LOCAL SERVICE Account Domain: NT AUTHORITY Logon ID: 0x3e5 Additional Information: Caller Workstation: LTRANPHD Target Account Name: Guest Target Account Domain: LTRANPHD
Security	Audit Success	13824	2015-04-22 19:49:44	Microsoft-Windows-Security-Auditing	4797: An attempt was made to query the existence of a blank password for an account. Subject: Security ID: S-1-5-19 Account Name: LOCAL SERVICE Account Domain: NT AUTHORITY Logon ID: 0x3e5 Additional Information: Caller Workstation: LTRANPHD Target Account Name: Administrator Target Account Domain: LTRANPHD
Security	Audit Success	13824	2015-04-22 19:49:44	Microsoft-Windows-Security-Auditing	4797: An attempt was made to query the existence of a blank password for an account. Subject: Security ID: S-1-5-19 Account Name: LOCAL SERVICE Account Domain: NT AUTHORITY Logon ID: 0x3e5 Additional Information: Caller Workstation: LTRANPHD Target Account Name: Liem Target Account Domain: LTRANPHD
Security	Audit Success	13824	2015-04-22 19:49:44	Microsoft-Windows-Security-Auditing	4797: An attempt was made to query the existence of a blank password for an account. Subject: Security ID: S-1-5-19 Account Name: LOCAL SERVICE Account Domain: NT AUTHORITY Logon ID: 0x3e5 Additional Information: Caller Workstation: LTRANPHD Target Account Name: Guest Target Account Domain: LTRANPHD
Security	Audit Success	13824	2015-04-22 19:49:44	Microsoft-Windows-Security-Auditing	4797: An attempt was made to query the existence of a blank password for an account. Subject: Security ID: S-1-5-19 Account Name: LOCAL SERVICE Account Domain: NT AUTHORITY Logon ID: 0x3e5 Additional Information: Caller Workstation: LTRANPHD Target Account Name: Liem Target Account Domain: LTRANPHD
Security	Audit Success	13824	2015-04-22 19:49:44	Microsoft-Windows-Security-Auditing	4797: An attempt was made to query the existence of a blank password for an account. Subject: Security ID: S-1-5-19 Account Name: LOCAL SERVICE Account Domain: NT AUTHORITY Logon ID: 0x3e5 Additional Information: Caller Workstation: LTRANPHD Target Account Name: Liem Target Account Domain: LTRANPHD
Security	Audit		2015-04-	Microsoft-Windows-Security-	4797: An attempt was made to query the existence of a blank password for an account. Subject: Security ID:

Security	Success	13824	22 19:49:44	Auditing	S-1-5-19 Account Name: LOCAL SERVICE Account Domain: NT AUTHORITY Logon ID: 0x3e5 Additional Information: Caller Workstation: LTRANPHD Target Account Name: Liem Target Account Domain: LTRANPHD
Security	Audit Success	13824	2015-04-22 19:50:17	Microsoft-Windows-Security-Auditing	4797: An attempt was made to query the existence of a blank password for an account. Subject: Security ID: S-1-5-21-1888849264-3803429180-4108621888-1001 Account Name: Liem Account Domain: LTRANPHD Logon ID: 0x17fe6 Additional Information: Caller Workstation: LTRANPHD Target Account Name: Administrator Target Account Domain: LTRANPHD
Security	Audit Success	12545	2015-04-22 19:52:43	Microsoft-Windows-Security-Auditing	4647: User initiated logoff: Subject: Security ID: S-1-5-21-1888849264-3803429180-4108621888-1001 Account Name: Liem Account Domain: LTRANPHD Logon ID: 0x17fe6 This event is generated when a logoff is initiated. No further user-initiated activity can occur. This event can be interpreted as a logoff event.
Security	Audit Success	103	2015-04-22 19:52:44	Microsoft-Windows-Eventlog	1100: The event logging service has shut down.
Security	Audit Success	12288	2015-04-22 19:52:56	Microsoft-Windows-Security-Auditing	4608: Windows is starting up. This event is logged when LSASS.EXE starts and the auditing subsystem is initialized.
Security	Audit Success	12544	2015-04-22 19:52:56	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-0-0 Account Name: - Account Domain: - Logon ID: 0x0 Logon Type: 0 Impersonation Level: - New Logon: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Logon ID: 0x3e7 Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x4 Process Name: Network Information: Workstation Name: - Source Network Address: - Source Port: - Detailed Authentication Information: Logon Process: - Authentication Package: - Transited Services: - Package Name (NTLM only): - Key Length: 0 This event is generated when a logon session is created. It is generated on the computer that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service such as the Server service, or a local process such as Winlogon.exe or Services.exe. The logon type field indicates the kind of logon that occurred. The most common types are 2 (interactive) and 3 (network). The New Logon fields indicate the account for whom the new logon was created, i.e. the account that was logged on. The network fields indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impersonation level field indicates the extent to which a process in the logon session can impersonate. The authentication information fields provide detailed information about this specific logon request. - Logon GUID is a unique identifier that can be used to correlate this event with a KDC event. - Transited services indicate which intermediate services have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indicates the length of the generated session key. This will be 0 if no session key was requested.
Security	Audit Success	13568	2015-04-22 19:52:56	Microsoft-Windows-Security-Auditing	4902: The Per-user audit policy table was created. Number of Elements: 0 Policy ID: 0x70d9
Security	Audit Success	12544	2015-04-22 19:52:57	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: LTRANPHD$ Account Domain: WORKGROUP Logon ID: 0x3e7 Logon Type: 5 Impersonation Level: %%1833 New Logon: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Logon ID: 0x3e7 Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x230 Process Name: C:\Windows\System32\services.exe Network Information: Workstation Name: Source Network Address: - Source Port: - Detailed Authentication Information: Logon Process: Advapi Authentication Package: Negotiate Transited Services: - Package Name (NTLM only): - Key Length: 0 This event is generated when a logon session is created. It is generated on the computer that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service such as the Server service, or a local process such as Winlogon.exe or Services.exe. The logon type field indicates the kind of logon that occurred. The most common types are 2 (interactive) and 3 (network). The New Logon fields indicate the account for whom the new logon was created, i.e. the account that was logged on. The network fields indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impersonation level field indicates the extent to which a process in the logon session can impersonate. The authentication information fields provide detailed information about this specific logon request. - Logon GUID is a unique identifier that can be used to correlate this event with a KDC event. - Transited services indicate which intermediate services have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indicates the length of the generated session key. This will be 0 if no session key was requested.
Security	Audit Success	12544	2015-04-22 19:52:57	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: LTRANPHD$ Account Domain: WORKGROUP Logon ID: 0x3e7 Logon Type: 5 Impersonation Level: %%1833 New Logon: Security ID: S-1-5-20 Account Name: NETWORK SERVICE Account Domain: NT AUTHORITY Logon ID: 0x3e4 Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x230 Process Name: C:\Windows\System32\services.exe Network Information: Workstation Name: Source Network Address: - Source Port: - Detailed Authentication Information: Logon Process: Advapi Authentication Package: Negotiate Transited Services: - Package Name (NTLM only): - Key Length: 0 This event is generated when a logon session is created. It is generated on the computer that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service such as the Server service, or a local process such as Winlogon.exe or Services.exe. The logon type field indicates the kind of logon that occurred. The most common types are 2 (interactive) and 3 (network). The New Logon fields indicate the account for

					whom the new logon was created, i.e. the account that was logged on. The network fields indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impersonation level field indicates the extent to which a process in the logon session can impersonate. The authentication information fields provide detailed information about this specific logon request. - Logon GUID is a unique identifier that can be used to correlate this event with a KDC event. - Transited services indicate which intermediate services have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indicates the length of the generated session key. This will be 0 if no session key was requested.
Security	Audit Success	12544	2015-04-22 19:52:57	Microsoft-Windows-Security-Auditing	4648: A logon was attempted using explicit credentials. Subject: Security ID: S-1-5-18 Account Name: LTRANPHD$ Account Domain: WORKGROUP Logon ID: 0x3e7 Logon GUID: {00000000-0000-0000-0000-000000000000} Account Whose Credentials Were Used: Account Name: DWM-1 Account Domain: Window Manager Logon GUID: {00000000-0000-0000-0000-000000000000} Target Server: Target Server Name: localhost Additional Information: localhost Process Information: Process ID: 0x200 Process Name: C:\Windows\System32\winlogon.exe Network Information: Network Address: - Port: - This event is generated when a process attempts to log on an account by explicitly specifying that account's credentials. This most commonly occurs in batch-type configurations such as scheduled tasks, or when using the RUNAS command.
Security	Audit Success	12544	2015-04-22 19:52:57	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: LTRANPHD$ Account Domain: WORKGROUP Logon ID: 0x3e7 Logon Type: 2 Impersonation Level: %%1833 New Logon: Security ID: S-1-5-90-1 Account Name: DWM-1 Account Domain: Window Manager Logon ID: 0xc945 Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x200 Process Name: C:\Windows\System32\winlogon.exe Network Information: Workstation Name: Source Network Address: - Source Port: - Detailed Authentication Information: Logon Process: Advapi Authentication Package: Negotiate Transited Services: - Package Name (NTLM only): - Key Length: 0 This event is generated when a logon session is created. It is generated on the computer that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service such as the Server service, or a local process such as Winlogon.exe or Services.exe. The logon type field indicates the kind of logon that occurred. The most common types are 2 (interactive) and 3 (network). The New Logon fields indicate the account for whom the new logon was created, i.e. the account that was logged on. The network fields indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impersonation level field indicates the extent to which a process in the logon session can impersonate. The authentication information fields provide detailed information about this specific logon request. - Logon GUID is a unique identifier that can be used to correlate this event with a KDC event. - Transited services indicate which intermediate services have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indicates the length of the generated session key. This will be 0 if no session key was requested.
Security	Audit Success	12544	2015-04-22 19:52:57	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: LTRANPHD$ Account Domain: WORKGROUP Logon ID: 0x3e7 Logon Type: 2 Impersonation Level: %%1833 New Logon: Security ID: S-1-5-90-1 Account Name: DWM-1 Account Domain: Window Manager Logon ID: 0xc95d Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x200 Process Name: C:\Windows\System32\winlogon.exe Network Information: Workstation Name: Source Network Address: - Source Port: - Detailed Authentication Information: Logon Process: Advapi Authentication Package: Negotiate Transited Services: - Package Name (NTLM only): - Key Length: 0 This event is generated when a logon session is created. It is generated on the computer that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service such as the Server service, or a local process such as Winlogon.exe or Services.exe. The logon type field indicates the kind of logon that occurred. The most common types are 2 (interactive) and 3 (network). The New Logon fields indicate the account for whom the new logon was created, i.e. the account that was logged on. The network fields indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impersonation level field indicates the extent to which a process in the logon session can impersonate. The authentication information fields provide detailed information about this specific logon request. - Logon GUID is a unique identifier that can be used to correlate this event with a KDC event. - Transited services indicate which intermediate services have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indicates the length of the generated session key. This will be 0 if no session key was requested.
Security	Audit Success	12548	2015-04-22 19:52:57	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Logon ID: 0x3e7 Privileges: SeAssignPrimaryTokenPrivilege SeTcbPrivilege SeSecurityPrivilege SeTakeOwnershipPrivilege SeLoadDriverPrivilege SeBackupPrivilege SeRestorePrivilege SeDebugPrivilege SeAuditPrivilege SeSystemEnvironmentPrivilege SeImpersonatePrivilege
Security	Audit Success	12548	2015-04-22 19:52:57	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-20 Account Name: NETWORK SERVICE Account Domain: NT AUTHORITY Logon ID: 0x3e4 Privileges: SeAssignPrimaryTokenPrivilege SeAuditPrivilege SeImpersonatePrivilege
Security	Audit Success	12548	2015-04-22 19:52:57	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-90-1 Account Name: DWM-1 Account Domain: Window Manager Logon ID: 0xc945 Privileges: SeAssignPrimaryTokenPrivilege SeAuditPrivilege SeImpersonatePrivilege
Security	Audit	12548	2015-04-22	Microsoft-Windows-Security-	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-90-1 Account Name: DWM-1

	Success		19:52:57	Auditing	Account Domain: Window Manager Logon ID: 0xc95d Privileges: SeAssignPrimaryTokenPrivilege SeAuditPrivilege
Security	Audit Success	12544	2015-04-22 19:52:58	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: LTRANPHD$ Account Domain: WORKGROUP Logon ID: 0x3e7 Logon Type: 5 Impersonation Level: %%1833 New Logon: Security ID: S-1-5-19 Account Name: LOCAL SERVICE Account Domain: NT AUTHORITY Logon ID: 0x3e5 Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x230 Process Name: C:\Windows\System32\services.exe Network Information: Workstation Name: Source Network Address: - Source Port: - Detailed Authentication Information: Logon Process: Advapi Authentication Package: Negotiate Transited Services: - Package Name (NTLM only): - Key Length: 0 This event is generated when a logon session is created. It is generated on the computer that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service such as the Server service, or a local process such as Winlogon.exe or Services.exe. The logon type field indicates the kind of logon that occurred. The most common types are 2 (interactive) and 3 (network). The New Logon fields indicate the account for whom the new logon was created, i.e. the account that was logged on. The network fields indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impersonation level field indicates the extent to which a process in the logon session can impersonate. The authentication information fields provide detailed information about this specific logon request. - Logon GUID is a unique identifier that can be used to correlate this event with a KDC event. - Transited services indicate which intermediate services have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indicates the length of the generated session key. This will be 0 if no session key was requested.
Security	Audit Success	12544	2015-04-22 19:52:58	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: LTRANPHD$ Account Domain: WORKGROUP Logon ID: 0x3e7 Logon Type: 5 Impersonation Level: %%1833 New Logon: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Logon ID: 0x3e7 Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x230 Process Name: C:\Windows\System32\services.exe Network Information: Workstation Name: Source Network Address: - Source Port: - Detailed Authentication Information: Logon Process: Advapi Authentication Package: Negotiate Transited Services: - Package Name (NTLM only): - Key Length: 0 This event is generated when a logon session is created. It is generated on the computer that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service such as the Server service, or a local process such as Winlogon.exe or Services.exe. The logon type field indicates the kind of logon that occurred. The most common types are 2 (interactive) and 3 (network). The New Logon fields indicate the account for whom the new logon was created, i.e. the account that was logged on. The network fields indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impersonation level field indicates the extent to which a process in the logon session can impersonate. The authentication information fields provide detailed information about this specific logon request. - Logon GUID is a unique identifier that can be used to correlate this event with a KDC event. - Transited services indicate which intermediate services have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indicates the length of the generated session key. This will be 0 if no session key was requested.
Security	Audit Success	12548	2015-04-22 19:52:58	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-19 Account Name: LOCAL SERVICE Account Domain: NT AUTHORITY Logon ID: 0x3e5 Privileges: SeAssignPrimaryTokenPrivilege SeAuditPrivilege SeImpersonatePrivilege
Security	Audit Success	12548	2015-04-22 19:52:58	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Logon ID: 0x3e7 Privileges: SeAssignPrimaryTokenPrivilege SeTcbPrivilege SeSecurityPrivilege SeTakeOwnershipPrivilege SeLoadDriverPrivilege SeBackupPrivilege SeRestorePrivilege SeDebugPrivilege SeAuditPrivilege SeSystemEnvironmentPrivilege SeImpersonatePrivilege
Security	Audit Success	12292	2015-04-22 19:52:59	Microsoft-Windows-Security-Auditing	5033: The Windows Firewall Driver started successfully.
Security	Audit Success	12544	2015-04-22 19:52:59	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: LTRANPHD$ Account Domain: WORKGROUP Logon ID: 0x3e7 Logon Type: 5 Impersonation Level: %%1833 New Logon: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Logon ID: 0x3e7 Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x230 Process Name: C:\Windows\System32\services.exe Network Information: Workstation Name: Source Network Address: - Source Port: - Detailed Authentication Information: Logon Process: Advapi Authentication Package: Negotiate Transited Services: - Package Name (NTLM only): - Key Length: 0 This event is generated when a logon session is created. It is generated on the computer that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service such as the Server service, or a local process such as Winlogon.exe or Services.exe. The logon type field indicates the kind of logon that occurred. The most common types are 2 (interactive) and 3 (network). The New Logon fields indicate the account for whom the new logon was created, i.e. the account that was logged on. The network fields indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impersonation level field indicates the extent to which a process in the logon session can impersonate. The authentication information fields provide detailed information about this specific logon request. - Logon GUID is a unique identifier that can be used to correlate this event with a KDC event. - Transited services indicate which intermediate services have participated in this logon request. - Package name indicates

						which sub-protocol was used among the NTLM protocols. - Key length indicates the length of the generated session key. This will be 0 if no session key was requested.
Security	Audit Success	12544	2015-04-22 19:52:59		Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: LTRANPHD$ Account Domain: WORKGROUP Logon ID: 0x3e7 Logon Type: 5 Impersonation Level: %%1833 New Logon: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Logon ID: 0x3e7 Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x230 Process Name: C:\Windows\System32\services.exe Network Information: Workstation Name: Source Network Address: - Source Port: - Detailed Authentication Information: Logon Process: Advapi Authentication Package: Negotiate Transited Services: - Package Name (NTLM only): - Key Length: 0 This event is generated when a logon session is created. It is generated on the computer that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service such as the Server service, or a local process such as Winlogon.exe or Services.exe. The logon type field indicates the kind of logon that occurred. The most common types are 2 (interactive) and 3 (network). The New Logon fields indicate the account for whom the new logon was created, i.e. the account that was logged on. The network fields indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impersonation level field indicates the extent to which a process in the logon session can impersonate. The authentication information fields provide detailed information about this specific logon request. - Logon GUID is a unique identifier that can be used to correlate this event with a KDC event. - Transited services indicate which intermediate services have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indicates the length of the generated session key. This will be 0 if no session key was requested.
Security	Audit Success	12544	2015-04-22 19:52:59		Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: LTRANPHD$ Account Domain: WORKGROUP Logon ID: 0x3e7 Logon Type: 5 Impersonation Level: %%1833 New Logon: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Logon ID: 0x3e7 Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x230 Process Name: C:\Windows\System32\services.exe Network Information: Workstation Name: Source Network Address: - Source Port: - Detailed Authentication Information: Logon Process: Advapi Authentication Package: Negotiate Transited Services: - Package Name (NTLM only): - Key Length: 0 This event is generated when a logon session is created. It is generated on the computer that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service such as the Server service, or a local process such as Winlogon.exe or Services.exe. The logon type field indicates the kind of logon that occurred. The most common types are 2 (interactive) and 3 (network). The New Logon fields indicate the account for whom the new logon was created, i.e. the account that was logged on. The network fields indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impersonation level field indicates the extent to which a process in the logon session can impersonate. The authentication information fields provide detailed information about this specific logon request. - Logon GUID is a unique identifier that can be used to correlate this event with a KDC event. - Transited services indicate which intermediate services have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indicates the length of the generated session key. This will be 0 if no session key was requested.
Security	Audit Success	12548	2015-04-22 19:52:59		Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Logon ID: 0x3e7 Privileges: SeAssignPrimaryTokenPrivilege SeTcbPrivilege SeSecurityPrivilege SeTakeOwnershipPrivilege SeLoadDriverPrivilege SeBackupPrivilege SeRestorePrivilege SeDebugPrivilege SeAuditPrivilege SeSystemEnvironmentPrivilege SeImpersonatePrivilege
Security	Audit Success	12548	2015-04-22 19:52:59		Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Logon ID: 0x3e7 Privileges: SeAssignPrimaryTokenPrivilege SeTcbPrivilege SeSecurityPrivilege SeTakeOwnershipPrivilege SeLoadDriverPrivilege SeBackupPrivilege SeRestorePrivilege SeDebugPrivilege SeAuditPrivilege SeSystemEnvironmentPrivilege SeImpersonatePrivilege
Security	Audit Success	12548	2015-04-22 19:52:59		Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Logon ID: 0x3e7 Privileges: SeAssignPrimaryTokenPrivilege SeTcbPrivilege SeSecurityPrivilege SeTakeOwnershipPrivilege SeLoadDriverPrivilege SeBackupPrivilege SeRestorePrivilege SeDebugPrivilege SeAuditPrivilege SeSystemEnvironmentPrivilege SeImpersonatePrivilege
Security	Audit Success	12292	2015-04-22 19:53:00		Microsoft-Windows-Security-Auditing	5024: The Windows Firewall service started successfully.
Security	Audit Success	12544	2015-04-22 19:53:00		Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: LTRANPHD$ Account Domain: WORKGROUP Logon ID: 0x3e7 Logon Type: 5 Impersonation Level: %%1833 New Logon: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Logon ID: 0x3e7 Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x230 Process Name: C:\Windows\System32\services.exe Network Information: Workstation Name: Source Network Address: - Source Port: - Detailed Authentication Information: Logon Process: Advapi Authentication Package: Negotiate Transited Services: - Package Name (NTLM only): - Key Length: 0 This event is generated when a logon session is created. It is generated on the computer that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service such as the Server service, or a local process such as Winlogon.exe or Services.exe. The logon type field indicates the kind of logon that occurred. The most common types are 2 (interactive) and 3 (network). The New Logon fields indicate the account for

					whom the new logon was created, i.e. the account that was logged on. The network fields indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impersonation level field indicates the extent to which a process in the logon session can impersonate. The authentication information fields provide detailed information about this specific logon request. - Logon GUID is a unique identifier that can be used to correlate this event with a KDC event. - Transited services indicate which intermediate services have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indicates the length of the generated session key. This will be 0 if no session key was requested.
Security	Audit Success	12544	2015-04-22 19:53:00	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-0-0 Account Name: - Account Domain: - Logon ID: 0x0 Logon Type: 3 Impersonation Level: %%1833 New Logon: Security ID: S-1-5-7 Account Name: ANONYMOUS LOGON Account Domain: NT AUTHORITY Logon ID: 0x1664f Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x0 Process Name: - Network Information: Workstation Name: Source Network Address: - Source Port: - Detailed Authentication Information: Logon Process: NtLmSsp Authentication Package: NTLM Transited Services: - Package Name (NTLM only): NTLM V1 Key Length: 0 This event is generated when a logon session is created. It is generated on the computer that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service such as the Server service, or a local process such as Winlogon.exe or Services.exe. The logon type field indicates the kind of logon that occurred. The most common types are 2 (interactive) and 3 (network). The New Logon fields indicate the account for whom the new logon was created, i.e. the account that was logged on. The network fields indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impersonation level field indicates the extent to which a process in the logon session can impersonate. The authentication information fields provide detailed information about this specific logon request. - Logon GUID is a unique identifier that can be used to correlate this event with a KDC event. - Transited services indicate which intermediate services have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indicates the length of the generated session key. This will be 0 if no session key was requested.
Security	Audit Success	12548	2015-04-22 19:53:00	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Logon ID: 0x3e7 Privileges: SeAssignPrimaryTokenPrivilege SeTcbPrivilege SeSecurityPrivilege SeTakeOwnershipPrivilege SeLoadDriverPrivilege SeBackupPrivilege SeRestorePrivilege SeDebugPrivilege SeAuditPrivilege SeSystemEnvironmentPrivilege SeImpersonatePrivilege
Security	Audit Success	12544	2015-04-22 19:53:02	Microsoft-Windows-Security-Auditing	4648: A logon was attempted using explicit credentials. Subject: Security ID: S-1-5-18 Account Name: LTRANPHD$ Account Domain: WORKGROUP Logon ID: 0x3e7 Logon GUID: {00000000-0000-0000-0000-000000000000} Account Whose Credentials Were Used: Account Name: Liem Account Domain: LTRANPHD Logon GUID: {00000000-0000-0000-0000-000000000000} Target Server: Target Server Name: localhost Additional Information: localhost Process Information: Process ID: 0x200 Process Name: C:\Windows\System32\winlogon.exe Network Information: Network Address: 127.0.0.1 Port: 0 This event is generated when a process attempts to log on an account by explicitly specifying that account's credentials. This most commonly occurs in batch-type configurations such as scheduled tasks, or when using the RUNAS command.
Security	Audit Success	12544	2015-04-22 19:53:02	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: LTRANPHD$ Account Domain: WORKGROUP Logon ID: 0x3e7 Logon Type: 2 Impersonation Level: %%1833 New Logon: Security ID: S-1-5-21-1888849264-3803429180-4108621888-1001 Account Name: Liem Account Domain: LTRANPHD Logon ID: 0x17e93 Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x200 Process Name: C:\Windows\System32\winlogon.exe Network Information: Workstation Name: LTRANPHD Source Network Address: 127.0.0.1 Source Port: 0 Detailed Authentication Information: Logon Process: User32 Authentication Package: Negotiate Transited Services: - Package Name (NTLM only): - Key Length: 0 This event is generated when a logon session is created. It is generated on the computer that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service such as the Server service, or a local process such as Winlogon.exe or Services.exe. The logon type field indicates the kind of logon that occurred. The most common types are 2 (interactive) and 3 (network). The New Logon fields indicate the account for whom the new logon was created, i.e. the account that was logged on. The network fields indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impersonation level field indicates the extent to which a process in the logon session can impersonate. The authentication information fields provide detailed information about this specific logon request. - Logon GUID is a unique identifier that can be used to correlate this event with a KDC event. - Transited services indicate which intermediate services have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indicates the length of the generated session key. This will be 0 if no session key was requested.
					4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: LTRANPHD$ Account Domain: WORKGROUP Logon ID: 0x3e7 Logon Type: 2 Impersonation Level: %%1833 New Logon: Security ID: S-1-5-21-1888849264-3803429180-4108621888-1001 Account Name: Liem Account Domain: LTRANPHD Logon ID: 0x17ec2 Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x200 Process Name: C:\Windows\System32\winlogon.exe Network Information: Workstation Name: LTRANPHD Source Network Address: 127.0.0.1 Source Port: 0 Detailed Authentication Information: Logon Process: User32 Authentication Package: Negotiate Transited Services: - Package Name (NTLM only): - Key Length: 0 This event is generated when a logon session is created. It is generated on the computer that

Security	Audit Success	12544	2015-04-22 19:53:02	Microsoft-Windows-Security-Auditing	was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service such as the Server service, or a local process such as Winlogon.exe or Services.exe. The logon type field indicates the kind of logon that occurred. The most common types are 2 (interactive) and 3 (network). The New Logon fields indicate the account for whom the new logon was created, i.e. the account that was logged on. The network fields indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impersonation level field indicates the extent to which a process in the logon session can impersonate. The authentication information fields provide detailed information about this specific logon request. - Logon GUID is a unique identifier that can be used to correlate this event with a KDC event. - Transited services indicate which intermediate services have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indicates the length of the generated session key. This will be 0 if no session key was requested.
Security	Audit Success	12548	2015-04-22 19:53:02	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-21-1888849264-3803429180-4108621888-1001 Account Name: Liem Account Domain: LTRANPHD Logon ID: 0x17e93 Privileges: SeSecurityPrivilege SeTakeOwnershipPrivilege SeLoadDriverPrivilege SeBackupPrivilege SeRestorePrivilege SeDebugPrivilege SeSystemEnvironmentPrivilege SeImpersonatePrivilege
Security	Audit Success	12544	2015-04-22 19:53:03	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: LTRANPHD$ Account Domain: WORKGROUP Logon ID: 0x3e7 Logon Type: 5 Impersonation Level: %%1833 New Logon: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Logon ID: 0x3e7 Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x230 Process Name: C:\Windows\System32\services.exe Network Information: Workstation Name: Source Network Address: - Source Port: - Detailed Authentication Information: Logon Process: Advapi Authentication Package: Negotiate Transited Services: - Package Name (NTLM only): - Key Length: 0 This event is generated when a logon session is created. It is generated on the computer that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service such as the Server service, or a local process such as Winlogon.exe or Services.exe. The logon type field indicates the kind of logon that occurred. The most common types are 2 (interactive) and 3 (network). The New Logon fields indicate the account for whom the new logon was created, i.e. the account that was logged on. The network fields indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impersonation level field indicates the extent to which a process in the logon session can impersonate. The authentication information fields provide detailed information about this specific logon request. - Logon GUID is a unique identifier that can be used to correlate this event with a KDC event. - Transited services indicate which intermediate services have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indicates the length of the generated session key. This will be 0 if no session key was requested.
Security	Audit Success	12548	2015-04-22 19:53:03	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Logon ID: 0x3e7 Privileges: SeAssignPrimaryTokenPrivilege SeTcbPrivilege SeSecurityPrivilege SeTakeOwnershipPrivilege SeLoadDriverPrivilege SeBackupPrivilege SeRestorePrivilege SeDebugPrivilege SeAuditPrivilege SeSystemEnvironmentPrivilege SeImpersonatePrivilege
Security	Audit Success	13824	2015-04-22 19:53:05	Microsoft-Windows-Security-Auditing	4797: An attempt was made to query the existence of a blank password for an account. Subject: Security ID: S-1-5-21-1888849264-3803429180-4108621888-1001 Account Name: Liem Account Domain: LTRANPHD Logon ID: 0x17ec2 Additional Information: Caller Workstation: LTRANPHD Target Account Name: Administrator Target Account Domain: LTRANPHD
Security	Audit Success	13824	2015-04-22 19:53:05	Microsoft-Windows-Security-Auditing	4797: An attempt was made to query the existence of a blank password for an account. Subject: Security ID: S-1-5-21-1888849264-3803429180-4108621888-1001 Account Name: Liem Account Domain: LTRANPHD Logon ID: 0x17ec2 Additional Information: Caller Workstation: LTRANPHD Target Account Name: Guest Target Account Domain: LTRANPHD
Security	Audit Success	13824	2015-04-22 19:53:05	Microsoft-Windows-Security-Auditing	4797: An attempt was made to query the existence of a blank password for an account. Subject: Security ID: S-1-5-21-1888849264-3803429180-4108621888-1001 Account Name: Liem Account Domain: LTRANPHD Logon ID: 0x17ec2 Additional Information: Caller Workstation: LTRANPHD Target Account Name: Administrator Target Account Domain: LTRANPHD
Security	Audit Success	13824	2015-04-22 19:53:05	Microsoft-Windows-Security-Auditing	4797: An attempt was made to query the existence of a blank password for an account. Subject: Security ID: S-1-5-21-1888849264-3803429180-4108621888-1001 Account Name: Liem Account Domain: LTRANPHD Logon ID: 0x17ec2 Additional Information: Caller Workstation: LTRANPHD Target Account Name: Guest Target Account Domain: LTRANPHD
Security	Audit Success	13824	2015-04-22 19:53:07	Microsoft-Windows-Security-Auditing	4797: An attempt was made to query the existence of a blank password for an account. Subject: Security ID: S-1-5-19 Account Name: LOCAL SERVICE Account Domain: NT AUTHORITY Logon ID: 0x3e5 Additional Information: Caller Workstation: LTRANPHD Target Account Name: Administrator Target Account Domain: LTRANPHD
Security	Audit Success	13824	2015-04-22 19:53:07	Microsoft-Windows-Security-Auditing	4797: An attempt was made to query the existence of a blank password for an account. Subject: Security ID: S-1-5-19 Account Name: LOCAL SERVICE Account Domain: NT AUTHORITY Logon ID: 0x3e5 Additional Information: Caller Workstation: LTRANPHD Target Account Name: Administrator Target Account Domain: LTRANPHD
Security	Audit Success	13824	2015-04-22 19:53:07	Microsoft-Windows-Security-Auditing	4797: An attempt was made to query the existence of a blank password for an account. Subject: Security ID: S-1-5-19 Account Name: LOCAL SERVICE Account Domain: NT AUTHORITY Logon ID: 0x3e5 Additional Information: Caller Workstation: LTRANPHD Target Account Name: Guest Target Account Domain: LTRANPHD

Security	Audit Success	13824	2015-04-22 19:53:07	Microsoft-Windows-Security-Auditing	4797: An attempt was made to query the existence of a blank password for an account. Subject: Security ID: S-1-5-19 Account Name: LOCAL SERVICE Account Domain: NT AUTHORITY Logon ID: 0x3e5 Additional Information: Caller Workstation: LTRANPHD Target Account Name: Guest Target Account Domain: LTRANPHD
Security	Audit Success	13824	2015-04-22 19:53:07	Microsoft-Windows-Security-Auditing	4797: An attempt was made to query the existence of a blank password for an account. Subject: Security ID: S-1-5-19 Account Name: LOCAL SERVICE Account Domain: NT AUTHORITY Logon ID: 0x3e5 Additional Information: Caller Workstation: LTRANPHD Target Account Name: Liem Target Account Domain: LTRANPHD
Security	Audit Success	13824	2015-04-22 19:53:07	Microsoft-Windows-Security-Auditing	4797: An attempt was made to query the existence of a blank password for an account. Subject: Security ID: S-1-5-19 Account Name: LOCAL SERVICE Account Domain: NT AUTHORITY Logon ID: 0x3e5 Additional Information: Caller Workstation: LTRANPHD Target Account Name: Liem Target Account Domain: LTRANPHD
Security	Audit Success	13824	2015-04-22 19:53:07	Microsoft-Windows-Security-Auditing	4797: An attempt was made to query the existence of a blank password for an account. Subject: Security ID: S-1-5-19 Account Name: LOCAL SERVICE Account Domain: NT AUTHORITY Logon ID: 0x3e5 Additional Information: Caller Workstation: LTRANPHD Target Account Name: Liem Target Account Domain: LTRANPHD
Security	Audit Success	13824	2015-04-22 19:53:07	Microsoft-Windows-Security-Auditing	4797: An attempt was made to query the existence of a blank password for an account. Subject: Security ID: S-1-5-19 Account Name: LOCAL SERVICE Account Domain: NT AUTHORITY Logon ID: 0x3e5 Additional Information: Caller Workstation: LTRANPHD Target Account Name: Liem Target Account Domain: LTRANPHD
Security	Audit Success	12544	2015-04-22 19:53:52	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: LTRANPHD$ Account Domain: WORKGROUP Logon ID: 0x3e7 Logon Type: 5 Impersonation Level: %%1833 New Logon: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Logon ID: 0x3e7 Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x230 Process Name: C:\Windows\System32\services.exe Network Information: Workstation Name: Source Network Address: - Source Port: - Detailed Authentication Information: Logon Process: Advapi Authentication Package: Negotiate Transited Services: - Package Name (NTLM only): - Key Length: 0 This event is generated when a logon session is created. It is generated on the computer that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service such as the Server service, or a local process such as Winlogon.exe or Services.exe. The logon type field indicates the kind of logon that occurred. The most common types are 2 (interactive) and 3 (network). The New Logon fields indicate the account for whom the new logon was created, i.e. the account that was logged on. The network fields indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impersonation level field indicates the extent to which a process in the logon session can impersonate. The authentication information fields provide detailed information about this specific logon request. - Logon GUID is a unique identifier that can be used to correlate this event with a KDC event. - Transited services indicate which intermediate services have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indicates the length of the generated session key. This will be 0 if no session key was requested.
Security	Audit Success	12548	2015-04-22 19:53:52	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Logon ID: 0x3e7 Privileges: SeAssignPrimaryTokenPrivilege SeTcbPrivilege SeSecurityPrivilege SeTakeOwnershipPrivilege SeLoadDriverPrivilege SeBackupPrivilege SeRestorePrivilege SeDebugPrivilege SeAuditPrivilege SeSystemEnvironmentPrivilege SeImpersonatePrivilege
Security	Audit Success	12545	2015-04-22 19:54:05	Microsoft-Windows-Security-Auditing	4647: User initiated logoff: Subject: Security ID: S-1-5-21-1888849264-3803429180-4108621888-1001 Account Name: Liem Account Domain: LTRANPHD Logon ID: 0x17ec2 This event is generated when a logoff is initiated. No further user-initiated activity can occur. This event can be interpreted as a logoff event.
Security	Audit Success	103	2015-04-22 19:54:06	Microsoft-Windows-Eventlog	1100: The event logging service has shut down.
Security	Audit Success	12288	2015-04-22 19:54:17	Microsoft-Windows-Security-Auditing	4608: Windows is starting up. This event is logged when LSASS.EXE starts and the auditing subsystem is initialized.
Security	Audit Success	12544	2015-04-22 19:54:17	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-0-0 Account Name: - Account Domain: - Logon ID: 0x0 Logon Type: 0 Impersonation Level: - New Logon: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Logon ID: 0x3e7 Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x4 Process Name: Network Information: Workstation Name: - Source Network Address: - Source Port: - Detailed Authentication Information: Logon Process: - Authentication Package: - Transited Services: - Package Name (NTLM only): - Key Length: 0 This event is generated when a logon session is created. It is generated on the computer that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service such as the Server service, or a local process such as Winlogon.exe or Services.exe. The logon type field indicates the kind of logon that occurred. The most common types are 2 (interactive) and 3 (network). The New Logon fields indicate the account for whom the new logon was created, i.e. the account that was logged on. The network fields indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impersonation level field indicates the extent to which a process in the logon session can impersonate. The authentication information fields provide detailed information about this specific logon request. - Logon GUID is a unique identifier that can be used to correlate this event with a KDC event. - Transited services indicate which intermediate services have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indicates the length of the generated session key. This will be 0 if no session key was requested.

Security	Audit Success	13568	2015-04-22 19:54:17	Microsoft-Windows-Security-Auditing	4902: The Per-user audit policy table was created. Number of Elements: 0 Policy ID: 0x7193
Security	Audit Success	12544	2015-04-22 19:54:21	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: LTRANPHD$ Account Domain: WORKGROUP Logon ID: 0x3e7 Logon Type: 5 Impersonation Level: %%1833 New Logon: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Logon ID: 0x3e7 Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x230 Process Name: C:\Windows\System32\services.exe Network Information: Workstation Name: Source Network Address: - Source Port: - Detailed Authentication Information: Logon Process: Advapi Authentication Package: Negotiate Transited Services: - Package Name (NTLM only): - Key Length: 0 This event is generated when a logon session is created. It is generated on the computer that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service such as the Server service, or a local process such as Winlogon.exe or Services.exe. The logon type field indicates the kind of logon that occurred. The most common types are 2 (interactive) and 3 (network). The New Logon fields indicate the account for whom the new logon was created, i.e. the account that was logged on. The network fields indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impersonation level field indicates the extent to which a process in the logon session can impersonate. The authentication information fields provide detailed information about this specific logon request. - Logon GUID is a unique identifier that can be used to correlate this event with a KDC event. - Transited services indicate which intermediate services have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indicates the length of the generated session key. This will be 0 if no session key was requested.
Security	Audit Success	12548	2015-04-22 19:54:21	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Logon ID: 0x3e7 Privileges: SeAssignPrimaryTokenPrivilege SeTcbPrivilege SeSecurityPrivilege SeTakeOwnershipPrivilege SeLoadDriverPrivilege SeBackupPrivilege SeRestorePrivilege SeDebugPrivilege SeAuditPrivilege SeSystemEnvironmentPrivilege SeImpersonatePrivilege
Security	Audit Success	12544	2015-04-22 19:54:22	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: LTRANPHD$ Account Domain: WORKGROUP Logon ID: 0x3e7 Logon Type: 5 Impersonation Level: %%1833 New Logon: Security ID: S-1-5-20 Account Name: NETWORK SERVICE Account Domain: NT AUTHORITY Logon ID: 0x3e4 Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x230 Process Name: C:\Windows\System32\services.exe Network Information: Workstation Name: Source Network Address: - Source Port: - Detailed Authentication Information: Logon Process: Advapi Authentication Package: Negotiate Transited Services: - Package Name (NTLM only): - Key Length: 0 This event is generated when a logon session is created. It is generated on the computer that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service such as the Server service, or a local process such as Winlogon.exe or Services.exe. The logon type field indicates the kind of logon that occurred. The most common types are 2 (interactive) and 3 (network). The New Logon fields indicate the account for whom the new logon was created, i.e. the account that was logged on. The network fields indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impersonation level field indicates the extent to which a process in the logon session can impersonate. The authentication information fields provide detailed information about this specific logon request. - Logon GUID is a unique identifier that can be used to correlate this event with a KDC event. - Transited services indicate which intermediate services have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indicates the length of the generated session key. This will be 0 if no session key was requested.
Security	Audit Success	12544	2015-04-22 19:54:22	Microsoft-Windows-Security-Auditing	4648: A logon was attempted using explicit credentials. Subject: Security ID: S-1-5-18 Account Name: LTRANPHD$ Account Domain: WORKGROUP Logon ID: 0x3e7 Logon GUID: {00000000-0000-0000-0000-000000000000} Account Whose Credentials Were Used: Account Name: DWM-1 Account Domain: Window Manager Logon GUID: {00000000-0000-0000-0000-000000000000} Target Server: Target Server Name: localhost Additional Information: localhost Process Information: Process ID: 0x200 Process Name: C:\Windows\System32\winlogon.exe Network Information: Network Address: - Port: - This event is generated when a process attempts to log on an account by explicitly specifying that account's credentials. This most commonly occurs in batch-type configurations such as scheduled tasks, or when using the RUNAS command.
Security	Audit Success	12544	2015-04-22 19:54:22	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: LTRANPHD$ Account Domain: WORKGROUP Logon ID: 0x3e7 Logon Type: 2 Impersonation Level: %%1833 New Logon: Security ID: S-1-5-90-1 Account Name: DWM-1 Account Domain: Window Manager Logon ID: 0xcae8 Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x200 Process Name: C:\Windows\System32\winlogon.exe Network Information: Workstation Name: Source Network Address: - Source Port: - Detailed Authentication Information: Logon Process: Advapi Authentication Package: Negotiate Transited Services: - Package Name (NTLM only): - Key Length: 0 This event is generated when a logon session is created. It is generated on the computer that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service such as the Server service, or a local process such as Winlogon.exe or Services.exe. The logon type field indicates the kind of logon that occurred. The most common types are 2 (interactive) and 3 (network). The New Logon fields indicate the account for whom the new logon was created, i.e. the account that was logged on. The network fields indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some

					cases. The impersonation level field indicates the extent to which a process in the logon session can impersonate. The authentication information fields provide detailed information about this specific logon request. - Logon GUID is a unique identifier that can be used to correlate this event with a KDC event. - Transited services indicate which intermediate services have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indicates the length of the generated session key. This will be 0 if no session key was requested.
Security	Audit Success	12544	2015-04-22 19:54:22	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: LTRANPHD$ Account Domain: WORKGROUP Logon ID: 0x3e7 Logon Type: 2 Impersonation Level: %%1833 New Logon: Security ID: S-1-5-90-1 Account Name: DWM-1 Account Domain: Window Manager Logon ID: 0xcb0a Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x200 Process Name: C:\Windows\System32\winlogon.exe Network Information: Workstation Name: Source Network Address: - Source Port: - Detailed Authentication Information: Logon Process: Advapi Authentication Package: Negotiate Transited Services: - Package Name (NTLM only): - Key Length: 0 This event is generated when a logon session is created. It is generated on the computer that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service such as the Server service, or a local process such as Winlogon.exe or Services.exe. The logon type field indicates the kind of logon that occurred. The most common types are 2 (interactive) and 3 (network). The New Logon fields indicate the account for whom the new logon was created, i.e. the account that was logged on. The network fields indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impersonation level field indicates the extent to which a process in the logon session can impersonate. The authentication information fields provide detailed information about this specific logon request. - Logon GUID is a unique identifier that can be used to correlate this event with a KDC event. - Transited services indicate which intermediate services have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indicates the length of the generated session key. This will be 0 if no session key was requested.
Security	Audit Success	12548	2015-04-22 19:54:22	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-20 Account Name: NETWORK SERVICE Account Domain: NT AUTHORITY Logon ID: 0x3e4 Privileges: SeAssignPrimaryTokenPrivilege SeAuditPrivilege SeImpersonatePrivilege
Security	Audit Success	12548	2015-04-22 19:54:22	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-90-1 Account Name: DWM-1 Account Domain: Window Manager Logon ID: 0xcae8 Privileges: SeAssignPrimaryTokenPrivilege SeAuditPrivilege SeImpersonatePrivilege
Security	Audit Success	12548	2015-04-22 19:54:22	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-90-1 Account Name: DWM-1 Account Domain: Window Manager Logon ID: 0xcb0a Privileges: SeAssignPrimaryTokenPrivilege SeAuditPrivilege
Security	Audit Success	12292	2015-04-22 19:54:23	Microsoft-Windows-Security-Auditing	5033: The Windows Firewall Driver started successfully.
Security	Audit Success	12544	2015-04-22 19:54:23	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: LTRANPHD$ Account Domain: WORKGROUP Logon ID: 0x3e7 Logon Type: 5 Impersonation Level: %%1833 New Logon: Security ID: S-1-5-19 Account Name: LOCAL SERVICE Account Domain: NT AUTHORITY Logon ID: 0x3e5 Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x230 Process Name: C:\Windows\System32\services.exe Network Information: Workstation Name: Source Network Address: - Source Port: - Detailed Authentication Information: Logon Process: Advapi Authentication Package: Negotiate Transited Services: - Package Name (NTLM only): - Key Length: 0 This event is generated when a logon session is created. It is generated on the computer that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service such as the Server service, or a local process such as Winlogon.exe or Services.exe. The logon type field indicates the kind of logon that occurred. The most common types are 2 (interactive) and 3 (network). The New Logon fields indicate the account for whom the new logon was created, i.e. the account that was logged on. The network fields indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impersonation level field indicates the extent to which a process in the logon session can impersonate. The authentication information fields provide detailed information about this specific logon request. - Logon GUID is a unique identifier that can be used to correlate this event with a KDC event. - Transited services indicate which intermediate services have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indicates the length of the generated session key. This will be 0 if no session key was requested.
Security	Audit	12544	2015-04-22	Microsoft-Windows-Security-	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: LTRANPHD$ Account Domain: WORKGROUP Logon ID: 0x3e7 Logon Type: 5 Impersonation Level: %%1833 New Logon: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Logon ID: 0x3e7 Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x230 Process Name: C:\Windows\System32\services.exe Network Information: Workstation Name: Source Network Address: - Source Port: - Detailed Authentication Information: Logon Process: Advapi Authentication Package: Negotiate Transited Services: - Package Name (NTLM only): - Key Length: 0 This event is generated when a logon session is created. It is generated on the computer that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service such as the Server service, or a local process such as Winlogon.exe or Services.exe. The logon type field indicates the kind of logon that occurred.

	Success		19:54:23	Auditing	The most common types are 2 (interactive) and 3 (network). The New Logon fields indicate the account for whom the new logon was created, i.e. the account that was logged on. The network fields indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impersonation level field indicates the extent to which a process in the logon session can impersonate. The authentication information fields provide detailed information about this specific logon request. - Logon GUID is a unique identifier that can be used to correlate this event with a KDC event. - Transited services indicate which intermediate services have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indicates the length of the generated session key. This will be 0 if no session key was requested.
Security	Audit Success	12544	2015-04-22 19:54:23	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: LTRANPHD$ Account Domain: WORKGROUP Logon ID: 0x3e7 Logon Type: 5 Impersonation Level: %%1833 New Logon: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Logon ID: 0x3e7 Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x230 Process Name: C:\Windows\System32\services.exe Network Information: Workstation Name: Source Network Address: - Source Port: - Detailed Authentication Information: Logon Process: Advapi Authentication Package: Negotiate Transited Services: - Package Name (NTLM only): - Key Length: 0 This event is generated when a logon session is created. It is generated on the computer that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service such as the Server service, or a local process such as Winlogon.exe or Services.exe. The logon type field indicates the kind of logon that occurred. The most common types are 2 (interactive) and 3 (network). The New Logon fields indicate the account for whom the new logon was created, i.e. the account that was logged on. The network fields indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impersonation level field indicates the extent to which a process in the logon session can impersonate. The authentication information fields provide detailed information about this specific logon request. - Logon GUID is a unique identifier that can be used to correlate this event with a KDC event. - Transited services indicate which intermediate services have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indicates the length of the generated session key. This will be 0 if no session key was requested.
Security	Audit Success	12544	2015-04-22 19:54:23	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: LTRANPHD$ Account Domain: WORKGROUP Logon ID: 0x3e7 Logon Type: 5 Impersonation Level: %%1833 New Logon: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Logon ID: 0x3e7 Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x230 Process Name: C:\Windows\System32\services.exe Network Information: Workstation Name: Source Network Address: - Source Port: - Detailed Authentication Information: Logon Process: Advapi Authentication Package: Negotiate Transited Services: - Package Name (NTLM only): - Key Length: 0 This event is generated when a logon session is created. It is generated on the computer that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service such as the Server service, or a local process such as Winlogon.exe or Services.exe. The logon type field indicates the kind of logon that occurred. The most common types are 2 (interactive) and 3 (network). The New Logon fields indicate the account for whom the new logon was created, i.e. the account that was logged on. The network fields indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impersonation level field indicates the extent to which a process in the logon session can impersonate. The authentication information fields provide detailed information about this specific logon request. - Logon GUID is a unique identifier that can be used to correlate this event with a KDC event. - Transited services indicate which intermediate services have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indicates the length of the generated session key. This will be 0 if no session key was requested.
Security	Audit Success	12544	2015-04-22 19:54:23	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: LTRANPHD$ Account Domain: WORKGROUP Logon ID: 0x3e7 Logon Type: 5 Impersonation Level: %%1833 New Logon: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Logon ID: 0x3e7 Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x230 Process Name: C:\Windows\System32\services.exe Network Information: Workstation Name: Source Network Address: - Source Port: - Detailed Authentication Information: Logon Process: Advapi Authentication Package: Negotiate Transited Services: - Package Name (NTLM only): - Key Length: 0 This event is generated when a logon session is created. It is generated on the computer that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service such as the Server service, or a local process such as Winlogon.exe or Services.exe. The logon type field indicates the kind of logon that occurred. The most common types are 2 (interactive) and 3 (network). The New Logon fields indicate the account for whom the new logon was created, i.e. the account that was logged on. The network fields indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impersonation level field indicates the extent to which a process in the logon session can impersonate. The authentication information fields provide detailed information about this specific logon request. - Logon GUID is a unique identifier that can be used to correlate this event with a KDC event. - Transited services indicate which intermediate services have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indicates the length of the generated session key. This will be 0 if no session key was requested.

Security	Audit Success	12548	2015-04-22 19:54:23	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-19 Account Name: LOCAL SERVICE Account Domain: NT AUTHORITY Logon ID: 0x3e5 Privileges: SeAssignPrimaryTokenPrivilege SeAuditPrivilege SeImpersonatePrivilege
Security	Audit Success	12548	2015-04-22 19:54:23	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Logon ID: 0x3e7 Privileges: SeAssignPrimaryTokenPrivilege SeTcbPrivilege SeSecurityPrivilege SeTakeOwnershipPrivilege SeLoadDriverPrivilege SeBackupPrivilege SeRestorePrivilege SeDebugPrivilege SeAuditPrivilege SeSystemEnvironmentPrivilege SeImpersonatePrivilege
Security	Audit Success	12548	2015-04-22 19:54:23	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Logon ID: 0x3e7 Privileges: SeAssignPrimaryTokenPrivilege SeTcbPrivilege SeSecurityPrivilege SeTakeOwnershipPrivilege SeLoadDriverPrivilege SeBackupPrivilege SeRestorePrivilege SeDebugPrivilege SeAuditPrivilege SeSystemEnvironmentPrivilege SeImpersonatePrivilege
Security	Audit Success	12548	2015-04-22 19:54:23	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Logon ID: 0x3e7 Privileges: SeAssignPrimaryTokenPrivilege SeTcbPrivilege SeSecurityPrivilege SeTakeOwnershipPrivilege SeLoadDriverPrivilege SeBackupPrivilege SeRestorePrivilege SeDebugPrivilege SeAuditPrivilege SeSystemEnvironmentPrivilege SeImpersonatePrivilege
Security	Audit Success	12548	2015-04-22 19:54:23	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Logon ID: 0x3e7 Privileges: SeAssignPrimaryTokenPrivilege SeTcbPrivilege SeSecurityPrivilege SeTakeOwnershipPrivilege SeLoadDriverPrivilege SeBackupPrivilege SeRestorePrivilege SeDebugPrivilege SeAuditPrivilege SeSystemEnvironmentPrivilege SeImpersonatePrivilege
Security	Audit Success	12292	2015-04-22 19:54:24	Microsoft-Windows-Security-Auditing	5024: The Windows Firewall service started successfully.
Security	Audit Success	12544	2015-04-22 19:54:24	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: LTRANPHD$ Account Domain: WORKGROUP Logon ID: 0x3e7 Logon Type: 5 Impersonation Level: %%1833 New Logon: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Logon ID: 0x3e7 Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x230 Process Name: C:\Windows\System32\services.exe Network Information: Workstation Name: Source Network Address: - Source Port: - Detailed Authentication Information: Logon Process: Advapi Authentication Package: Negotiate Transited Services: - Package Name (NTLM only): - Key Length: 0 This event is generated when a logon session is created. It is generated on the computer that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service such as the Server service, or a local process such as Winlogon.exe or Services.exe. The logon type field indicates the kind of logon that occurred. The most common types are 2 (interactive) and 3 (network). The New Logon fields indicate the account for whom the new logon was created, i.e. the account that was logged on. The network fields indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impersonation level field indicates the extent to which a process in the logon session can impersonate. The authentication information fields provide detailed information about this specific logon request. - Logon GUID is a unique identifier that can be used to correlate this event with a KDC event. - Transited services indicate which intermediate services have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indicates the length of the generated session key. This will be 0 if no session key was requested.
Security	Audit Success	12544	2015-04-22 19:54:24	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-0-0 Account Name: - Account Domain: - Logon ID: 0x0 Logon Type: 3 Impersonation Level: %%1833 New Logon: Security ID: S-1-5-7 Account Name: ANONYMOUS LOGON Account Domain: NT AUTHORITY Logon ID: 0x1698f Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x0 Process Name: - Network Information: Workstation Name: Source Network Address: - Source Port: - Detailed Authentication Information: Logon Process: NtLmSsp Authentication Package: NTLM Transited Services: - Package Name (NTLM only): NTLM V1 Key Length: 0 This event is generated when a logon session is created. It is generated on the computer that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service such as the Server service, or a local process such as Winlogon.exe or Services.exe. The logon type field indicates the kind of logon that occurred. The most common types are 2 (interactive) and 3 (network). The New Logon fields indicate the account for whom the new logon was created, i.e. the account that was logged on. The network fields indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impersonation level field indicates the extent to which a process in the logon session can impersonate. The authentication information fields provide detailed information about this specific logon request. - Logon GUID is a unique identifier that can be used to correlate this event with a KDC event. - Transited services indicate which intermediate services have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indicates the length of the generated session key. This will be 0 if no session key was requested.
Security	Audit Success	12548	2015-04-22 19:54:24	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Logon ID: 0x3e7 Privileges: SeAssignPrimaryTokenPrivilege SeTcbPrivilege SeSecurityPrivilege SeTakeOwnershipPrivilege SeLoadDriverPrivilege SeBackupPrivilege SeRestorePrivilege SeDebugPrivilege SeAuditPrivilege SeSystemEnvironmentPrivilege SeImpersonatePrivilege
					4648: A logon was attempted using explicit credentials. Subject: Security ID: S-1-5-18 Account Name: LTRANPHD$ Account Domain: WORKGROUP Logon ID: 0x3e7 Logon GUID: {00000000-0000-0000-0000-

Security	Audit Success	12544	2015-04-22 19:54:25	Microsoft-Windows-Security-Auditing	000000000000} Account Whose Credentials Were Used: Account Name: Liem Account Domain: LTRANPHD Logon GUID: {00000000-0000-0000-0000-000000000000} Target Server: Target Server Name: localhost Additional Information: localhost Process Information: Process ID: 0x200 Process Name: C:\Windows\System32\winlogon.exe Network Information: Network Address: 127.0.0.1 Port: 0 This event is generated when a process attempts to log on an account by explicitly specifying that account's credentials. This most commonly occurs in batch-type configurations such as scheduled tasks, or when using the RUNAS command.
Security	Audit Success	12544	2015-04-22 19:54:25	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: LTRANPHD$ Account Domain: WORKGROUP Logon ID: 0x3e7 Logon Type: 2 Impersonation Level: %%1833 New Logon: Security ID: S-1-5-21-1888849264-3803429180-4108621888-1001 Account Name: Liem Account Domain: LTRANPHD Logon ID: 0x17c97 Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x200 Process Name: C:\Windows\System32\winlogon.exe Network Information: Workstation Name: LTRANPHD Source Network Address: 127.0.0.1 Source Port: 0 Detailed Authentication Information: Logon Process: User32 Authentication Package: Negotiate Transited Services: - Package Name (NTLM only): - Key Length: 0 This event is generated when a logon session is created. It is generated on the computer that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service such as the Server service, or a local process such as Winlogon.exe or Services.exe. The logon type field indicates the kind of logon that occurred. The most common types are 2 (interactive) and 3 (network). The New Logon fields indicate the account for whom the new logon was created, i.e. the account that was logged on. The network fields indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impersonation level field indicates the extent to which a process in the logon session can impersonate. The authentication information fields provide detailed information about this specific logon request. - Logon GUID is a unique identifier that can be used to correlate this event with a KDC event. - Transited services indicate which intermediate services have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indicates the length of the generated session key. This will be 0 if no session key was requested.
Security	Audit Success	12544	2015-04-22 19:54:25	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: LTRANPHD$ Account Domain: WORKGROUP Logon ID: 0x3e7 Logon Type: 2 Impersonation Level: %%1833 New Logon: Security ID: S-1-5-21-1888849264-3803429180-4108621888-1001 Account Name: Liem Account Domain: LTRANPHD Logon ID: 0x17cfb Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x200 Process Name: C:\Windows\System32\winlogon.exe Network Information: Workstation Name: LTRANPHD Source Network Address: 127.0.0.1 Source Port: 0 Detailed Authentication Information: Logon Process: User32 Authentication Package: Negotiate Transited Services: - Package Name (NTLM only): - Key Length: 0 This event is generated when a logon session is created. It is generated on the computer that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service such as the Server service, or a local process such as Winlogon.exe or Services.exe. The logon type field indicates the kind of logon that occurred. The most common types are 2 (interactive) and 3 (network). The New Logon fields indicate the account for whom the new logon was created, i.e. the account that was logged on. The network fields indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impersonation level field indicates the extent to which a process in the logon session can impersonate. The authentication information fields provide detailed information about this specific logon request. - Logon GUID is a unique identifier that can be used to correlate this event with a KDC event. - Transited services indicate which intermediate services have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indicates the length of the generated session key. This will be 0 if no session key was requested.
Security	Audit Success	12548	2015-04-22 19:54:25	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-21-1888849264-3803429180-4108621888-1001 Account Name: Liem Account Domain: LTRANPHD Logon ID: 0x17c97 Privileges: SeSecurityPrivilege SeTakeOwnershipPrivilege SeLoadDriverPrivilege SeBackupPrivilege SeRestorePrivilege SeDebugPrivilege SeSystemEnvironmentPrivilege SeImpersonatePrivilege
Security	Audit Success	12544	2015-04-22 19:54:26	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: LTRANPHD$ Account Domain: WORKGROUP Logon ID: 0x3e7 Logon Type: 5 Impersonation Level: %%1833 New Logon: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Logon ID: 0x3e7 Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x230 Process Name: C:\Windows\System32\services.exe Network Information: Workstation Name: Source Network Address: - Source Port: - Detailed Authentication Information: Logon Process: Advapi Authentication Package: Negotiate Transited Services: - Package Name (NTLM only): - Key Length: 0 This event is generated when a logon session is created. It is generated on the computer that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service such as the Server service, or a local process such as Winlogon.exe or Services.exe. The logon type field indicates the kind of logon that occurred. The most common types are 2 (interactive) and 3 (network). The New Logon fields indicate the account for whom the new logon was created, i.e. the account that was logged on. The network fields indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impersonation level field indicates the extent to which a process in the logon session can impersonate. The authentication information fields provide detailed information about this specific logon request. - Logon GUID is a unique identifier that can be used to correlate this event with a KDC event. - Transited services indicate which intermediate services have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indicates the length of the generated

					session key. This will be 0 if no session key was requested.
Security	Audit Success	12548	2015-04-22 19:54:26	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Logon ID: 0x3e7 Privileges: SeAssignPrimaryTokenPrivilege SeTcbPrivilege SeSecurityPrivilege SeTakeOwnershipPrivilege SeLoadDriverPrivilege SeBackupPrivilege SeRestorePrivilege SeDebugPrivilege SeAuditPrivilege SeSystemEnvironmentPrivilege SeImpersonatePrivilege
Security	Audit Success	13824	2015-04-22 19:54:28	Microsoft-Windows-Security-Auditing	4797: An attempt was made to query the existence of a blank password for an account. Subject: Security ID: S-1-5-21-1888849264-3803429180-4108621888-1001 Account Name: Liem Account Domain: LTRANPHD Logon ID: 0x17cfb Additional Information: Caller Workstation: LTRANPHD Target Account Name: Administrator Target Account Domain: LTRANPHD
Security	Audit Success	13824	2015-04-22 19:54:28	Microsoft-Windows-Security-Auditing	4797: An attempt was made to query the existence of a blank password for an account. Subject: Security ID: S-1-5-21-1888849264-3803429180-4108621888-1001 Account Name: Liem Account Domain: LTRANPHD Logon ID: 0x17cfb Additional Information: Caller Workstation: LTRANPHD Target Account Name: Guest Target Account Domain: LTRANPHD
Security	Audit Success	13824	2015-04-22 19:54:28	Microsoft-Windows-Security-Auditing	4797: An attempt was made to query the existence of a blank password for an account. Subject: Security ID: S-1-5-21-1888849264-3803429180-4108621888-1001 Account Name: Liem Account Domain: LTRANPHD Logon ID: 0x17cfb Additional Information: Caller Workstation: LTRANPHD Target Account Name: Administrator Target Account Domain: LTRANPHD
Security	Audit Success	13824	2015-04-22 19:54:28	Microsoft-Windows-Security-Auditing	4797: An attempt was made to query the existence of a blank password for an account. Subject: Security ID: S-1-5-21-1888849264-3803429180-4108621888-1001 Account Name: Liem Account Domain: LTRANPHD Logon ID: 0x17cfb Additional Information: Caller Workstation: LTRANPHD Target Account Name: Guest Target Account Domain: LTRANPHD
Security	Audit Success	13824	2015-04-22 19:54:32	Microsoft-Windows-Security-Auditing	4797: An attempt was made to query the existence of a blank password for an account. Subject: Security ID: S-1-5-19 Account Name: LOCAL SERVICE Account Domain: NT AUTHORITY Logon ID: 0x3e5 Additional Information: Caller Workstation: LTRANPHD Target Account Name: Administrator Target Account Domain: LTRANPHD
Security	Audit Success	13824	2015-04-22 19:54:32	Microsoft-Windows-Security-Auditing	4797: An attempt was made to query the existence of a blank password for an account. Subject: Security ID: S-1-5-19 Account Name: LOCAL SERVICE Account Domain: NT AUTHORITY Logon ID: 0x3e5 Additional Information: Caller Workstation: LTRANPHD Target Account Name: Guest Target Account Domain: LTRANPHD
Security	Audit Success	13824	2015-04-22 19:54:32	Microsoft-Windows-Security-Auditing	4797: An attempt was made to query the existence of a blank password for an account. Subject: Security ID: S-1-5-19 Account Name: LOCAL SERVICE Account Domain: NT AUTHORITY Logon ID: 0x3e5 Additional Information: Caller Workstation: LTRANPHD Target Account Name: Administrator Target Account Domain: LTRANPHD
Security	Audit Success	13824	2015-04-22 19:54:32	Microsoft-Windows-Security-Auditing	4797: An attempt was made to query the existence of a blank password for an account. Subject: Security ID: S-1-5-19 Account Name: LOCAL SERVICE Account Domain: NT AUTHORITY Logon ID: 0x3e5 Additional Information: Caller Workstation: LTRANPHD Target Account Name: Liem Target Account Domain: LTRANPHD
Security	Audit Success	13824	2015-04-22 19:54:32	Microsoft-Windows-Security-Auditing	4797: An attempt was made to query the existence of a blank password for an account. Subject: Security ID: S-1-5-19 Account Name: LOCAL SERVICE Account Domain: NT AUTHORITY Logon ID: 0x3e5 Additional Information: Caller Workstation: LTRANPHD Target Account Name: Guest Target Account Domain: LTRANPHD
Security	Audit Success	13824	2015-04-22 19:54:32	Microsoft-Windows-Security-Auditing	4797: An attempt was made to query the existence of a blank password for an account. Subject: Security ID: S-1-5-19 Account Name: LOCAL SERVICE Account Domain: NT AUTHORITY Logon ID: 0x3e5 Additional Information: Caller Workstation: LTRANPHD Target Account Name: Liem Target Account Domain: LTRANPHD
Security	Audit Success	13824	2015-04-22 19:54:32	Microsoft-Windows-Security-Auditing	4797: An attempt was made to query the existence of a blank password for an account. Subject: Security ID: S-1-5-19 Account Name: LOCAL SERVICE Account Domain: NT AUTHORITY Logon ID: 0x3e5 Additional Information: Caller Workstation: LTRANPHD Target Account Name: Liem Target Account Domain: LTRANPHD
Security	Audit Success	13824	2015-04-22 19:54:53	Microsoft-Windows-Security-Auditing	4797: An attempt was made to query the existence of a blank password for an account. Subject: Security ID: S-1-5-21-1888849264-3803429180-4108621888-1001 Account Name: Liem Account Domain: LTRANPHD Logon ID: 0x17cfb Additional Information: Caller Workstation: LTRANPHD Target Account Name: Administrator Target Account Domain: LTRANPHD
Security	Audit Success	12544	2015-04-22 19:55:18	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: LTRANPHD$ Account Domain: WORKGROUP Logon ID: 0x3e7 Logon Type: 5 Impersonation Level: %%1833 New Logon: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Logon ID: 0x3e7 Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x230 Process Name: C:\Windows\System32\services.exe Network Information: Workstation Name: Source Network Address: - Source Port: - Detailed Authentication Information: Logon Process: Advapi Authentication Package: Negotiate Transited Services: - Package Name (NTLM only): - Key Length: 0 This event is generated when a logon session is created. It is generated on the computer that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service such as the Server service, or a local process such as Winlogon.exe or Services.exe. The logon type field indicates the kind of logon that occurred. The most common types are 2 (interactive) and 3 (network). The New Logon fields indicate the account for whom the new logon was created, i.e. the account that was logged on. The network fields indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some

					cases. The impersonation level field indicates the extent to which a process in the logon session can impersonate. The authentication information fields provide detailed information about this specific logon request. - Logon GUID is a unique identifier that can be used to correlate this event with a KDC event. - Transited services indicate which intermediate services have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indicates the length of the generated session key. This will be 0 if no session key was requested.
Security	Audit Success	12548	2015-04-22 19:55:18	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Logon ID: 0x3e7 Privileges: SeAssignPrimaryTokenPrivilege SeTcbPrivilege SeSecurityPrivilege SeTakeOwnershipPrivilege SeLoadDriverPrivilege SeBackupPrivilege SeRestorePrivilege SeDebugPrivilege SeAuditPrivilege SeSystemEnvironmentPrivilege SeImpersonatePrivilege
Security	Audit Success	12544	2015-04-22 19:55:19	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: LTRANPHD$ Account Domain: WORKGROUP Logon ID: 0x3e7 Logon Type: 5 Impersonation Level: %%1833 New Logon: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Logon ID: 0x3e7 Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x230 Process Name: C:\Windows\System32\services.exe Network Information: Workstation Name: Source Network Address: - Source Port: - Detailed Authentication Information: Logon Process: Advapi Authentication Package: Negotiate Transited Services: - Package Name (NTLM only): - Key Length: 0 This event is generated when a logon session is created. It is generated on the computer that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service such as the Server service, or a local process such as Winlogon.exe or Services.exe. The logon type field indicates the kind of logon that occurred. The most common types are 2 (interactive) and 3 (network). The New Logon fields indicate the account for whom the new logon was created, i.e. the account that was logged on. The network fields indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impersonation level field indicates the extent to which a process in the logon session can impersonate. The authentication information fields provide detailed information about this specific logon request. - Logon GUID is a unique identifier that can be used to correlate this event with a KDC event. - Transited services indicate which intermediate services have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indicates the length of the generated session key. This will be 0 if no session key was requested.
Security	Audit Success	12548	2015-04-22 19:55:19	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Logon ID: 0x3e7 Privileges: SeAssignPrimaryTokenPrivilege SeTcbPrivilege SeSecurityPrivilege SeTakeOwnershipPrivilege SeLoadDriverPrivilege SeBackupPrivilege SeRestorePrivilege SeDebugPrivilege SeAuditPrivilege SeSystemEnvironmentPrivilege SeImpersonatePrivilege
Security	Audit Success	12544	2015-04-22 19:57:37	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: LTRANPHD$ Account Domain: WORKGROUP Logon ID: 0x3e7 Logon Type: 5 Impersonation Level: %%1833 New Logon: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Logon ID: 0x3e7 Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x230 Process Name: C:\Windows\System32\services.exe Network Information: Workstation Name: Source Network Address: - Source Port: - Detailed Authentication Information: Logon Process: Advapi Authentication Package: Negotiate Transited Services: - Package Name (NTLM only): - Key Length: 0 This event is generated when a logon session is created. It is generated on the computer that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service such as the Server service, or a local process such as Winlogon.exe or Services.exe. The logon type field indicates the kind of logon that occurred. The most common types are 2 (interactive) and 3 (network). The New Logon fields indicate the account for whom the new logon was created, i.e. the account that was logged on. The network fields indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impersonation level field indicates the extent to which a process in the logon session can impersonate. The authentication information fields provide detailed information about this specific logon request. - Logon GUID is a unique identifier that can be used to correlate this event with a KDC event. - Transited services indicate which intermediate services have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indicates the length of the generated session key. This will be 0 if no session key was requested.
Security	Audit Success	12548	2015-04-22 19:57:37	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Logon ID: 0x3e7 Privileges: SeAssignPrimaryTokenPrivilege SeTcbPrivilege SeSecurityPrivilege SeTakeOwnershipPrivilege SeLoadDriverPrivilege SeBackupPrivilege SeRestorePrivilege SeDebugPrivilege SeAuditPrivilege SeSystemEnvironmentPrivilege SeImpersonatePrivilege
Security	Audit Success	12544	2015-04-22	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: LTRANPHD$ Account Domain: WORKGROUP Logon ID: 0x3e7 Logon Type: 5 Impersonation Level: %%1833 New Logon: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Logon ID: 0x3e7 Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x230 Process Name: C:\Windows\System32\services.exe Network Information: Workstation Name: Source Network Address: - Source Port: - Detailed Authentication Information: Logon Process: Advapi Authentication Package: Negotiate Transited Services: - Package Name (NTLM only): - Key Length: 0 This event is generated when a logon session is created. It is generated on the computer that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service such as the Server service, or a local process such as Winlogon.exe or Services.exe. The logon type field indicates the kind of logon that occurred.

			19:57:57		The most common types are 2 (interactive) and 3 (network). The New Logon fields indicate the account for whom the new logon was created, i.e. the account that was logged on. The network fields indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impersonation level field indicates the extent to which a process in the logon session can impersonate. The authentication information fields provide detailed information about this specific logon request. - Logon GUID is a unique identifier that can be used to correlate this event with a KDC event. - Transited services indicate which intermediate services have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indicates the length of the generated session key. This will be 0 if no session key was requested.
Security	Audit Success	12548	2015-04-22 19:57:57	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Logon ID: 0x3e7 Privileges: SeAssignPrimaryTokenPrivilege SeTcbPrivilege SeSecurityPrivilege SeTakeOwnershipPrivilege SeLoadDriverPrivilege SeBackupPrivilege SeRestorePrivilege SeDebugPrivilege SeAuditPrivilege SeSystemEnvironmentPrivilege SeImpersonatePrivilege
Security	Audit Success	13824	2015-04-22 20:06:42	Microsoft-Windows-Security-Auditing	4797: An attempt was made to query the existence of a blank password for an account. Subject: Security ID: S-1-5-21-1888849264-3803429180-4108621888-1001 Account Name: Liem Account Domain: LTRANPHD Logon ID: 0x17cfb Additional Information: Caller Workstation: LTRANPHD Target Account Name: Administrator Target Account Domain: LTRANPHD
Security	Audit Success	13824	2015-04-22 20:06:42	Microsoft-Windows-Security-Auditing	4797: An attempt was made to query the existence of a blank password for an account. Subject: Security ID: S-1-5-21-1888849264-3803429180-4108621888-1001 Account Name: Liem Account Domain: LTRANPHD Logon ID: 0x17cfb Additional Information: Caller Workstation: LTRANPHD Target Account Name: Guest Target Account Domain: LTRANPHD
Security	Audit Success	13824	2015-04-22 20:06:42	Microsoft-Windows-Security-Auditing	4797: An attempt was made to query the existence of a blank password for an account. Subject: Security ID: S-1-5-21-1888849264-3803429180-4108621888-1001 Account Name: Liem Account Domain: LTRANPHD Logon ID: 0x17cfb Additional Information: Caller Workstation: LTRANPHD Target Account Name: Administrator Target Account Domain: LTRANPHD
Security	Audit Success	13824	2015-04-22 20:06:42	Microsoft-Windows-Security-Auditing	4797: An attempt was made to query the existence of a blank password for an account. Subject: Security ID: S-1-5-21-1888849264-3803429180-4108621888-1001 Account Name: Liem Account Domain: LTRANPHD Logon ID: 0x17cfb Additional Information: Caller Workstation: LTRANPHD Target Account Name: Guest Target Account Domain: LTRANPHD
Security	Audit Failure	12290	2015-04-22 20:07:23	Microsoft-Windows-Security-Auditing	5061: Cryptographic operation. Subject: Security ID: S-1-5-21-1888849264-3803429180-4108621888-1001 Account Name: Liem Account Domain: LTRANPHD Logon ID: 0x17cfb Cryptographic Parameters: Provider Name: Microsoft Software Key Storage Provider Algorithm Name: UNKNOWN Key Name: CD1CC265-0DA0-4230-8419-CB6F808FE688 Key Type: %%2500 Cryptographic Operation: Operation: %%2480 Return Code: 0x80090016
Security	Audit Failure	12290	2015-04-22 20:07:23	Microsoft-Windows-Security-Auditing	5061: Cryptographic operation. Subject: Security ID: S-1-5-21-1888849264-3803429180-4108621888-1001 Account Name: Liem Account Domain: LTRANPHD Logon ID: 0x17cfb Cryptographic Parameters: Provider Name: Microsoft Software Key Storage Provider Algorithm Name: UNKNOWN Key Name: CD1CC265-0DA0-4230-8419-CB6F808FE688 Key Type: %%2500 Cryptographic Operation: Operation: %%2480 Return Code: 0x80090016
Security	Audit Failure	12290	2015-04-22 20:07:23	Microsoft-Windows-Security-Auditing	5061: Cryptographic operation. Subject: Security ID: S-1-5-21-1888849264-3803429180-4108621888-1001 Account Name: Liem Account Domain: LTRANPHD Logon ID: 0x17cfb Cryptographic Parameters: Provider Name: Microsoft Software Key Storage Provider Algorithm Name: UNKNOWN Key Name: CD1CC265-0DA0-4230-8419-CB6F808FE688 Key Type: %%2500 Cryptographic Operation: Operation: %%2480 Return Code: 0x80090016
Security	Audit Success	12544	2015-04-22 20:07:54	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: LTRANPHD$ Account Domain: WORKGROUP Logon ID: 0x3e7 Logon Type: 5 Impersonation Level: %%1833 New Logon: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Logon ID: 0x3e7 Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x230 Process Name: C:\Windows\System32\services.exe Network Information: Workstation Name: Source Network Address: - Source Port: - Detailed Authentication Information: Logon Process: Advapi Authentication Package: Negotiate Transited Services: - Package Name (NTLM only): - Key Length: 0 This event is generated when a logon session is created. It is generated on the computer that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service such as the Server service, or a local process such as Winlogon.exe or Services.exe. The logon type field indicates the kind of logon that occurred. The most common types are 2 (interactive) and 3 (network). The New Logon fields indicate the account for whom the new logon was created, i.e. the account that was logged on. The network fields indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impersonation level field indicates the extent to which a process in the logon session can impersonate. The authentication information fields provide detailed information about this specific logon request. - Logon GUID is a unique identifier that can be used to correlate this event with a KDC event. - Transited services indicate which intermediate services have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indicates the length of the generated session key. This will be 0 if no session key was requested.
Security	Audit Success	12548	2015-04-22 20:07:54	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Logon ID: 0x3e7 Privileges: SeAssignPrimaryTokenPrivilege SeTcbPrivilege SeSecurityPrivilege SeTakeOwnershipPrivilege SeLoadDriverPrivilege SeBackupPrivilege SeRestorePrivilege SeDebugPrivilege SeAuditPrivilege SeSystemEnvironmentPrivilege SeImpersonatePrivilege
					4797: An attempt was made to query the existence of a blank password for an account. Subject: Security ID:

Security	Audit Success	13824	2015-04-22 20:07:54	Microsoft-Windows-Security-Auditing	S-1-5-21-1888849264-3803429180-4108621888-1001 Account Name: Liem Account Domain: LTRANPHD Logon ID: 0x17cfb Additional Information: Caller Workstation: LTRANPHD Target Account Name: Administrator Target Account Domain: LTRANPHD
Security	Audit Success	12288	2015-04-22 20:24:36	Microsoft-Windows-Security-Auditing	4608: Windows is starting up. This event is logged when LSASS.EXE starts and the auditing subsystem is initialized.
Security	Audit Success	12544	2015-04-22 20:24:36	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-0-0 Account Name: - Account Domain: - Logon ID: 0x0 Logon Type: 0 Impersonation Level: - New Logon: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Logon ID: 0x3e7 Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x4 Process Name: Network Information: Workstation Name: - Source Network Address: - Source Port: - Detailed Authentication Information: Logon Process: - Authentication Package: - Transited Services: - Package Name (NTLM only): - Key Length: 0 This event is generated when a logon session is created. It is generated on the computer that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service such as the Server service, or a local process such as Winlogon.exe or Services.exe. The logon type field indicates the kind of logon that occurred. The most common types are 2 (interactive) and 3 (network). The New Logon fields indicate the account for whom the new logon was created, i.e. the account that was logged on. The network fields indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impersonation level field indicates the extent to which a process in the logon session can impersonate. The authentication information fields provide detailed information about this specific logon request. - Logon GUID is a unique identifier that can be used to correlate this event with a KDC event. - Transited services indicate which intermediate services have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indicates the length of the generated session key. This will be 0 if no session key was requested.
Security	Audit Success	13568	2015-04-22 20:24:36	Microsoft-Windows-Security-Auditing	4902: The Per-user audit policy table was created. Number of Elements: 0 Policy ID: 0x7e96
Security	Audit Success	12544	2015-04-22 20:24:37	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: LTRANPHD$ Account Domain: WORKGROUP Logon ID: 0x3e7 Logon Type: 5 Impersonation Level: %%1833 New Logon: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Logon ID: 0x3e7 Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x228 Process Name: C:\Windows\System32\services.exe Network Information: Workstation Name: Source Network Address: - Source Port: - Detailed Authentication Information: Logon Process: Advapi Authentication Package: Negotiate Transited Services: - Package Name (NTLM only): - Key Length: 0 This event is generated when a logon session is created. It is generated on the computer that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service such as the Server service, or a local process such as Winlogon.exe or Services.exe. The logon type field indicates the kind of logon that occurred. The most common types are 2 (interactive) and 3 (network). The New Logon fields indicate the account for whom the new logon was created, i.e. the account that was logged on. The network fields indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impersonation level field indicates the extent to which a process in the logon session can impersonate. The authentication information fields provide detailed information about this specific logon request. - Logon GUID is a unique identifier that can be used to correlate this event with a KDC event. - Transited services indicate which intermediate services have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indicates the length of the generated session key. This will be 0 if no session key was requested.
Security	Audit Success	12544	2015-04-22 20:24:37	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: LTRANPHD$ Account Domain: WORKGROUP Logon ID: 0x3e7 Logon Type: 5 Impersonation Level: %%1833 New Logon: Security ID: S-1-5-20 Account Name: NETWORK SERVICE Account Domain: NT AUTHORITY Logon ID: 0x3e4 Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x228 Process Name: C:\Windows\System32\services.exe Network Information: Workstation Name: Source Network Address: - Source Port: - Detailed Authentication Information: Logon Process: Advapi Authentication Package: Negotiate Transited Services: - Package Name (NTLM only): - Key Length: 0 This event is generated when a logon session is created. It is generated on the computer that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service such as the Server service, or a local process such as Winlogon.exe or Services.exe. The logon type field indicates the kind of logon that occurred. The most common types are 2 (interactive) and 3 (network). The New Logon fields indicate the account for whom the new logon was created, i.e. the account that was logged on. The network fields indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impersonation level field indicates the extent to which a process in the logon session can impersonate. The authentication information fields provide detailed information about this specific logon request. - Logon GUID is a unique identifier that can be used to correlate this event with a KDC event. - Transited services indicate which intermediate services have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indicates the length of the generated session key. This will be 0 if no session key was requested.
					4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account

Security	Audit Success	12548	2015-04-22 20:24:37	Microsoft-Windows-Security-Auditing	Domain: NT AUTHORITY Logon ID: 0x3e7 Privileges: SeAssignPrimaryTokenPrivilege SeTcbPrivilege SeSecurityPrivilege SeTakeOwnershipPrivilege SeLoadDriverPrivilege SeBackupPrivilege SeRestorePrivilege SeDebugPrivilege SeAuditPrivilege SeSystemEnvironmentPrivilege SeImpersonatePrivilege
Security	Audit Success	12548	2015-04-22 20:24:37	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-20 Account Name: NETWORK SERVICE Account Domain: NT AUTHORITY Logon ID: 0x3e4 Privileges: SeAssignPrimaryTokenPrivilege SeAuditPrivilege SeImpersonatePrivilege
Security	Audit Success	12544	2015-04-22 20:24:38	Microsoft-Windows-Security-Auditing	4648: A logon was attempted using explicit credentials. Subject: Security ID: S-1-5-18 Account Name: LTRANPHD$ Account Domain: WORKGROUP Logon ID: 0x3e7 Logon GUID: {00000000-0000-0000-0000-000000000000} Account Whose Credentials Were Used: Account Name: DWM-1 Account Domain: Window Manager Logon GUID: {00000000-0000-0000-0000-000000000000} Target Server: Target Server Name: localhost Additional Information: localhost Process Information: Process ID: 0x200 Process Name: C:\Windows\System32\winlogon.exe Network Information: Network Address: - Port: - This event is generated when a process attempts to log on an account by explicitly specifying that account's credentials. This most commonly occurs in batch-type configurations such as scheduled tasks, or when using the RUNAS command.
Security	Audit Success	12544	2015-04-22 20:24:38	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: LTRANPHD$ Account Domain: WORKGROUP Logon ID: 0x3e7 Logon Type: 2 Impersonation Level: %%1833 New Logon: Security ID: S-1-5-90-1 Account Name: DWM-1 Account Domain: Window Manager Logon ID: 0xe5d4 Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x200 Process Name: C:\Windows\System32\winlogon.exe Network Information: Workstation Name: Source Network Address: - Source Port: - Detailed Authentication Information: Logon Process: Advapi Authentication Package: Negotiate Transited Services: - Package Name (NTLM only): - Key Length: 0 This event is generated when a logon session is created. It is generated on the computer that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service such as the Server service, or a local process such as Winlogon.exe or Services.exe. The logon type field indicates the kind of logon that occurred. The most common types are 2 (interactive) and 3 (network). The New Logon fields indicate the account for whom the new logon was created, i.e. the account that was logged on. The network fields indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impersonation level field indicates the extent to which a process in the logon session can impersonate. The authentication information fields provide detailed information about this specific logon request. - Logon GUID is a unique identifier that can be used to correlate this event with a KDC event. - Transited services indicate which intermediate services have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indicates the length of the generated session key. This will be 0 if no session key was requested.
Security	Audit Success	12544	2015-04-22 20:24:38	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: LTRANPHD$ Account Domain: WORKGROUP Logon ID: 0x3e7 Logon Type: 2 Impersonation Level: %%1833 New Logon: Security ID: S-1-5-90-1 Account Name: DWM-1 Account Domain: Window Manager Logon ID: 0xe5f2 Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x200 Process Name: C:\Windows\System32\winlogon.exe Network Information: Workstation Name: Source Network Address: - Source Port: - Detailed Authentication Information: Logon Process: Advapi Authentication Package: Negotiate Transited Services: - Package Name (NTLM only): - Key Length: 0 This event is generated when a logon session is created. It is generated on the computer that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service such as the Server service, or a local process such as Winlogon.exe or Services.exe. The logon type field indicates the kind of logon that occurred. The most common types are 2 (interactive) and 3 (network). The New Logon fields indicate the account for whom the new logon was created, i.e. the account that was logged on. The network fields indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impersonation level field indicates the extent to which a process in the logon session can impersonate. The authentication information fields provide detailed information about this specific logon request. - Logon GUID is a unique identifier that can be used to correlate this event with a KDC event. - Transited services indicate which intermediate services have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indicates the length of the generated session key. This will be 0 if no session key was requested.
Security	Audit Success	12544	2015-04-22 20:24:38	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: LTRANPHD$ Account Domain: WORKGROUP Logon ID: 0x3e7 Logon Type: 5 Impersonation Level: %%1833 New Logon: Security ID: S-1-5-19 Account Name: LOCAL SERVICE Account Domain: NT AUTHORITY Logon ID: 0x3e5 Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x228 Process Name: C:\Windows\System32\services.exe Network Information: Workstation Name: Source Network Address: - Source Port: - Detailed Authentication Information: Logon Process: Advapi Authentication Package: Negotiate Transited Services: - Package Name (NTLM only): - Key Length: 0 This event is generated when a logon session is created. It is generated on the computer that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service such as the Server service, or a local process such as Winlogon.exe or Services.exe. The logon type field indicates the kind of logon that occurred. The most common types are 2 (interactive) and 3 (network). The New Logon fields indicate the account for whom the new logon was created, i.e. the account that was logged on. The network fields indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impersonation level field indicates the extent to which a process in the logon session can

					impersonate. The authentication information fields provide detailed information about this specific logon request. - Logon GUID is a unique identifier that can be used to correlate this event with a KDC event. - Transited services indicate which intermediate services have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indicates the length of the generated session key. This will be 0 if no session key was requested.
Security	Audit Success	12544	2015-04-22 20:24:38	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: LTRANPHD$ Account Domain: WORKGROUP Logon ID: 0x3e7 Logon Type: 5 Impersonation Level: %%1833 New Logon: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Logon ID: 0x3e7 Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x228 Process Name: C:\Windows\System32\services.exe Network Information: Workstation Name: Source Network Address: - Source Port: - Detailed Authentication Information: Logon Process: Advapi Authentication Package: Negotiate Transited Services: - Package Name (NTLM only): - Key Length: 0 This event is generated when a logon session is created. It is generated on the computer that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service such as the Server service, or a local process such as Winlogon.exe or Services.exe. The logon type field indicates the kind of logon that occurred. The most common types are 2 (interactive) and 3 (network). The New Logon fields indicate the account for whom the new logon was created, i.e. the account that was logged on. The network fields indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impersonation level field indicates the extent to which a process in the logon session can impersonate. The authentication information fields provide detailed information about this specific logon request. - Logon GUID is a unique identifier that can be used to correlate this event with a KDC event. - Transited services indicate which intermediate services have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indicates the length of the generated session key. This will be 0 if no session key was requested.
Security	Audit Success	12548	2015-04-22 20:24:38	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-90-1 Account Name: DWM-1 Account Domain: Window Manager Logon ID: 0xe5d4 Privileges: SeAssignPrimaryTokenPrivilege SeAuditPrivilege SeImpersonatePrivilege
Security	Audit Success	12548	2015-04-22 20:24:38	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-90-1 Account Name: DWM-1 Account Domain: Window Manager Logon ID: 0xe5f2 Privileges: SeAssignPrimaryTokenPrivilege SeAuditPrivilege
Security	Audit Success	12548	2015-04-22 20:24:38	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-19 Account Name: LOCAL SERVICE Account Domain: NT AUTHORITY Logon ID: 0x3e5 Privileges: SeAssignPrimaryTokenPrivilege SeAuditPrivilege SeImpersonatePrivilege
Security	Audit Success	12548	2015-04-22 20:24:38	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Logon ID: 0x3e7 Privileges: SeAssignPrimaryTokenPrivilege SeTcbPrivilege SeSecurityPrivilege SeTakeOwnershipPrivilege SeLoadDriverPrivilege SeBackupPrivilege SeRestorePrivilege SeDebugPrivilege SeAuditPrivilege SeSystemEnvironmentPrivilege SeImpersonatePrivilege
Security	Audit Success	101	2015-04-22 20:24:39	Microsoft-Windows-Eventlog	1101: Audit events have been dropped by the transport. 0
Security	Audit Success	12292	2015-04-22 20:24:39	Microsoft-Windows-Security-Auditing	5033: The Windows Firewall Driver started successfully.
Security	Audit Success	12544	2015-04-22 20:24:39	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: LTRANPHD$ Account Domain: WORKGROUP Logon ID: 0x3e7 Logon Type: 5 Impersonation Level: %%1833 New Logon: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Logon ID: 0x3e7 Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x228 Process Name: C:\Windows\System32\services.exe Network Information: Workstation Name: Source Network Address: - Source Port: - Detailed Authentication Information: Logon Process: Advapi Authentication Package: Negotiate Transited Services: - Package Name (NTLM only): - Key Length: 0 This event is generated when a logon session is created. It is generated on the computer that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service such as the Server service, or a local process such as Winlogon.exe or Services.exe. The logon type field indicates the kind of logon that occurred. The most common types are 2 (interactive) and 3 (network). The New Logon fields indicate the account for whom the new logon was created, i.e. the account that was logged on. The network fields indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impersonation level field indicates the extent to which a process in the logon session can impersonate. The authentication information fields provide detailed information about this specific logon request. - Logon GUID is a unique identifier that can be used to correlate this event with a KDC event. - Transited services indicate which intermediate services have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indicates the length of the generated session key. This will be 0 if no session key was requested.
					4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: LTRANPHD$ Account Domain: WORKGROUP Logon ID: 0x3e7 Logon Type: 5 Impersonation Level: %%1833 New Logon: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Logon ID: 0x3e7 Logon GUID:

Security	Audit Success	12544	2015-04-22 20:24:39	Microsoft-Windows-Security-Auditing	{00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x228 Process Name: C:\Windows\System32\services.exe Network Information: Workstation Name: Source Network Address: - Source Port: - Detailed Authentication Information: Logon Process: Advapi Authentication Package: Negotiate Transited Services: - Package Name (NTLM only): - Key Length: 0 This event is generated when a logon session is created. It is generated on the computer that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service such as the Server service, or a local process such as Winlogon.exe or Services.exe. The logon type field indicates the kind of logon that occurred. The most common types are 2 (interactive) and 3 (network). The New Logon fields indicate the account for whom the new logon was created, i.e. the account that was logged on. The network fields indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impersonation level field indicates the extent to which a process in the logon session can impersonate. The authentication information fields provide detailed information about this specific logon request. - Logon GUID is a unique identifier that can be used to correlate this event with a KDC event. - Transited services indicate which intermediate services have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indicates the length of the generated session key. This will be 0 if no session key was requested.
Security	Audit Success	12544	2015-04-22 20:24:39	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: LTRANPHD$ Account Domain: WORKGROUP Logon ID: 0x3e7 Logon Type: 5 Impersonation Level: %%1833 New Logon: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Logon ID: 0x3e7 Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x228 Process Name: C:\Windows\System32\services.exe Network Information: Workstation Name: Source Network Address: - Source Port: - Detailed Authentication Information: Logon Process: Advapi Authentication Package: Negotiate Transited Services: - Package Name (NTLM only): - Key Length: 0 This event is generated when a logon session is created. It is generated on the computer that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service such as the Server service, or a local process such as Winlogon.exe or Services.exe. The logon type field indicates the kind of logon that occurred. The most common types are 2 (interactive) and 3 (network). The New Logon fields indicate the account for whom the new logon was created, i.e. the account that was logged on. The network fields indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impersonation level field indicates the extent to which a process in the logon session can impersonate. The authentication information fields provide detailed information about this specific logon request. - Logon GUID is a unique identifier that can be used to correlate this event with a KDC event. - Transited services indicate which intermediate services have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indicates the length of the generated session key. This will be 0 if no session key was requested.
Security	Audit Success	12548	2015-04-22 20:24:39	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Logon ID: 0x3e7 Privileges: SeAssignPrimaryTokenPrivilege SeTcbPrivilege SeSecurityPrivilege SeTakeOwnershipPrivilege SeLoadDriverPrivilege SeBackupPrivilege SeRestorePrivilege SeDebugPrivilege SeAuditPrivilege SeSystemEnvironmentPrivilege SeImpersonatePrivilege
Security	Audit Success	12548	2015-04-22 20:24:39	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Logon ID: 0x3e7 Privileges: SeAssignPrimaryTokenPrivilege SeTcbPrivilege SeSecurityPrivilege SeTakeOwnershipPrivilege SeLoadDriverPrivilege SeBackupPrivilege SeRestorePrivilege SeDebugPrivilege SeAuditPrivilege SeSystemEnvironmentPrivilege SeImpersonatePrivilege
Security	Audit Success	12548	2015-04-22 20:24:39	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Logon ID: 0x3e7 Privileges: SeAssignPrimaryTokenPrivilege SeTcbPrivilege SeSecurityPrivilege SeTakeOwnershipPrivilege SeLoadDriverPrivilege SeBackupPrivilege SeRestorePrivilege SeDebugPrivilege SeAuditPrivilege SeSystemEnvironmentPrivilege SeImpersonatePrivilege
Security	Audit Success	12292	2015-04-22 20:24:40	Microsoft-Windows-Security-Auditing	5024: The Windows Firewall service started successfully.
Security	Audit Success	12544	2015-04-22 20:24:40	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: LTRANPHD$ Account Domain: WORKGROUP Logon ID: 0x3e7 Logon Type: 5 Impersonation Level: %%1833 New Logon: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Logon ID: 0x3e7 Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x228 Process Name: C:\Windows\System32\services.exe Network Information: Workstation Name: Source Network Address: - Source Port: - Detailed Authentication Information: Logon Process: Advapi Authentication Package: Negotiate Transited Services: - Package Name (NTLM only): - Key Length: 0 This event is generated when a logon session is created. It is generated on the computer that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service such as the Server service, or a local process such as Winlogon.exe or Services.exe. The logon type field indicates the kind of logon that occurred. The most common types are 2 (interactive) and 3 (network). The New Logon fields indicate the account for whom the new logon was created, i.e. the account that was logged on. The network fields indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impersonation level field indicates the extent to which a process in the logon session can impersonate. The authentication information fields provide detailed information about this specific logon request. - Logon GUID is a unique identifier that can be used to correlate this event with a KDC event. - Transited

					services indicate which intermediate services have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indicates the length of the generated session key. This will be 0 if no session key was requested.
Security	Audit Success	12544	2015-04-22 20:24:40	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-0-0 Account Name: - Account Domain: - Logon ID: 0x0 Logon Type: 3 Impersonation Level: %%1833 New Logon: Security ID: S-1-5-7 Account Name: ANONYMOUS LOGON Account Domain: NT AUTHORITY Logon ID: 0x18433 Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x0 Process Name: - Network Information: Workstation Name: Source Network Address: - Source Port: - Detailed Authentication Information: Logon Process: NtLmSsp Authentication Package: NTLM Transited Services: - Package Name (NTLM only): NTLM V1 Key Length: 0 This event is generated when a logon session is created. It is generated on the computer that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service such as the Server service, or a local process such as Winlogon.exe or Services.exe. The logon type field indicates the kind of logon that occurred. The most common types are 2 (interactive) and 3 (network). The New Logon fields indicate the account for whom the new logon was created, i.e. the account that was logged on. The network fields indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impersonation level field indicates the extent to which a process in the logon session can impersonate. The authentication information fields provide detailed information about this specific logon request. - Logon GUID is a unique identifier that can be used to correlate this event with a KDC event. - Transited services indicate which intermediate services have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indicates the length of the generated session key. This will be 0 if no session key was requested.
Security	Audit Success	12548	2015-04-22 20:24:40	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Logon ID: 0x3e7 Privileges: SeAssignPrimaryTokenPrivilege SeTcbPrivilege SeSecurityPrivilege SeTakeOwnershipPrivilege SeLoadDriverPrivilege SeBackupPrivilege SeRestorePrivilege SeDebugPrivilege SeAuditPrivilege SeSystemEnvironmentPrivilege SeImpersonatePrivilege
Security	Audit Success	12544	2015-04-22 20:24:45	Microsoft-Windows-Security-Auditing	4648: A logon was attempted using explicit credentials. Subject: Security ID: S-1-5-18 Account Name: LTRANPHD$ Account Domain: WORKGROUP Logon ID: 0x3e7 Logon GUID: {00000000-0000-0000-0000-000000000000} Account Whose Credentials Were Used: Account Name: Liem Account Domain: LTRANPHD Logon GUID: {00000000-0000-0000-0000-000000000000} Target Server: Target Server Name: localhost Additional Information: localhost Process Information: Process ID: 0x200 Process Name: C:\Windows\System32\winlogon.exe Network Information: Network Address: 127.0.0.1 Port: 0 This event is generated when a process attempts to log on an account by explicitly specifying that account's credentials. This most commonly occurs in batch-type configurations such as scheduled tasks, or when using the RUNAS command.
Security	Audit Success	12544	2015-04-22 20:24:45	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: LTRANPHD$ Account Domain: WORKGROUP Logon ID: 0x3e7 Logon Type: 2 Impersonation Level: %%1833 New Logon: Security ID: S-1-5-21-1888849264-3803429180-4108621888-1001 Account Name: Liem Account Domain: LTRANPHD Logon ID: 0x1e385 Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x200 Process Name: C:\Windows\System32\winlogon.exe Network Information: Workstation Name: LTRANPHD Source Network Address: 127.0.0.1 Source Port: 0 Detailed Authentication Information: Logon Process: User32 Authentication Package: Negotiate Transited Services: - Package Name (NTLM only): - Key Length: 0 This event is generated when a logon session is created. It is generated on the computer that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service such as the Server service, or a local process such as Winlogon.exe or Services.exe. The logon type field indicates the kind of logon that occurred. The most common types are 2 (interactive) and 3 (network). The New Logon fields indicate the account for whom the new logon was created, i.e. the account that was logged on. The network fields indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impersonation level field indicates the extent to which a process in the logon session can impersonate. The authentication information fields provide detailed information about this specific logon request. - Logon GUID is a unique identifier that can be used to correlate this event with a KDC event. - Transited services indicate which intermediate services have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indicates the length of the generated session key. This will be 0 if no session key was requested.
Security	Audit Success	12544	2015-04-22 20:24:45	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: LTRANPHD$ Account Domain: WORKGROUP Logon ID: 0x3e7 Logon Type: 2 Impersonation Level: %%1833 New Logon: Security ID: S-1-5-21-1888849264-3803429180-4108621888-1001 Account Name: Liem Account Domain: LTRANPHD Logon ID: 0x1e3e2 Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x200 Process Name: C:\Windows\System32\winlogon.exe Network Information: Workstation Name: LTRANPHD Source Network Address: 127.0.0.1 Source Port: 0 Detailed Authentication Information: Logon Process: User32 Authentication Package: Negotiate Transited Services: - Package Name (NTLM only): - Key Length: 0 This event is generated when a logon session is created. It is generated on the computer that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service such as the Server service, or a local process such as Winlogon.exe or Services.exe. The logon type field indicates the kind of logon that occurred. The most common types are 2 (interactive) and 3 (network). The New Logon fields indicate the account for whom the new logon was created, i.e. the account that was logged on. The network fields indicate where a remote logon request originated. Workstation name is

					not always available and may be left blank in some cases. The impersonation level field indicates the extent to which a process in the logon session can impersonate. The authentication information fields provide detailed information about this specific logon request. - Logon GUID is a unique identifier that can be used to correlate this event with a KDC event. - Transited services indicate which intermediate services have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indicates the length of the generated session key. This will be 0 if no session key was requested.
Security	Audit Success	12544	2015-04-22 20:24:45	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: LTRANPHD$ Account Domain: WORKGROUP Logon ID: 0x3e7 Logon Type: 5 Impersonation Level: %%1833 New Logon: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Logon ID: 0x3e7 Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x228 Process Name: C:\Windows\System32\services.exe Network Information: Workstation Name: Source Network Address: - Source Port: - Detailed Authentication Information: Logon Process: Advapi Authentication Package: Negotiate Transited Services: - Package Name (NTLM only): - Key Length: 0 This event is generated when a logon session is created. It is generated on the computer that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service such as the Server service, or a local process such as Winlogon.exe or Services.exe. The logon type field indicates the kind of logon that occurred. The most common types are 2 (interactive) and 3 (network). The New Logon fields indicate the account for whom the new logon was created, i.e. the account that was logged on. The network fields indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impersonation level field indicates the extent to which a process in the logon session can impersonate. The authentication information fields provide detailed information about this specific logon request. - Logon GUID is a unique identifier that can be used to correlate this event with a KDC event. - Transited services indicate which intermediate services have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indicates the length of the generated session key. This will be 0 if no session key was requested.
Security	Audit Success	12548	2015-04-22 20:24:45	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-21-1888849264-3803429180-4108621888-1001 Account Name: Liem Account Domain: LTRANPHD Logon ID: 0x1e385 Privileges: SeSecurityPrivilege SeTakeOwnershipPrivilege SeLoadDriverPrivilege SeBackupPrivilege SeRestorePrivilege SeDebugPrivilege SeSystemEnvironmentPrivilege SeImpersonatePrivilege
Security	Audit Success	12548	2015-04-22 20:24:45	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Logon ID: 0x3e7 Privileges: SeAssignPrimaryTokenPrivilege SeTcbPrivilege SeSecurityPrivilege SeTakeOwnershipPrivilege SeLoadDriverPrivilege SeBackupPrivilege SeRestorePrivilege SeDebugPrivilege SeAuditPrivilege SeSystemEnvironmentPrivilege SeImpersonatePrivilege
Security	Audit Success	13824	2015-04-22 20:24:48	Microsoft-Windows-Security-Auditing	4797: An attempt was made to query the existence of a blank password for an account. Subject: Security ID: S-1-5-21-1888849264-3803429180-4108621888-1001 Account Name: Liem Account Domain: LTRANPHD Logon ID: 0x1e3e2 Additional Information: Caller Workstation: LTRANPHD Target Account Name: Administrator Target Account Domain: LTRANPHD
Security	Audit Success	13824	2015-04-22 20:24:48	Microsoft-Windows-Security-Auditing	4797: An attempt was made to query the existence of a blank password for an account. Subject: Security ID: S-1-5-21-1888849264-3803429180-4108621888-1001 Account Name: Liem Account Domain: LTRANPHD Logon ID: 0x1e3e2 Additional Information: Caller Workstation: LTRANPHD Target Account Name: Guest Target Account Domain: LTRANPHD
Security	Audit Success	13824	2015-04-22 20:24:48	Microsoft-Windows-Security-Auditing	4797: An attempt was made to query the existence of a blank password for an account. Subject: Security ID: S-1-5-21-1888849264-3803429180-4108621888-1001 Account Name: Liem Account Domain: LTRANPHD Logon ID: 0x1e3e2 Additional Information: Caller Workstation: LTRANPHD Target Account Name: Administrator Target Account Domain: LTRANPHD
Security	Audit Success	13824	2015-04-22 20:24:48	Microsoft-Windows-Security-Auditing	4797: An attempt was made to query the existence of a blank password for an account. Subject: Security ID: S-1-5-21-1888849264-3803429180-4108621888-1001 Account Name: Liem Account Domain: LTRANPHD Logon ID: 0x1e3e2 Additional Information: Caller Workstation: LTRANPHD Target Account Name: Guest Target Account Domain: LTRANPHD
Security	Audit Success	13824	2015-04-22 20:24:48	Microsoft-Windows-Security-Auditing	4797: An attempt was made to query the existence of a blank password for an account. Subject: Security ID: S-1-5-19 Account Name: LOCAL SERVICE Account Domain: NT AUTHORITY Logon ID: 0x3e5 Additional Information: Caller Workstation: LTRANPHD Target Account Name: Administrator Target Account Domain: LTRANPHD
Security	Audit Success	13824	2015-04-22 20:24:48	Microsoft-Windows-Security-Auditing	4797: An attempt was made to query the existence of a blank password for an account. Subject: Security ID: S-1-5-19 Account Name: LOCAL SERVICE Account Domain: NT AUTHORITY Logon ID: 0x3e5 Additional Information: Caller Workstation: LTRANPHD Target Account Name: Administrator Target Account Domain: LTRANPHD
Security	Audit Success	13824	2015-04-22 20:24:48	Microsoft-Windows-Security-Auditing	4797: An attempt was made to query the existence of a blank password for an account. Subject: Security ID: S-1-5-19 Account Name: LOCAL SERVICE Account Domain: NT AUTHORITY Logon ID: 0x3e5 Additional Information: Caller Workstation: LTRANPHD Target Account Name: Guest Target Account Domain: LTRANPHD
Security	Audit Success	13824	2015-04-22 20:24:48	Microsoft-Windows-Security-Auditing	4797: An attempt was made to query the existence of a blank password for an account. Subject: Security ID: S-1-5-19 Account Name: LOCAL SERVICE Account Domain: NT AUTHORITY Logon ID: 0x3e5 Additional Information: Caller Workstation: LTRANPHD Target Account Name: Guest Target Account Domain: LTRANPHD
Security	Audit	13824	2015-04-22	Microsoft-Windows-Security-	4797: An attempt was made to query the existence of a blank password for an account. Subject: Security ID: S-1-5-19 Account Name: LOCAL SERVICE Account Domain: NT AUTHORITY Logon ID: 0x3e5 Additional

	Success		20:24:48	Auditing	Information: Caller Workstation: LTRANPHD Target Account Name: Liem Target Account Domain: LTRANPHD
Security	Audit Success	13824	2015-04-22 20:24:48	Microsoft-Windows-Security-Auditing	4797: An attempt was made to query the existence of a blank password for an account. Subject: Security ID: S-1-5-19 Account Name: LOCAL SERVICE Account Domain: NT AUTHORITY Logon ID: 0x3e5 Additional Information: Caller Workstation: LTRANPHD Target Account Name: Liem Target Account Domain: LTRANPHD
Security	Audit Success	13824	2015-04-22 20:24:48	Microsoft-Windows-Security-Auditing	4797: An attempt was made to query the existence of a blank password for an account. Subject: Security ID: S-1-5-19 Account Name: LOCAL SERVICE Account Domain: NT AUTHORITY Logon ID: 0x3e5 Additional Information: Caller Workstation: LTRANPHD Target Account Name: Liem Target Account Domain: LTRANPHD
Security	Audit Success	13824	2015-04-22 20:24:48	Microsoft-Windows-Security-Auditing	4797: An attempt was made to query the existence of a blank password for an account. Subject: Security ID: S-1-5-19 Account Name: LOCAL SERVICE Account Domain: NT AUTHORITY Logon ID: 0x3e5 Additional Information: Caller Workstation: LTRANPHD Target Account Name: Liem Target Account Domain: LTRANPHD
Security	Audit Success	12288	2015-04-22 20:56:12	Microsoft-Windows-Security-Auditing	4608: Windows is starting up. This event is logged when LSASS.EXE starts and the auditing subsystem is initialized.
Security	Audit Success	12544	2015-04-22 20:56:12	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-0-0 Account Name: - Account Domain: - Logon ID: 0x0 Logon Type: 0 Impersonation Level: - New Logon: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Logon ID: 0x3e7 Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x4 Process Name: Network Information: Workstation Name: - Source Network Address: - Source Port: - Detailed Authentication Information: Logon Process: - Authentication Package: - Transited Services: - Package Name (NTLM only): - Key Length: 0 This event is generated when a logon session is created. It is generated on the computer that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service such as the Server service, or a local process such as Winlogon.exe or Services.exe. The logon type field indicates the kind of logon that occurred. The most common types are 2 (interactive) and 3 (network). The New Logon fields indicate the account for whom the new logon was created, i.e. the account that was logged on. The network fields indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impersonation level field indicates the extent to which a process in the logon session can impersonate. The authentication information fields provide detailed information about this specific logon request. - Logon GUID is a unique identifier that can be used to correlate this event with a KDC event. - Transited services indicate which intermediate services have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indicates the length of the generated session key. This will be 0 if no session key was requested.
Security	Audit Success	13568	2015-04-22 20:56:12	Microsoft-Windows-Security-Auditing	4902: The Per-user audit policy table was created. Number of Elements: 0 Policy ID: 0x7f6c
Security	Audit Success	12544	2015-04-22 20:56:13	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: LTRANPHD$ Account Domain: WORKGROUP Logon ID: 0x3e7 Logon Type: 5 Impersonation Level: %%1833 New Logon: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Logon ID: 0x3e7 Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x228 Process Name: C:\Windows\System32\services.exe Network Information: Workstation Name: Source Network Address: - Source Port: - Detailed Authentication Information: Logon Process: Advapi Authentication Package: Negotiate Transited Services: - Package Name (NTLM only): - Key Length: 0 This event is generated when a logon session is created. It is generated on the computer that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service such as the Server service, or a local process such as Winlogon.exe or Services.exe. The logon type field indicates the kind of logon that occurred. The most common types are 2 (interactive) and 3 (network). The New Logon fields indicate the account for whom the new logon was created, i.e. the account that was logged on. The network fields indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impersonation level field indicates the extent to which a process in the logon session can impersonate. The authentication information fields provide detailed information about this specific logon request. - Logon GUID is a unique identifier that can be used to correlate this event with a KDC event. - Transited services indicate which intermediate services have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indicates the length of the generated session key. This will be 0 if no session key was requested.
Security	Audit Success	12544	2015-04-22 20:56:13	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: LTRANPHD$ Account Domain: WORKGROUP Logon ID: 0x3e7 Logon Type: 5 Impersonation Level: %%1833 New Logon: Security ID: S-1-5-20 Account Name: NETWORK SERVICE Account Domain: NT AUTHORITY Logon ID: 0x3e4 Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x228 Process Name: C:\Windows\System32\services.exe Network Information: Workstation Name: Source Network Address: - Source Port: - Detailed Authentication Information: Logon Process: Advapi Authentication Package: Negotiate Transited Services: - Package Name (NTLM only): - Key Length: 0 This event is generated when a logon session is created. It is generated on the computer that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service such as the Server service, or a local process such as Winlogon.exe or Services.exe. The logon type field indicates the kind of logon that occurred. The most common types are 2 (interactive) and 3 (network). The New Logon fields indicate the account for whom the new logon was created, i.e. the account that was logged on. The network fields indicate where a

					remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impersonation level field indicates the extent to which a process in the logon session can impersonate. The authentication information fields provide detailed information about this specific logon request. - Logon GUID is a unique identifier that can be used to correlate this event with a KDC event. - Transited services indicate which intermediate services have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indicates the length of the generated session key. This will be 0 if no session key was requested.
Security	Audit Success	12544	2015-04-22 20:56:13	Microsoft-Windows-Security-Auditing	4648: A logon was attempted using explicit credentials. Subject: Security ID: S-1-5-18 Account Name: LTRANPHD$ Account Domain: WORKGROUP Logon ID: 0x3e7 Logon GUID: {00000000-0000-0000-0000-000000000000} Account Whose Credentials Were Used: Account Name: DWM-1 Account Domain: Window Manager Logon GUID: {00000000-0000-0000-0000-000000000000} Target Server: Target Server Name: localhost Additional Information: localhost Process Information: Process ID: 0x200 Process Name: C:\Windows\System32\winlogon.exe Network Information: Network Address: - Port: - This event is generated when a process attempts to log on an account by explicitly specifying that account's credentials. This most commonly occurs in batch-type configurations such as scheduled tasks, or when using the RUNAS command.
Security	Audit Success	12544	2015-04-22 20:56:13	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: LTRANPHD$ Account Domain: WORKGROUP Logon ID: 0x3e7 Logon Type: 2 Impersonation Level: %%1833 New Logon: Security ID: S-1-5-90-1 Account Name: DWM-1 Account Domain: Window Manager Logon ID: 0xe461 Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x200 Process Name: C:\Windows\System32\winlogon.exe Network Information: Workstation Name: Source Network Address: - Source Port: - Detailed Authentication Information: Logon Process: Advapi Authentication Package: Negotiate Transited Services: - Package Name (NTLM only): - Key Length: 0 This event is generated when a logon session is created. It is generated on the computer that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service such as the Server service, or a local process such as Winlogon.exe or Services.exe. The logon type field indicates the kind of logon that occurred. The most common types are 2 (interactive) and 3 (network). The New Logon fields indicate the account for whom the new logon was created, i.e. the account that was logged on. The network fields indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impersonation level field indicates the extent to which a process in the logon session can impersonate. The authentication information fields provide detailed information about this specific logon request. - Logon GUID is a unique identifier that can be used to correlate this event with a KDC event. - Transited services indicate which intermediate services have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indicates the length of the generated session key. This will be 0 if no session key was requested.
Security	Audit Success	12544	2015-04-22 20:56:13	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: LTRANPHD$ Account Domain: WORKGROUP Logon ID: 0x3e7 Logon Type: 2 Impersonation Level: %%1833 New Logon: Security ID: S-1-5-90-1 Account Name: DWM-1 Account Domain: Window Manager Logon ID: 0xe48c Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x200 Process Name: C:\Windows\System32\winlogon.exe Network Information: Workstation Name: Source Network Address: - Source Port: - Detailed Authentication Information: Logon Process: Advapi Authentication Package: Negotiate Transited Services: - Package Name (NTLM only): - Key Length: 0 This event is generated when a logon session is created. It is generated on the computer that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service such as the Server service, or a local process such as Winlogon.exe or Services.exe. The logon type field indicates the kind of logon that occurred. The most common types are 2 (interactive) and 3 (network). The New Logon fields indicate the account for whom the new logon was created, i.e. the account that was logged on. The network fields indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impersonation level field indicates the extent to which a process in the logon session can impersonate. The authentication information fields provide detailed information about this specific logon request. - Logon GUID is a unique identifier that can be used to correlate this event with a KDC event. - Transited services indicate which intermediate services have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indicates the length of the generated session key. This will be 0 if no session key was requested.
Security	Audit Success	12544	2015-04-22 20:56:13	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: LTRANPHD$ Account Domain: WORKGROUP Logon ID: 0x3e7 Logon Type: 5 Impersonation Level: %%1833 New Logon: Security ID: S-1-5-19 Account Name: LOCAL SERVICE Account Domain: NT AUTHORITY Logon ID: 0x3e5 Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x228 Process Name: C:\Windows\System32\services.exe Network Information: Workstation Name: Source Network Address: - Source Port: - Detailed Authentication Information: Logon Process: Advapi Authentication Package: Negotiate Transited Services: - Package Name (NTLM only): - Key Length: 0 This event is generated when a logon session is created. It is generated on the computer that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service such as the Server service, or a local process such as Winlogon.exe or Services.exe. The logon type field indicates the kind of logon that occurred. The most common types are 2 (interactive) and 3 (network). The New Logon fields indicate the account for whom the new logon was created, i.e. the account that was logged on. The network fields indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impersonation level field indicates the extent to which a process in the logon session can

					impersonate. The authentication information fields provide detailed information about this specific logon request. - Logon GUID is a unique identifier that can be used to correlate this event with a KDC event. - Transited services indicate which intermediate services have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indicates the length of the generated session key. This will be 0 if no session key was requested.
Security	Audit Success	12548	2015-04-22 20:56:13	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Logon ID: 0x3e7 Privileges: SeAssignPrimaryTokenPrivilege SeTcbPrivilege SeSecurityPrivilege SeTakeOwnershipPrivilege SeLoadDriverPrivilege SeBackupPrivilege SeRestorePrivilege SeDebugPrivilege SeAuditPrivilege SeSystemEnvironmentPrivilege SeImpersonatePrivilege
Security	Audit Success	12548	2015-04-22 20:56:13	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-20 Account Name: NETWORK SERVICE Account Domain: NT AUTHORITY Logon ID: 0x3e4 Privileges: SeAssignPrimaryTokenPrivilege SeAuditPrivilege SeImpersonatePrivilege
Security	Audit Success	12548	2015-04-22 20:56:13	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-90-1 Account Name: DWM-1 Account Domain: Window Manager Logon ID: 0xe461 Privileges: SeAssignPrimaryTokenPrivilege SeAuditPrivilege SeImpersonatePrivilege
Security	Audit Success	12548	2015-04-22 20:56:13	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-90-1 Account Name: DWM-1 Account Domain: Window Manager Logon ID: 0xe48c Privileges: SeAssignPrimaryTokenPrivilege SeAuditPrivilege
Security	Audit Success	12548	2015-04-22 20:56:13	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-19 Account Name: LOCAL SERVICE Account Domain: NT AUTHORITY Logon ID: 0x3e5 Privileges: SeAssignPrimaryTokenPrivilege SeAuditPrivilege SeImpersonatePrivilege
Security	Audit Success	12544	2015-04-22 20:56:14	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: LTRANPHD$ Account Domain: WORKGROUP Logon ID: 0x3e7 Logon Type: 5 Impersonation Level: %%1833 New Logon: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Logon ID: 0x3e7 Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x228 Process Name: C:\Windows\System32\services.exe Network Information: Workstation Name: Source Network Address: - Source Port: - Detailed Authentication Information: Logon Process: Advapi Authentication Package: Negotiate Transited Services: - Package Name (NTLM only): - Key Length: 0 This event is generated when a logon session is created. It is generated on the computer that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service such as the Server service, or a local process such as Winlogon.exe or Services.exe. The logon type field indicates the kind of logon that occurred. The most common types are 2 (interactive) and 3 (network). The New Logon fields indicate the account for whom the new logon was created, i.e. the account that was logged on. The network fields indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impersonation level field indicates the extent to which a process in the logon session can impersonate. The authentication information fields provide detailed information about this specific logon request. - Logon GUID is a unique identifier that can be used to correlate this event with a KDC event. - Transited services indicate which intermediate services have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indicates the length of the generated session key. This will be 0 if no session key was requested.
Security	Audit Success	12544	2015-04-22 20:56:14	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: LTRANPHD$ Account Domain: WORKGROUP Logon ID: 0x3e7 Logon Type: 5 Impersonation Level: %%1833 New Logon: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Logon ID: 0x3e7 Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x228 Process Name: C:\Windows\System32\services.exe Network Information: Workstation Name: Source Network Address: - Source Port: - Detailed Authentication Information: Logon Process: Advapi Authentication Package: Negotiate Transited Services: - Package Name (NTLM only): - Key Length: 0 This event is generated when a logon session is created. It is generated on the computer that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service such as the Server service, or a local process such as Winlogon.exe or Services.exe. The logon type field indicates the kind of logon that occurred. The most common types are 2 (interactive) and 3 (network). The New Logon fields indicate the account for whom the new logon was created, i.e. the account that was logged on. The network fields indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impersonation level field indicates the extent to which a process in the logon session can impersonate. The authentication information fields provide detailed information about this specific logon request. - Logon GUID is a unique identifier that can be used to correlate this event with a KDC event. - Transited services indicate which intermediate services have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indicates the length of the generated session key. This will be 0 if no session key was requested.
Security	Audit Success	12548	2015-04-22 20:56:14	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Logon ID: 0x3e7 Privileges: SeAssignPrimaryTokenPrivilege SeTcbPrivilege SeSecurityPrivilege SeTakeOwnershipPrivilege SeLoadDriverPrivilege SeBackupPrivilege SeRestorePrivilege SeDebugPrivilege SeAuditPrivilege SeSystemEnvironmentPrivilege SeImpersonatePrivilege
Security	Audit	12548	2015-04-22	Microsoft-Windows-Security-	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Logon ID: 0x3e7 Privileges: SeAssignPrimaryTokenPrivilege SeTcbPrivilege

	Success		20:56:14	Auditing	SeSecurityPrivilege SeTakeOwnershipPrivilege SeLoadDriverPrivilege SeBackupPrivilege SeRestorePrivilege SeDebugPrivilege SeAuditPrivilege SeSystemEnvironmentPrivilege SeImpersonatePrivilege
Security	Audit Success	101	2015-04-22 20:56:15	Microsoft-Windows-Eventlog	1101: Audit events have been dropped by the transport. 0
Security	Audit Success	12292	2015-04-22 20:56:15	Microsoft-Windows-Security-Auditing	5033: The Windows Firewall Driver started successfully.
Security	Audit Success	12544	2015-04-22 20:56:15	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: LTRANPHD$ Account Domain: WORKGROUP Logon ID: 0x3e7 Logon Type: 5 Impersonation Level: %%1833 New Logon: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Logon ID: 0x3e7 Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x228 Process Name: C:\Windows\System32\services.exe Network Information: Workstation Name: Source Network Address: - Source Port: - Detailed Authentication Information: Logon Process: Advapi Authentication Package: Negotiate Transited Services: - Package Name (NTLM only): - Key Length: 0 This event is generated when a logon session is created. It is generated on the computer that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service such as the Server service, or a local process such as Winlogon.exe or Services.exe. The logon type field indicates the kind of logon that occurred. The most common types are 2 (interactive) and 3 (network). The New Logon fields indicate the account for whom the new logon was created, i.e. the account that was logged on. The network fields indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impersonation level field indicates the extent to which a process in the logon session can impersonate. The authentication information fields provide detailed information about this specific logon request. - Logon GUID is a unique identifier that can be used to correlate this event with a KDC event. - Transited services indicate which intermediate services have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indicates the length of the generated session key. This will be 0 if no session key was requested.
Security	Audit Success	12548	2015-04-22 20:56:15	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Logon ID: 0x3e7 Privileges: SeAssignPrimaryTokenPrivilege SeTcbPrivilege SeSecurityPrivilege SeTakeOwnershipPrivilege SeLoadDriverPrivilege SeBackupPrivilege SeRestorePrivilege SeDebugPrivilege SeAuditPrivilege SeSystemEnvironmentPrivilege SeImpersonatePrivilege
Security	Audit Success	12292	2015-04-22 20:56:16	Microsoft-Windows-Security-Auditing	5024: The Windows Firewall service started successfully.
Security	Audit Success	12544	2015-04-22 20:56:16	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: LTRANPHD$ Account Domain: WORKGROUP Logon ID: 0x3e7 Logon Type: 5 Impersonation Level: %%1833 New Logon: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Logon ID: 0x3e7 Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x228 Process Name: C:\Windows\System32\services.exe Network Information: Workstation Name: Source Network Address: - Source Port: - Detailed Authentication Information: Logon Process: Advapi Authentication Package: Negotiate Transited Services: - Package Name (NTLM only): - Key Length: 0 This event is generated when a logon session is created. It is generated on the computer that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service such as the Server service, or a local process such as Winlogon.exe or Services.exe. The logon type field indicates the kind of logon that occurred. The most common types are 2 (interactive) and 3 (network). The New Logon fields indicate the account for whom the new logon was created, i.e. the account that was logged on. The network fields indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impersonation level field indicates the extent to which a process in the logon session can impersonate. The authentication information fields provide detailed information about this specific logon request. - Logon GUID is a unique identifier that can be used to correlate this event with a KDC event. - Transited services indicate which intermediate services have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indicates the length of the generated session key. This will be 0 if no session key was requested.
Security	Audit Success	12548	2015-04-22 20:56:16	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Logon ID: 0x3e7 Privileges: SeAssignPrimaryTokenPrivilege SeTcbPrivilege SeSecurityPrivilege SeTakeOwnershipPrivilege SeLoadDriverPrivilege SeBackupPrivilege SeRestorePrivilege SeDebugPrivilege SeAuditPrivilege SeSystemEnvironmentPrivilege SeImpersonatePrivilege
			2015-04-		4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: LTRANPHD$ Account Domain: WORKGROUP Logon ID: 0x3e7 Logon Type: 5 Impersonation Level: %%1833 New Logon: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Logon ID: 0x3e7 Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x228 Process Name: C:\Windows\System32\services.exe Network Information: Workstation Name: Source Network Address: - Source Port: - Detailed Authentication Information: Logon Process: Advapi Authentication Package: Negotiate Transited Services: - Package Name (NTLM only): - Key Length: 0 This event is generated when a logon session is created. It is generated on the computer that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service such as the Server service, or a local

Security	Audit Success	12544	22 20:56:17	Microsoft-Windows-Security-Auditing	process such as Winlogon.exe or Services.exe. The logon type field indicates the kind of logon that occurred. The most common types are 2 (interactive) and 3 (network). The New Logon fields indicate the account for whom the new logon was created, i.e. the account that was logged on. The network fields indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impersonation level field indicates the extent to which a process in the logon session can impersonate. The authentication information fields provide detailed information about this specific logon request. - Logon GUID is a unique identifier that can be used to correlate this event with a KDC event. - Transited services indicate which intermediate services have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indicates the length of the generated session key. This will be 0 if no session key was requested.
Security	Audit Success	12544	2015-04-22 20:56:17	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-0-0 Account Name: - Account Domain: - Logon ID: 0x0 Logon Type: 3 Impersonation Level: %%1833 New Logon: Security ID: S-1-5-7 Account Name: ANONYMOUS LOGON Account Domain: NT AUTHORITY Logon ID: 0x19469 Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x0 Process Name: - Network Information: Workstation Name: Source Network Address: - Source Port: - Detailed Authentication Information: Logon Process: NtLmSsp Authentication Package: NTLM Transited Services: - Package Name (NTLM only): NTLM V1 Key Length: 0 This event is generated when a logon session is created. It is generated on the computer that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service such as the Server service, or a local process such as Winlogon.exe or Services.exe. The logon type field indicates the kind of logon that occurred. The most common types are 2 (interactive) and 3 (network). The New Logon fields indicate the account for whom the new logon was created, i.e. the account that was logged on. The network fields indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impersonation level field indicates the extent to which a process in the logon session can impersonate. The authentication information fields provide detailed information about this specific logon request. - Logon GUID is a unique identifier that can be used to correlate this event with a KDC event. - Transited services indicate which intermediate services have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indicates the length of the generated session key. This will be 0 if no session key was requested.
Security	Audit Success	12548	2015-04-22 20:56:17	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Logon ID: 0x3e7 Privileges: SeAssignPrimaryTokenPrivilege SeTcbPrivilege SeSecurityPrivilege SeTakeOwnershipPrivilege SeLoadDriverPrivilege SeBackupPrivilege SeRestorePrivilege SeDebugPrivilege SeAuditPrivilege SeSystemEnvironmentPrivilege SeImpersonatePrivilege
Security	Audit Success	12544	2015-04-22 20:56:23	Microsoft-Windows-Security-Auditing	4648: A logon was attempted using explicit credentials. Subject: Security ID: S-1-5-18 Account Name: LTRANPHD$ Account Domain: WORKGROUP Logon ID: 0x3e7 Logon GUID: {00000000-0000-0000-0000-000000000000} Account Whose Credentials Were Used: Account Name: Liem Account Domain: LTRANPHD Logon GUID: {00000000-0000-0000-0000-000000000000} Target Server: Target Server Name: localhost Additional Information: localhost Process Information: Process ID: 0x200 Process Name: C:\Windows\System32\winlogon.exe Network Information: Network Address: 127.0.0.1 Port: 0 This event is generated when a process attempts to log on an account by explicitly specifying that account's credentials. This most commonly occurs in batch-type configurations such as scheduled tasks, or when using the RUNAS command.
Security	Audit Success	12544	2015-04-22 20:56:23	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: LTRANPHD$ Account Domain: WORKGROUP Logon ID: 0x3e7 Logon Type: 2 Impersonation Level: %%1833 New Logon: Security ID: S-1-5-21-1888849264-3803429180-4108621888-1001 Account Name: Liem Account Domain: LTRANPHD Logon ID: 0x1e2a3 Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x200 Process Name: C:\Windows\System32\winlogon.exe Network Information: Workstation Name: LTRANPHD Source Network Address: 127.0.0.1 Source Port: 0 Detailed Authentication Information: Logon Process: User32 Authentication Package: Negotiate Transited Services: - Package Name (NTLM only): - Key Length: 0 This event is generated when a logon session is created. It is generated on the computer that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service such as the Server service, or a local process such as Winlogon.exe or Services.exe. The logon type field indicates the kind of logon that occurred. The most common types are 2 (interactive) and 3 (network). The New Logon fields indicate the account for whom the new logon was created, i.e. the account that was logged on. The network fields indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impersonation level field indicates the extent to which a process in the logon session can impersonate. The authentication information fields provide detailed information about this specific logon request. - Logon GUID is a unique identifier that can be used to correlate this event with a KDC event. - Transited services indicate which intermediate services have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indicates the length of the generated session key. This will be 0 if no session key was requested.
					4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: LTRANPHD$ Account Domain: WORKGROUP Logon ID: 0x3e7 Logon Type: 2 Impersonation Level: %%1833 New Logon: Security ID: S-1-5-21-1888849264-3803429180-4108621888-1001 Account Name: Liem Account Domain: LTRANPHD Logon ID: 0x1e2f7 Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x200 Process Name: C:\Windows\System32\winlogon.exe Network Information: Workstation Name: LTRANPHD Source Network Address: 127.0.0.1 Source Port: 0 Detailed Authentication Information:

Security	Audit Success	12544	2015-04-22 20:56:23	Microsoft-Windows-Security-Auditing	Logon Process: User32 Authentication Package: Negotiate Transited Services: - Package Name (NTLM only): - Key Length: 0 This event is generated when a logon session is created. It is generated on the computer that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service such as the Server service, or a local process such as Winlogon.exe or Services.exe. The logon type field indicates the kind of logon that occurred. The most common types are 2 (interactive) and 3 (network). The New Logon fields indicate the account for whom the new logon was created, i.e. the account that was logged on. The network fields indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impersonation level field indicates the extent to which a process in the logon session can impersonate. The authentication information fields provide detailed information about this specific logon request. - Logon GUID is a unique identifier that can be used to correlate this event with a KDC event. - Transited services indicate which intermediate services have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indicates the length of the generated session key. This will be 0 if no session key was requested.
Security	Audit Success	12548	2015-04-22 20:56:23	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-21-1888849264-3803429180-4108621888-1001 Account Name: Liem Account Domain: LTRANPHD Logon ID: 0x1e2a3 Privileges: SeSecurityPrivilege SeTakeOwnershipPrivilege SeLoadDriverPrivilege SeBackupPrivilege SeRestorePrivilege SeDebugPrivilege SeSystemEnvironmentPrivilege SeImpersonatePrivilege
Security	Audit Success	12544	2015-04-22 20:56:24	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: LTRANPHD$ Account Domain: WORKGROUP Logon ID: 0x3e7 Logon Type: 5 Impersonation Level: %%1833 New Logon: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Logon ID: 0x3e7 Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x228 Process Name: C:\Windows\System32\services.exe Network Information: Workstation Name: Source Network Address: - Source Port: - Detailed Authentication Information: Logon Process: Advapi Authentication Package: Negotiate Transited Services: - Package Name (NTLM only): - Key Length: 0 This event is generated when a logon session is created. It is generated on the computer that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service such as the Server service, or a local process such as Winlogon.exe or Services.exe. The logon type field indicates the kind of logon that occurred. The most common types are 2 (interactive) and 3 (network). The New Logon fields indicate the account for whom the new logon was created, i.e. the account that was logged on. The network fields indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impersonation level field indicates the extent to which a process in the logon session can impersonate. The authentication information fields provide detailed information about this specific logon request. - Logon GUID is a unique identifier that can be used to correlate this event with a KDC event. - Transited services indicate which intermediate services have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indicates the length of the generated session key. This will be 0 if no session key was requested.
Security	Audit Success	12548	2015-04-22 20:56:24	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Logon ID: 0x3e7 Privileges: SeAssignPrimaryTokenPrivilege SeTcbPrivilege SeSecurityPrivilege SeTakeOwnershipPrivilege SeLoadDriverPrivilege SeBackupPrivilege SeRestorePrivilege SeDebugPrivilege SeAuditPrivilege SeSystemEnvironmentPrivilege SeImpersonatePrivilege
Security	Audit Success	13824	2015-04-22 20:56:26	Microsoft-Windows-Security-Auditing	4797: An attempt was made to query the existence of a blank password for an account. Subject: Security ID: S-1-5-21-1888849264-3803429180-4108621888-1001 Account Name: Liem Account Domain: LTRANPHD Logon ID: 0x1e2f7 Additional Information: Caller Workstation: LTRANPHD Target Account Name: Administrator Target Account Domain: LTRANPHD
Security	Audit Success	13824	2015-04-22 20:56:26	Microsoft-Windows-Security-Auditing	4797: An attempt was made to query the existence of a blank password for an account. Subject: Security ID: S-1-5-21-1888849264-3803429180-4108621888-1001 Account Name: Liem Account Domain: LTRANPHD Logon ID: 0x1e2f7 Additional Information: Caller Workstation: LTRANPHD Target Account Name: Guest Target Account Domain: LTRANPHD
Security	Audit Success	13824	2015-04-22 20:56:26	Microsoft-Windows-Security-Auditing	4797: An attempt was made to query the existence of a blank password for an account. Subject: Security ID: S-1-5-21-1888849264-3803429180-4108621888-1001 Account Name: Liem Account Domain: LTRANPHD Logon ID: 0x1e2f7 Additional Information: Caller Workstation: LTRANPHD Target Account Name: Administrator Target Account Domain: LTRANPHD
Security	Audit Success	13824	2015-04-22 20:56:26	Microsoft-Windows-Security-Auditing	4797: An attempt was made to query the existence of a blank password for an account. Subject: Security ID: S-1-5-21-1888849264-3803429180-4108621888-1001 Account Name: Liem Account Domain: LTRANPHD Logon ID: 0x1e2f7 Additional Information: Caller Workstation: LTRANPHD Target Account Name: Guest Target Account Domain: LTRANPHD
Security	Audit Success	13824	2015-04-22 20:56:44	Microsoft-Windows-Security-Auditing	4797: An attempt was made to query the existence of a blank password for an account. Subject: Security ID: S-1-5-19 Account Name: LOCAL SERVICE Account Domain: NT AUTHORITY Logon ID: 0x3e5 Additional Information: Caller Workstation: LTRANPHD Target Account Name: Administrator Target Account Domain: LTRANPHD
Security	Audit Success	13824	2015-04-22 20:56:44	Microsoft-Windows-Security-Auditing	4797: An attempt was made to query the existence of a blank password for an account. Subject: Security ID: S-1-5-19 Account Name: LOCAL SERVICE Account Domain: NT AUTHORITY Logon ID: 0x3e5 Additional Information: Caller Workstation: LTRANPHD Target Account Name: Administrator Target Account Domain: LTRANPHD
	Audit		2015-04-	Microsoft-Windows-Security-	4797: An attempt was made to query the existence of a blank password for an account. Subject: Security ID:

Security	Success	13824	22 20:56:44	Auditing	S-1-5-19 Account Name: LOCAL SERVICE Account Domain: NT AUTHORITY Logon ID: 0x3e5 Additional Information: Caller Workstation: LTRANPHD Target Account Name: Guest Target Account Domain: LTRANPHD
Security	Audit Success	13824	2015-04-22 20:56:44	Microsoft-Windows-Security-Auditing	4797: An attempt was made to query the existence of a blank password for an account. Subject: Security ID: S-1-5-19 Account Name: LOCAL SERVICE Account Domain: NT AUTHORITY Logon ID: 0x3e5 Additional Information: Caller Workstation: LTRANPHD Target Account Name: Guest Target Account Domain: LTRANPHD
Security	Audit Success	13824	2015-04-22 20:56:44	Microsoft-Windows-Security-Auditing	4797: An attempt was made to query the existence of a blank password for an account. Subject: Security ID: S-1-5-19 Account Name: LOCAL SERVICE Account Domain: NT AUTHORITY Logon ID: 0x3e5 Additional Information: Caller Workstation: LTRANPHD Target Account Name: Liem Target Account Domain: LTRANPHD
Security	Audit Success	13824	2015-04-22 20:56:44	Microsoft-Windows-Security-Auditing	4797: An attempt was made to query the existence of a blank password for an account. Subject: Security ID: S-1-5-19 Account Name: LOCAL SERVICE Account Domain: NT AUTHORITY Logon ID: 0x3e5 Additional Information: Caller Workstation: LTRANPHD Target Account Name: Liem Target Account Domain: LTRANPHD
Security	Audit Success	13824	2015-04-22 20:56:44	Microsoft-Windows-Security-Auditing	4797: An attempt was made to query the existence of a blank password for an account. Subject: Security ID: S-1-5-19 Account Name: LOCAL SERVICE Account Domain: NT AUTHORITY Logon ID: 0x3e5 Additional Information: Caller Workstation: LTRANPHD Target Account Name: Liem Target Account Domain: LTRANPHD
Security	Audit Success	13824	2015-04-22 20:56:44	Microsoft-Windows-Security-Auditing	4797: An attempt was made to query the existence of a blank password for an account. Subject: Security ID: S-1-5-19 Account Name: LOCAL SERVICE Account Domain: NT AUTHORITY Logon ID: 0x3e5 Additional Information: Caller Workstation: LTRANPHD Target Account Name: Liem Target Account Domain: LTRANPHD
Security	Audit Success	12544	2015-04-22 21:01:26	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: LTRANPHD$ Account Domain: WORKGROUP Logon ID: 0x3e7 Logon Type: 5 Impersonation Level: %%1833 New Logon: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Logon ID: 0x3e7 Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x228 Process Name: C:\Windows\System32\services.exe Network Information: Workstation Name: Source Network Address: - Source Port: - Detailed Authentication Information: Logon Process: Advapi Authentication Package: Negotiate Transited Services: - Package Name (NTLM only): - Key Length: 0 This event is generated when a logon session is created. It is generated on the computer that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service such as the Server service, or a local process such as Winlogon.exe or Services.exe. The logon type field indicates the kind of logon that occurred. The most common types are 2 (interactive) and 3 (network). The New Logon fields indicate the account for whom the new logon was created, i.e. the account that was logged on. The network fields indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impersonation level field indicates the extent to which a process in the logon session can impersonate. The authentication information fields provide detailed information about this specific logon request. - Logon GUID is a unique identifier that can be used to correlate this event with a KDC event. - Transited services indicate which intermediate services have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indicates the length of the generated session key. This will be 0 if no session key was requested.
Security	Audit Success	12548	2015-04-22 21:01:26	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Logon ID: 0x3e7 Privileges: SeAssignPrimaryTokenPrivilege SeTcbPrivilege SeSecurityPrivilege SeTakeOwnershipPrivilege SeLoadDriverPrivilege SeBackupPrivilege SeRestorePrivilege SeDebugPrivilege SeAuditPrivilege SeSystemEnvironmentPrivilege SeImpersonatePrivilege
Security	Audit Success	12544	2015-04-22 21:01:27	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: LTRANPHD$ Account Domain: WORKGROUP Logon ID: 0x3e7 Logon Type: 5 Impersonation Level: %%1833 New Logon: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Logon ID: 0x3e7 Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x228 Process Name: C:\Windows\System32\services.exe Network Information: Workstation Name: Source Network Address: - Source Port: - Detailed Authentication Information: Logon Process: Advapi Authentication Package: Negotiate Transited Services: - Package Name (NTLM only): - Key Length: 0 This event is generated when a logon session is created. It is generated on the computer that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service such as the Server service, or a local process such as Winlogon.exe or Services.exe. The logon type field indicates the kind of logon that occurred. The most common types are 2 (interactive) and 3 (network). The New Logon fields indicate the account for whom the new logon was created, i.e. the account that was logged on. The network fields indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impersonation level field indicates the extent to which a process in the logon session can impersonate. The authentication information fields provide detailed information about this specific logon request. - Logon GUID is a unique identifier that can be used to correlate this event with a KDC event. - Transited services indicate which intermediate services have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indicates the length of the generated session key. This will be 0 if no session key was requested.
Security	Audit Success	12548	2015-04-22 21:01:27	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Logon ID: 0x3e7 Privileges: SeAssignPrimaryTokenPrivilege SeTcbPrivilege SeSecurityPrivilege SeTakeOwnershipPrivilege SeLoadDriverPrivilege SeBackupPrivilege SeRestorePrivilege SeDebugPrivilege SeAuditPrivilege SeSystemEnvironmentPrivilege SeImpersonatePrivilege
Security	Audit Success	103	2015-04-22	Microsoft-Windows-Eventlog	1100: The event logging service has shut down.

			21:17:09		
Security	Audit Success	12545	2015-04-22 21:17:09	Microsoft-Windows-Security-Auditing	4647: User initiated logoff: Subject: Security ID: S-1-5-21-1888849264-3803429180-4108621888-1001 Account Name: Liem Account Domain: LTRANPHD Logon ID: 0x1e2f7 This event is generated when a logoff is initiated. No further user-initiated activity can occur. This event can be interpreted as a logoff event.
Security	Audit Success	12288	2015-04-22 21:18:08	Microsoft-Windows-Security-Auditing	4608: Windows is starting up. This event is logged when LSASS.EXE starts and the auditing subsystem is initialized.
Security	Audit Success	12544	2015-04-22 21:18:08	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-0-0 Account Name: - Account Domain: - Logon ID: 0x0 Logon Type: 0 Impersonation Level: - New Logon: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Logon ID: 0x3e7 Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x4 Process Name: Network Information: Workstation Name: - Source Network Address: - Source Port: - Detailed Authentication Information: Logon Process: - Authentication Package: - Transited Services: - Package Name (NTLM only): - Key Length: 0 This event is generated when a logon session is created. It is generated on the computer that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service such as the Server service, or a local process such as Winlogon.exe or Services.exe. The logon type field indicates the kind of logon that occurred. The most common types are 2 (interactive) and 3 (network). The New Logon fields indicate the account for whom the new logon was created, i.e. the account that was logged on. The network fields indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impersonation level field indicates the extent to which a process in the logon session can impersonate. The authentication information fields provide detailed information about this specific logon request. - Logon GUID is a unique identifier that can be used to correlate this event with a KDC event. - Transited services indicate which intermediate services have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indicates the length of the generated session key. This will be 0 if no session key was requested.
Security	Audit Success	12544	2015-04-22 21:18:08	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: LTRANPHD$ Account Domain: WORKGROUP Logon ID: 0x3e7 Logon Type: 5 Impersonation Level: %%1833 New Logon: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Logon ID: 0x3e7 Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x230 Process Name: C:\Windows\System32\services.exe Network Information: Workstation Name: Source Network Address: - Source Port: - Detailed Authentication Information: Logon Process: Advapi Authentication Package: Negotiate Transited Services: - Package Name (NTLM only): - Key Length: 0 This event is generated when a logon session is created. It is generated on the computer that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service such as the Server service, or a local process such as Winlogon.exe or Services.exe. The logon type field indicates the kind of logon that occurred. The most common types are 2 (interactive) and 3 (network). The New Logon fields indicate the account for whom the new logon was created, i.e. the account that was logged on. The network fields indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impersonation level field indicates the extent to which a process in the logon session can impersonate. The authentication information fields provide detailed information about this specific logon request. - Logon GUID is a unique identifier that can be used to correlate this event with a KDC event. - Transited services indicate which intermediate services have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indicates the length of the generated session key. This will be 0 if no session key was requested.
Security	Audit Success	12544	2015-04-22 21:18:08	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: LTRANPHD$ Account Domain: WORKGROUP Logon ID: 0x3e7 Logon Type: 5 Impersonation Level: %%1833 New Logon: Security ID: S-1-5-20 Account Name: NETWORK SERVICE Account Domain: NT AUTHORITY Logon ID: 0x3e4 Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x230 Process Name: C:\Windows\System32\services.exe Network Information: Workstation Name: Source Network Address: - Source Port: - Detailed Authentication Information: Logon Process: Advapi Authentication Package: Negotiate Transited Services: - Package Name (NTLM only): - Key Length: 0 This event is generated when a logon session is created. It is generated on the computer that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service such as the Server service, or a local process such as Winlogon.exe or Services.exe. The logon type field indicates the kind of logon that occurred. The most common types are 2 (interactive) and 3 (network). The New Logon fields indicate the account for whom the new logon was created, i.e. the account that was logged on. The network fields indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impersonation level field indicates the extent to which a process in the logon session can impersonate. The authentication information fields provide detailed information about this specific logon request. - Logon GUID is a unique identifier that can be used to correlate this event with a KDC event. - Transited services indicate which intermediate services have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indicates the length of the generated session key. This will be 0 if no session key was requested.
			2015-04-		4648: A logon was attempted using explicit credentials. Subject: Security ID: S-1-5-18 Account Name: LTRANPHD$ Account Domain: WORKGROUP Logon ID: 0x3e7 Logon GUID: {00000000-0000-0000-0000-000000000000} Account Whose Credentials Were Used: Account Name: DWM-1 Account Domain: Window

Security	Audit Success	12544	22 21:18:08	Microsoft-Windows-Security-Auditing	Manager Logon GUID: {00000000-0000-0000-0000-000000000000} Target Server: Target Server Name: localhost Additional Information: localhost Process Information: Process ID: 0x200 Process Name: C:\Windows\System32\winlogon.exe Network Information: Network Address: - Port: - This event is generated when a process attempts to log on an account by explicitly specifying that account's credentials. This most commonly occurs in batch-type configurations such as scheduled tasks, or when using the RUNAS command.
Security	Audit Success	12544	2015-04-22 21:18:08	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: LTRANPHD$ Account Domain: WORKGROUP Logon ID: 0x3e7 Logon Type: 2 Impersonation Level: %%1833 New Logon: Security ID: S-1-5-90-1 Account Name: DWM-1 Account Domain: Window Manager Logon ID: 0xc374 Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x200 Process Name: C:\Windows\System32\winlogon.exe Network Information: Workstation Name: Source Network Address: - Source Port: - Detailed Authentication Information: Logon Process: Advapi Authentication Package: Negotiate Transited Services: - Package Name (NTLM only): - Key Length: 0 This event is generated when a logon session is created. It is generated on the computer that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service such as the Server service, or a local process such as Winlogon.exe or Services.exe. The logon type field indicates the kind of logon that occurred. The most common types are 2 (interactive) and 3 (network). The New Logon fields indicate the account for whom the new logon was created, i.e. the account that was logged on. The network fields indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impersonation level field indicates the extent to which a process in the logon session can impersonate. The authentication information fields provide detailed information about this specific logon request. - Logon GUID is a unique identifier that can be used to correlate this event with a KDC event. - Transited services indicate which intermediate services have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indicates the length of the generated session key. This will be 0 if no session key was requested.
Security	Audit Success	12544	2015-04-22 21:18:08	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: LTRANPHD$ Account Domain: WORKGROUP Logon ID: 0x3e7 Logon Type: 2 Impersonation Level: %%1833 New Logon: Security ID: S-1-5-90-1 Account Name: DWM-1 Account Domain: Window Manager Logon ID: 0xc386 Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x200 Process Name: C:\Windows\System32\winlogon.exe Network Information: Workstation Name: Source Network Address: - Source Port: - Detailed Authentication Information: Logon Process: Advapi Authentication Package: Negotiate Transited Services: - Package Name (NTLM only): - Key Length: 0 This event is generated when a logon session is created. It is generated on the computer that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service such as the Server service, or a local process such as Winlogon.exe or Services.exe. The logon type field indicates the kind of logon that occurred. The most common types are 2 (interactive) and 3 (network). The New Logon fields indicate the account for whom the new logon was created, i.e. the account that was logged on. The network fields indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impersonation level field indicates the extent to which a process in the logon session can impersonate. The authentication information fields provide detailed information about this specific logon request. - Logon GUID is a unique identifier that can be used to correlate this event with a KDC event. - Transited services indicate which intermediate services have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indicates the length of the generated session key. This will be 0 if no session key was requested.
Security	Audit Success	12548	2015-04-22 21:18:08	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Logon ID: 0x3e7 Privileges: SeAssignPrimaryTokenPrivilege SeTcbPrivilege SeSecurityPrivilege SeTakeOwnershipPrivilege SeLoadDriverPrivilege SeBackupPrivilege SeRestorePrivilege SeDebugPrivilege SeAuditPrivilege SeSystemEnvironmentPrivilege SeImpersonatePrivilege
Security	Audit Success	12548	2015-04-22 21:18:08	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-20 Account Name: NETWORK SERVICE Account Domain: NT AUTHORITY Logon ID: 0x3e4 Privileges: SeAssignPrimaryTokenPrivilege SeAuditPrivilege SeImpersonatePrivilege
Security	Audit Success	12548	2015-04-22 21:18:08	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-90-1 Account Name: DWM-1 Account Domain: Window Manager Logon ID: 0xc374 Privileges: SeAssignPrimaryTokenPrivilege SeAuditPrivilege SeImpersonatePrivilege
Security	Audit Success	12548	2015-04-22 21:18:08	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-90-1 Account Name: DWM-1 Account Domain: Window Manager Logon ID: 0xc386 Privileges: SeAssignPrimaryTokenPrivilege SeAuditPrivilege
Security	Audit Success	13568	2015-04-22 21:18:08	Microsoft-Windows-Security-Auditing	4902: The Per-user audit policy table was created. Number of Elements: 0 Policy ID: 0x745b
					4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: LTRANPHD$ Account Domain: WORKGROUP Logon ID: 0x3e7 Logon Type: 5 Impersonation Level: %%1833 New Logon: Security ID: S-1-5-19 Account Name: LOCAL SERVICE Account Domain: NT AUTHORITY Logon ID: 0x3e5 Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x230 Process Name: C:\Windows\System32\services.exe Network Information: Workstation Name: Source Network Address: - Source Port: - Detailed Authentication Information: Logon Process: Advapi Authentication Package: Negotiate Transited Services: - Package Name (NTLM only): - Key Length: 0 This event is generated when a logon session is

Security	Audit Success	12544	2015-04-22 21:18:09	Microsoft-Windows-Security-Auditing	created. It is generated on the computer that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service such as the Server service, or a local process such as Winlogon.exe or Services.exe. The logon type field indicates the kind of logon that occurred. The most common types are 2 (interactive) and 3 (network). The New Logon fields indicate the account for whom the new logon was created, i.e. the account that was logged on. The network fields indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impersonation level field indicates the extent to which a process in the logon session can impersonate. The authentication information fields provide detailed information about this specific logon request. - Logon GUID is a unique identifier that can be used to correlate this event with a KDC event. - Transited services indicate which intermediate services have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indicates the length of the generated session key. This will be 0 if no session key was requested.
Security	Audit Success	12544	2015-04-22 21:18:09	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: LTRANPHD$ Account Domain: WORKGROUP Logon ID: 0x3e7 Logon Type: 5 Impersonation Level: %%1833 New Logon: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Logon ID: 0x3e7 Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x230 Process Name: C:\Windows\System32\services.exe Network Information: Workstation Name: Source Network Address: - Source Port: - Detailed Authentication Information: Logon Process: Advapi Authentication Package: Negotiate Transited Services: - Package Name (NTLM only): - Key Length: 0 This event is generated when a logon session is created. It is generated on the computer that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service such as the Server service, or a local process such as Winlogon.exe or Services.exe. The logon type field indicates the kind of logon that occurred. The most common types are 2 (interactive) and 3 (network). The New Logon fields indicate the account for whom the new logon was created, i.e. the account that was logged on. The network fields indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impersonation level field indicates the extent to which a process in the logon session can impersonate. The authentication information fields provide detailed information about this specific logon request. - Logon GUID is a unique identifier that can be used to correlate this event with a KDC event. - Transited services indicate which intermediate services have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indicates the length of the generated session key. This will be 0 if no session key was requested.
Security	Audit Success	12548	2015-04-22 21:18:09	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-19 Account Name: LOCAL SERVICE Account Domain: NT AUTHORITY Logon ID: 0x3e5 Privileges: SeAssignPrimaryTokenPrivilege SeAuditPrivilege SeImpersonatePrivilege
Security	Audit Success	12548	2015-04-22 21:18:09	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Logon ID: 0x3e7 Privileges: SeAssignPrimaryTokenPrivilege SeTcbPrivilege SeSecurityPrivilege SeTakeOwnershipPrivilege SeLoadDriverPrivilege SeBackupPrivilege SeRestorePrivilege SeDebugPrivilege SeAuditPrivilege SeSystemEnvironmentPrivilege SeImpersonatePrivilege
Security	Audit Success	12292	2015-04-22 21:18:10	Microsoft-Windows-Security-Auditing	5033: The Windows Firewall Driver started successfully.
Security	Audit Success	12544	2015-04-22 21:18:10	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: LTRANPHD$ Account Domain: WORKGROUP Logon ID: 0x3e7 Logon Type: 5 Impersonation Level: %%1833 New Logon: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Logon ID: 0x3e7 Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x230 Process Name: C:\Windows\System32\services.exe Network Information: Workstation Name: Source Network Address: - Source Port: - Detailed Authentication Information: Logon Process: Advapi Authentication Package: Negotiate Transited Services: - Package Name (NTLM only): - Key Length: 0 This event is generated when a logon session is created. It is generated on the computer that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service such as the Server service, or a local process such as Winlogon.exe or Services.exe. The logon type field indicates the kind of logon that occurred. The most common types are 2 (interactive) and 3 (network). The New Logon fields indicate the account for whom the new logon was created, i.e. the account that was logged on. The network fields indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impersonation level field indicates the extent to which a process in the logon session can impersonate. The authentication information fields provide detailed information about this specific logon request. - Logon GUID is a unique identifier that can be used to correlate this event with a KDC event. - Transited services indicate which intermediate services have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indicates the length of the generated session key. This will be 0 if no session key was requested.
					4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: LTRANPHD$ Account Domain: WORKGROUP Logon ID: 0x3e7 Logon Type: 5 Impersonation Level: %%1833 New Logon: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Logon ID: 0x3e7 Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x230 Process Name: C:\Windows\System32\services.exe Network Information: Workstation Name: Source Network Address: - Source Port: - Detailed Authentication Information: Logon Process: Advapi Authentication Package: Negotiate Transited

Security	Audit Success	12544	2015-04-22 21:18:10	Microsoft-Windows-Security-Auditing	Services: - Package Name (NTLM only): - Key Length: 0 This event is generated when a logon session is created. It is generated on the computer that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service such as the Server service, or a local process such as Winlogon.exe or Services.exe. The logon type field indicates the kind of logon that occurred. The most common types are 2 (interactive) and 3 (network). The New Logon fields indicate the account for whom the new logon was created, i.e. the account that was logged on. The network fields indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impersonation level field indicates the extent to which a process in the logon session can impersonate. The authentication information fields provide detailed information about this specific logon request. - Logon GUID is a unique identifier that can be used to correlate this event with a KDC event. - Transited services indicate which intermediate services have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indicates the length of the generated session key. This will be 0 if no session key was requested.
Security	Audit Success	12544	2015-04-22 21:18:10	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: LTRANPHD$ Account Domain: WORKGROUP Logon ID: 0x3e7 Logon Type: 5 Impersonation Level: %%1833 New Logon: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Logon ID: 0x3e7 Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x230 Process Name: C:\Windows\System32\services.exe Network Information: Workstation Name: Source Network Address: - Source Port: - Detailed Authentication Information: Logon Process: Advapi Authentication Package: Negotiate Transited Services: - Package Name (NTLM only): - Key Length: 0 This event is generated when a logon session is created. It is generated on the computer that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service such as the Server service, or a local process such as Winlogon.exe or Services.exe. The logon type field indicates the kind of logon that occurred. The most common types are 2 (interactive) and 3 (network). The New Logon fields indicate the account for whom the new logon was created, i.e. the account that was logged on. The network fields indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impersonation level field indicates the extent to which a process in the logon session can impersonate. The authentication information fields provide detailed information about this specific logon request. - Logon GUID is a unique identifier that can be used to correlate this event with a KDC event. - Transited services indicate which intermediate services have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indicates the length of the generated session key. This will be 0 if no session key was requested.
Security	Audit Success	12548	2015-04-22 21:18:10	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Logon ID: 0x3e7 Privileges: SeAssignPrimaryTokenPrivilege SeTcbPrivilege SeSecurityPrivilege SeTakeOwnershipPrivilege SeLoadDriverPrivilege SeBackupPrivilege SeRestorePrivilege SeDebugPrivilege SeAuditPrivilege SeSystemEnvironmentPrivilege SeImpersonatePrivilege
Security	Audit Success	12548	2015-04-22 21:18:10	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Logon ID: 0x3e7 Privileges: SeAssignPrimaryTokenPrivilege SeTcbPrivilege SeSecurityPrivilege SeTakeOwnershipPrivilege SeLoadDriverPrivilege SeBackupPrivilege SeRestorePrivilege SeDebugPrivilege SeAuditPrivilege SeSystemEnvironmentPrivilege SeImpersonatePrivilege
Security	Audit Success	12548	2015-04-22 21:18:10	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Logon ID: 0x3e7 Privileges: SeAssignPrimaryTokenPrivilege SeTcbPrivilege SeSecurityPrivilege SeTakeOwnershipPrivilege SeLoadDriverPrivilege SeBackupPrivilege SeRestorePrivilege SeDebugPrivilege SeAuditPrivilege SeSystemEnvironmentPrivilege SeImpersonatePrivilege
Security	Audit Success	12292	2015-04-22 21:18:11	Microsoft-Windows-Security-Auditing	5024: The Windows Firewall service started successfully.
Security	Audit Success	12544	2015-04-22 21:18:11	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: LTRANPHD$ Account Domain: WORKGROUP Logon ID: 0x3e7 Logon Type: 5 Impersonation Level: %%1833 New Logon: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Logon ID: 0x3e7 Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x230 Process Name: C:\Windows\System32\services.exe Network Information: Workstation Name: Source Network Address: - Source Port: - Detailed Authentication Information: Logon Process: Advapi Authentication Package: Negotiate Transited Services: - Package Name (NTLM only): - Key Length: 0 This event is generated when a logon session is created. It is generated on the computer that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service such as the Server service, or a local process such as Winlogon.exe or Services.exe. The logon type field indicates the kind of logon that occurred. The most common types are 2 (interactive) and 3 (network). The New Logon fields indicate the account for whom the new logon was created, i.e. the account that was logged on. The network fields indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impersonation level field indicates the extent to which a process in the logon session can impersonate. The authentication information fields provide detailed information about this specific logon request. - Logon GUID is a unique identifier that can be used to correlate this event with a KDC event. - Transited services indicate which intermediate services have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indicates the length of the generated session key. This will be 0 if no session key was requested.

Security	Audit Success	12544	2015-04-22 21:18:11	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-0-0 Account Name: - Account Domain: - Logon ID: 0x0 Logon Type: 3 Impersonation Level: %%1833 New Logon: Security ID: S-1-5-7 Account Name: ANONYMOUS LOGON Account Domain: NT AUTHORITY Logon ID: 0x174c5 Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x0 Process Name: - Network Information: Workstation Name: Source Network Address: - Source Port: - Detailed Authentication Information: Logon Process: NtLmSsp Authentication Package: NTLM Transited Services: - Package Name (NTLM only): NTLM V1 Key Length: 0 This event is generated when a logon session is created. It is generated on the computer that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service such as the Server service, or a local process such as Winlogon.exe or Services.exe. The logon type field indicates the kind of logon that occurred. The most common types are 2 (interactive) and 3 (network). The New Logon fields indicate the account for whom the new logon was created, i.e. the account that was logged on. The network fields indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impersonation level field indicates the extent to which a process in the logon session can impersonate. The authentication information fields provide detailed information about this specific logon request. - Logon GUID is a unique identifier that can be used to correlate this event with a KDC event. - Transited services indicate which intermediate services have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indicates the length of the generated session key. This will be 0 if no session key was requested.
Security	Audit Success	12548	2015-04-22 21:18:11	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Logon ID: 0x3e7 Privileges: SeAssignPrimaryTokenPrivilege SeTcbPrivilege SeSecurityPrivilege SeTakeOwnershipPrivilege SeLoadDriverPrivilege SeBackupPrivilege SeRestorePrivilege SeDebugPrivilege SeAuditPrivilege SeSystemEnvironmentPrivilege SeImpersonatePrivilege
Security	Audit Success	12544	2015-04-22 21:18:12	Microsoft-Windows-Security-Auditing	4648: A logon was attempted using explicit credentials. Subject: Security ID: S-1-5-18 Account Name: LTRANPHD$ Account Domain: WORKGROUP Logon ID: 0x3e7 Logon GUID: {00000000-0000-0000-0000-000000000000} Account Whose Credentials Were Used: Account Name: Liem Account Domain: LTRANPHD Logon GUID: {00000000-0000-0000-0000-000000000000} Target Server: Target Server Name: localhost Additional Information: localhost Process Information: Process ID: 0x200 Process Name: C:\Windows\System32\winlogon.exe Network Information: Network Address: 127.0.0.1 Port: 0 This event is generated when a process attempts to log on an account by explicitly specifying that account's credentials. This most commonly occurs in batch-type configurations such as scheduled tasks, or when using the RUNAS command.
Security	Audit Success	12544	2015-04-22 21:18:12	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: LTRANPHD$ Account Domain: WORKGROUP Logon ID: 0x3e7 Logon Type: 2 Impersonation Level: %%1833 New Logon: Security ID: S-1-5-21-1888849264-3803429180-4108621888-1001 Account Name: Liem Account Domain: LTRANPHD Logon ID: 0x18b60 Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x200 Process Name: C:\Windows\System32\winlogon.exe Network Information: Workstation Name: LTRANPHD Source Network Address: 127.0.0.1 Source Port: 0 Detailed Authentication Information: Logon Process: User32 Authentication Package: Negotiate Transited Services: - Package Name (NTLM only): - Key Length: 0 This event is generated when a logon session is created. It is generated on the computer that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service such as the Server service, or a local process such as Winlogon.exe or Services.exe. The logon type field indicates the kind of logon that occurred. The most common types are 2 (interactive) and 3 (network). The New Logon fields indicate the account for whom the new logon was created, i.e. the account that was logged on. The network fields indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impersonation level field indicates the extent to which a process in the logon session can impersonate. The authentication information fields provide detailed information about this specific logon request. - Logon GUID is a unique identifier that can be used to correlate this event with a KDC event. - Transited services indicate which intermediate services have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indicates the length of the generated session key. This will be 0 if no session key was requested.
Security	Audit Success	12544	2015-04-22 21:18:12	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: LTRANPHD$ Account Domain: WORKGROUP Logon ID: 0x3e7 Logon Type: 2 Impersonation Level: %%1833 New Logon: Security ID: S-1-5-21-1888849264-3803429180-4108621888-1001 Account Name: Liem Account Domain: LTRANPHD Logon ID: 0x18b93 Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x200 Process Name: C:\Windows\System32\winlogon.exe Network Information: Workstation Name: LTRANPHD Source Network Address: 127.0.0.1 Source Port: 0 Detailed Authentication Information: Logon Process: User32 Authentication Package: Negotiate Transited Services: - Package Name (NTLM only): - Key Length: 0 This event is generated when a logon session is created. It is generated on the computer that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service such as the Server service, or a local process such as Winlogon.exe or Services.exe. The logon type field indicates the kind of logon that occurred. The most common types are 2 (interactive) and 3 (network). The New Logon fields indicate the account for whom the new logon was created, i.e. the account that was logged on. The network fields indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impersonation level field indicates the extent to which a process in the logon session can impersonate. The authentication information fields provide detailed information about this specific logon request. - Logon GUID is a unique identifier that can be used to correlate this event with a KDC event. - Transited services indicate which intermediate services have participated in this

					logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indicates the length of the generated session key. This will be 0 if no session key was requested.
Security	Audit Success	12544	2015-04-22 21:18:12	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: LTRANPHD$ Account Domain: WORKGROUP Logon ID: 0x3e7 Logon Type: 5 Impersonation Level: %%1833 New Logon: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Logon ID: 0x3e7 Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x230 Process Name: C:\Windows\System32\services.exe Network Information: Workstation Name: Source Network Address: - Source Port: - Detailed Authentication Information: Logon Process: Advapi Authentication Package: Negotiate Transited Services: - Package Name (NTLM only): - Key Length: 0 This event is generated when a logon session is created. It is generated on the computer that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service such as the Server service, or a local process such as Winlogon.exe or Services.exe. The logon type field indicates the kind of logon that occurred. The most common types are 2 (interactive) and 3 (network). The New Logon fields indicate the account for whom the new logon was created, i.e. the account that was logged on. The network fields indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impersonation level field indicates the extent to which a process in the logon session can impersonate. The authentication information fields provide detailed information about this specific logon request. - Logon GUID is a unique identifier that can be used to correlate this event with a KDC event. - Transited services indicate which intermediate services have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indicates the length of the generated session key. This will be 0 if no session key was requested.
Security	Audit Success	12548	2015-04-22 21:18:12	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-21-1888849264-3803429180-4108621888-1001 Account Name: Liem Account Domain: LTRANPHD Logon ID: 0x18b60 Privileges: SeSecurityPrivilege SeTakeOwnershipPrivilege SeLoadDriverPrivilege SeBackupPrivilege SeRestorePrivilege SeDebugPrivilege SeSystemEnvironmentPrivilege SeImpersonatePrivilege
Security	Audit Success	12548	2015-04-22 21:18:12	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Logon ID: 0x3e7 Privileges: SeAssignPrimaryTokenPrivilege SeTcbPrivilege SeSecurityPrivilege SeTakeOwnershipPrivilege SeLoadDriverPrivilege SeBackupPrivilege SeRestorePrivilege SeDebugPrivilege SeAuditPrivilege SeSystemEnvironmentPrivilege SeImpersonatePrivilege
Security	Audit Success	13824	2015-04-22 21:18:15	Microsoft-Windows-Security-Auditing	4797: An attempt was made to query the existence of a blank password for an account. Subject: Security ID: S-1-5-21-1888849264-3803429180-4108621888-1001 Account Name: Liem Account Domain: LTRANPHD Logon ID: 0x18b93 Additional Information: Caller Workstation: LTRANPHD Target Account Name: Administrator Target Account Domain: LTRANPHD
Security	Audit Success	13824	2015-04-22 21:18:15	Microsoft-Windows-Security-Auditing	4797: An attempt was made to query the existence of a blank password for an account. Subject: Security ID: S-1-5-21-1888849264-3803429180-4108621888-1001 Account Name: Liem Account Domain: LTRANPHD Logon ID: 0x18b93 Additional Information: Caller Workstation: LTRANPHD Target Account Name: Guest Target Account Domain: LTRANPHD
Security	Audit Success	13824	2015-04-22 21:18:15	Microsoft-Windows-Security-Auditing	4797: An attempt was made to query the existence of a blank password for an account. Subject: Security ID: S-1-5-21-1888849264-3803429180-4108621888-1001 Account Name: Liem Account Domain: LTRANPHD Logon ID: 0x18b93 Additional Information: Caller Workstation: LTRANPHD Target Account Name: Administrator Target Account Domain: LTRANPHD
Security	Audit Success	13824	2015-04-22 21:18:15	Microsoft-Windows-Security-Auditing	4797: An attempt was made to query the existence of a blank password for an account. Subject: Security ID: S-1-5-21-1888849264-3803429180-4108621888-1001 Account Name: Liem Account Domain: LTRANPHD Logon ID: 0x18b93 Additional Information: Caller Workstation: LTRANPHD Target Account Name: Guest Target Account Domain: LTRANPHD
Security	Audit Success	13824	2015-04-22 21:18:19	Microsoft-Windows-Security-Auditing	4797: An attempt was made to query the existence of a blank password for an account. Subject: Security ID: S-1-5-19 Account Name: LOCAL SERVICE Account Domain: NT AUTHORITY Logon ID: 0x3e5 Additional Information: Caller Workstation: LTRANPHD Target Account Name: Administrator Target Account Domain: LTRANPHD
Security	Audit Success	13824	2015-04-22 21:18:19	Microsoft-Windows-Security-Auditing	4797: An attempt was made to query the existence of a blank password for an account. Subject: Security ID: S-1-5-19 Account Name: LOCAL SERVICE Account Domain: NT AUTHORITY Logon ID: 0x3e5 Additional Information: Caller Workstation: LTRANPHD Target Account Name: Guest Target Account Domain: LTRANPHD
Security	Audit Success	13824	2015-04-22 21:18:19	Microsoft-Windows-Security-Auditing	4797: An attempt was made to query the existence of a blank password for an account. Subject: Security ID: S-1-5-19 Account Name: LOCAL SERVICE Account Domain: NT AUTHORITY Logon ID: 0x3e5 Additional Information: Caller Workstation: LTRANPHD Target Account Name: Liem Target Account Domain: LTRANPHD
Security	Audit Success	13824	2015-04-22 21:18:19	Microsoft-Windows-Security-Auditing	4797: An attempt was made to query the existence of a blank password for an account. Subject: Security ID: S-1-5-19 Account Name: LOCAL SERVICE Account Domain: NT AUTHORITY Logon ID: 0x3e5 Additional Information: Caller Workstation: LTRANPHD Target Account Name: Liem Target Account Domain: LTRANPHD
Security	Audit Success	13824	2015-04-22 21:18:19	Microsoft-Windows-Security-Auditing	4797: An attempt was made to query the existence of a blank password for an account. Subject: Security ID: S-1-5-19 Account Name: LOCAL SERVICE Account Domain: NT AUTHORITY Logon ID: 0x3e5 Additional Information: Caller Workstation: LTRANPHD Target Account Name: Administrator Target Account Domain: LTRANPHD
Security	Audit Success	13824	2015-04-22	Microsoft-Windows-Security-Auditing	4797: An attempt was made to query the existence of a blank password for an account. Subject: Security ID: S-1-5-19 Account Name: LOCAL SERVICE Account Domain: NT AUTHORITY Logon ID: 0x3e5 Additional

			21:18:19		Information: Caller Workstation: LTRANPHD Target Account Name: Guest Target Account Domain: LTRANPHD
Security	Audit Success	13824	2015-04-22 21:18:19	Microsoft-Windows-Security-Auditing	4797: An attempt was made to query the existence of a blank password for an account. Subject: Security ID: S-1-5-19 Account Name: LOCAL SERVICE Account Domain: NT AUTHORITY Logon ID: 0x3e5 Additional Information: Caller Workstation: LTRANPHD Target Account Name: Liem Target Account Domain: LTRANPHD
Security	Audit Success	13824	2015-04-22 21:18:19	Microsoft-Windows-Security-Auditing	4797: An attempt was made to query the existence of a blank password for an account. Subject: Security ID: S-1-5-19 Account Name: LOCAL SERVICE Account Domain: NT AUTHORITY Logon ID: 0x3e5 Additional Information: Caller Workstation: LTRANPHD Target Account Name: Liem Target Account Domain: LTRANPHD
Security	Audit Success	12544	2015-04-22 21:33:45	Microsoft-Windows-Security-Auditing	4648: A logon was attempted using explicit credentials. Subject: Security ID: S-1-5-18 Account Name: LTRANPHD$ Account Domain: WORKGROUP Logon ID: 0x3e7 Logon GUID: {00000000-0000-0000-0000-000000000000} Account Whose Credentials Were Used: Account Name: Liem Account Domain: LTRANPHD Logon GUID: {00000000-0000-0000-0000-000000000000} Target Server: Target Server Name: localhost Additional Information: localhost Process Information: Process ID: 0x200 Process Name: C:\Windows\System32\winlogon.exe Network Information: Network Address: 127.0.0.1 Port: 0 This event is generated when a process attempts to log on an account by explicitly specifying that account's credentials. This most commonly occurs in batch-type configurations such as scheduled tasks, or when using the RUNAS command.
Security	Audit Success	12544	2015-04-22 21:33:45	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: LTRANPHD$ Account Domain: WORKGROUP Logon ID: 0x3e7 Logon Type: 7 Impersonation Level: %%1833 New Logon: Security ID: S-1-5-21-1888849264-3803429180-4108621888-1001 Account Name: Liem Account Domain: LTRANPHD Logon ID: 0x10f7ab Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x200 Process Name: C:\Windows\System32\winlogon.exe Network Information: Workstation Name: LTRANPHD Source Network Address: 127.0.0.1 Source Port: 0 Detailed Authentication Information: Logon Process: User32 Authentication Package: Negotiate Transited Services: - Package Name (NTLM only): - Key Length: 0 This event is generated when a logon session is created. It is generated on the computer that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service such as the Server service, or a local process such as Winlogon.exe or Services.exe. The logon type field indicates the kind of logon that occurred. The most common types are 2 (interactive) and 3 (network). The New Logon fields indicate the account for whom the new logon was created, i.e. the account that was logged on. The network fields indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impersonation level field indicates the extent to which a process in the logon session can impersonate. The authentication information fields provide detailed information about this specific logon request. - Logon GUID is a unique identifier that can be used to correlate this event with a KDC event. - Transited services indicate which intermediate services have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indicates the length of the generated session key. This will be 0 if no session key was requested.
Security	Audit Success	12544	2015-04-22 21:33:45	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: LTRANPHD$ Account Domain: WORKGROUP Logon ID: 0x3e7 Logon Type: 7 Impersonation Level: %%1833 New Logon: Security ID: S-1-5-21-1888849264-3803429180-4108621888-1001 Account Name: Liem Account Domain: LTRANPHD Logon ID: 0x10f7ca Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x200 Process Name: C:\Windows\System32\winlogon.exe Network Information: Workstation Name: LTRANPHD Source Network Address: 127.0.0.1 Source Port: 0 Detailed Authentication Information: Logon Process: User32 Authentication Package: Negotiate Transited Services: - Package Name (NTLM only): - Key Length: 0 This event is generated when a logon session is created. It is generated on the computer that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service such as the Server service, or a local process such as Winlogon.exe or Services.exe. The logon type field indicates the kind of logon that occurred. The most common types are 2 (interactive) and 3 (network). The New Logon fields indicate the account for whom the new logon was created, i.e. the account that was logged on. The network fields indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impersonation level field indicates the extent to which a process in the logon session can impersonate. The authentication information fields provide detailed information about this specific logon request. - Logon GUID is a unique identifier that can be used to correlate this event with a KDC event. - Transited services indicate which intermediate services have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indicates the length of the generated session key. This will be 0 if no session key was requested.
Security	Audit Success	12545	2015-04-22 21:33:45	Microsoft-Windows-Security-Auditing	4634: An account was logged off. Subject: Security ID: S-1-5-21-1888849264-3803429180-4108621888-1001 Account Name: Liem Account Domain: LTRANPHD Logon ID: 0x10f7ca Logon Type: 7 This event is generated when a logon session is destroyed. It may be positively correlated with a logon event using the Logon ID value. Logon IDs are only unique between reboots on the same computer.
Security	Audit Success	12545	2015-04-22 21:33:45	Microsoft-Windows-Security-Auditing	4634: An account was logged off. Subject: Security ID: S-1-5-21-1888849264-3803429180-4108621888-1001 Account Name: Liem Account Domain: LTRANPHD Logon ID: 0x10f7ab Logon Type: 7 This event is generated when a logon session is destroyed. It may be positively correlated with a logon event using the Logon ID value. Logon IDs are only unique between reboots on the same computer.
	Audit		2015-04-	Microsoft-Windows-Security-	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-21-1888849264-3803429180-4108621888-1001 Account Name: Liem Account Domain: LTRANPHD Logon ID: 0x10f7ab Privileges:

Security	Success	12548	22 21:33:45	Auditing	SeSecurityPrivilege SeTakeOwnershipPrivilege SeLoadDriverPrivilege SeBackupPrivilege SeRestorePrivilege SeDebugPrivilege SeSystemEnvironmentPrivilege SeImpersonatePrivilege
Security	Audit Success	103	2015-04-22 22:02:12	Microsoft-Windows-Eventlog	1100: The event logging service has shut down.
Security	Audit Success	12545	2015-04-22 22:02:12	Microsoft-Windows-Security-Auditing	4647: User initiated logoff: Subject: Security ID: S-1-5-21-1888849264-3803429180-4108621888-1001 Account Name: Liem Account Domain: LTRANPHD Logon ID: 0x18b93 This event is generated when a logoff is initiated. No further user-initiated activity can occur. This event can be interpreted as a logoff event.
Security	Audit Success	12288	2015-04-23 07:23:43	Microsoft-Windows-Security-Auditing	4608: Windows is starting up. This event is logged when LSASS.EXE starts and the auditing subsystem is initialized.
Security	Audit Success	12544	2015-04-23 07:23:44	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-0-0 Account Name: - Account Domain: - Logon ID: 0x0 Logon Type: 0 Impersonation Level: - New Logon: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Logon ID: 0x3e7 Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x4 Process Name: Network Information: Workstation Name: - Source Network Address: - Source Port: - Detailed Authentication Information: Logon Process: - Authentication Package: - Transited Services: - Package Name (NTLM only): - Key Length: 0 This event is generated when a logon session is created. It is generated on the computer that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service such as the Server service, or a local process such as Winlogon.exe or Services.exe. The logon type field indicates the kind of logon that occurred. The most common types are 2 (interactive) and 3 (network). The New Logon fields indicate the account for whom the new logon was created, i.e. the account that was logged on. The network fields indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impersonation level field indicates the extent to which a process in the logon session can impersonate. The authentication information fields provide detailed information about this specific logon request. - Logon GUID is a unique identifier that can be used to correlate this event with a KDC event. - Transited services indicate which intermediate services have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indicates the length of the generated session key. This will be 0 if no session key was requested.
Security	Audit Success	12544	2015-04-23 07:23:44	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: LTRANPHD$ Account Domain: WORKGROUP Logon ID: 0x3e7 Logon Type: 5 Impersonation Level: %%1833 New Logon: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Logon ID: 0x3e7 Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x230 Process Name: C:\Windows\System32\services.exe Network Information: Workstation Name: Source Network Address: - Source Port: - Detailed Authentication Information: Logon Process: Advapi Authentication Package: Negotiate Transited Services: - Package Name (NTLM only): - Key Length: 0 This event is generated when a logon session is created. It is generated on the computer that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service such as the Server service, or a local process such as Winlogon.exe or Services.exe. The logon type field indicates the kind of logon that occurred. The most common types are 2 (interactive) and 3 (network). The New Logon fields indicate the account for whom the new logon was created, i.e. the account that was logged on. The network fields indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impersonation level field indicates the extent to which a process in the logon session can impersonate. The authentication information fields provide detailed information about this specific logon request. - Logon GUID is a unique identifier that can be used to correlate this event with a KDC event. - Transited services indicate which intermediate services have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indicates the length of the generated session key. This will be 0 if no session key was requested.
Security	Audit Success	12544	2015-04-23 07:23:44	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: LTRANPHD$ Account Domain: WORKGROUP Logon ID: 0x3e7 Logon Type: 5 Impersonation Level: %%1833 New Logon: Security ID: S-1-5-20 Account Name: NETWORK SERVICE Account Domain: NT AUTHORITY Logon ID: 0x3e4 Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x230 Process Name: C:\Windows\System32\services.exe Network Information: Workstation Name: Source Network Address: - Source Port: - Detailed Authentication Information: Logon Process: Advapi Authentication Package: Negotiate Transited Services: - Package Name (NTLM only): - Key Length: 0 This event is generated when a logon session is created. It is generated on the computer that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service such as the Server service, or a local process such as Winlogon.exe or Services.exe. The logon type field indicates the kind of logon that occurred. The most common types are 2 (interactive) and 3 (network). The New Logon fields indicate the account for whom the new logon was created, i.e. the account that was logged on. The network fields indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impersonation level field indicates the extent to which a process in the logon session can impersonate. The authentication information fields provide detailed information about this specific logon request. - Logon GUID is a unique identifier that can be used to correlate this event with a KDC event. - Transited services indicate which intermediate services have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indicates the length of the generated

					session key. This will be 0 if no session key was requested.
Security	Audit Success	12544	2015-04-23 07:23:44	Microsoft-Windows-Security-Auditing	4648: A logon was attempted using explicit credentials. Subject: Security ID: S-1-5-18 Account Name: LTRANPHD$ Account Domain: WORKGROUP Logon ID: 0x3e7 Logon GUID: {00000000-0000-0000-0000-000000000000} Account Whose Credentials Were Used: Account Name: DWM-1 Account Domain: Window Manager Logon GUID: {00000000-0000-0000-0000-000000000000} Target Server: Target Server Name: localhost Additional Information: localhost Process Information: Process ID: 0x200 Process Name: C:\Windows\System32\winlogon.exe Network Information: Network Address: - Port: - This event is generated when a process attempts to log on an account by explicitly specifying that account's credentials. This most commonly occurs in batch-type configurations such as scheduled tasks, or when using the RUNAS command.
Security	Audit Success	12544	2015-04-23 07:23:44	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: LTRANPHD$ Account Domain: WORKGROUP Logon ID: 0x3e7 Logon Type: 2 Impersonation Level: %%1833 New Logon: Security ID: S-1-5-90-1 Account Name: DWM-1 Account Domain: Window Manager Logon ID: 0xc3a8 Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x200 Process Name: C:\Windows\System32\winlogon.exe Network Information: Workstation Name: Source Network Address: - Source Port: - Detailed Authentication Information: Logon Process: Advapi Authentication Package: Negotiate Transited Services: - Package Name (NTLM only): - Key Length: 0 This event is generated when a logon session is created. It is generated on the computer that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service such as the Server service, or a local process such as Winlogon.exe or Services.exe. The logon type field indicates the kind of logon that occurred. The most common types are 2 (interactive) and 3 (network). The New Logon fields indicate the account for whom the new logon was created, i.e. the account that was logged on. The network fields indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impersonation level field indicates the extent to which a process in the logon session can impersonate. The authentication information fields provide detailed information about this specific logon request. - Logon GUID is a unique identifier that can be used to correlate this event with a KDC event. - Transited services indicate which intermediate services have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indicates the length of the generated session key. This will be 0 if no session key was requested.
Security	Audit Success	12544	2015-04-23 07:23:44	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: LTRANPHD$ Account Domain: WORKGROUP Logon ID: 0x3e7 Logon Type: 2 Impersonation Level: %%1833 New Logon: Security ID: S-1-5-90-1 Account Name: DWM-1 Account Domain: Window Manager Logon ID: 0xc3c4 Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x200 Process Name: C:\Windows\System32\winlogon.exe Network Information: Workstation Name: Source Network Address: - Source Port: - Detailed Authentication Information: Logon Process: Advapi Authentication Package: Negotiate Transited Services: - Package Name (NTLM only): - Key Length: 0 This event is generated when a logon session is created. It is generated on the computer that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service such as the Server service, or a local process such as Winlogon.exe or Services.exe. The logon type field indicates the kind of logon that occurred. The most common types are 2 (interactive) and 3 (network). The New Logon fields indicate the account for whom the new logon was created, i.e. the account that was logged on. The network fields indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impersonation level field indicates the extent to which a process in the logon session can impersonate. The authentication information fields provide detailed information about this specific logon request. - Logon GUID is a unique identifier that can be used to correlate this event with a KDC event. - Transited services indicate which intermediate services have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indicates the length of the generated session key. This will be 0 if no session key was requested.
Security	Audit Success	12544	2015-04-23 07:23:44	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: LTRANPHD$ Account Domain: WORKGROUP Logon ID: 0x3e7 Logon Type: 5 Impersonation Level: %%1833 New Logon: Security ID: S-1-5-19 Account Name: LOCAL SERVICE Account Domain: NT AUTHORITY Logon ID: 0x3e5 Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x230 Process Name: C:\Windows\System32\services.exe Network Information: Workstation Name: Source Network Address: - Source Port: - Detailed Authentication Information: Logon Process: Advapi Authentication Package: Negotiate Transited Services: - Package Name (NTLM only): - Key Length: 0 This event is generated when a logon session is created. It is generated on the computer that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service such as the Server service, or a local process such as Winlogon.exe or Services.exe. The logon type field indicates the kind of logon that occurred. The most common types are 2 (interactive) and 3 (network). The New Logon fields indicate the account for whom the new logon was created, i.e. the account that was logged on. The network fields indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impersonation level field indicates the extent to which a process in the logon session can impersonate. The authentication information fields provide detailed information about this specific logon request. - Logon GUID is a unique identifier that can be used to correlate this event with a KDC event. - Transited services indicate which intermediate services have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indicates the length of the generated session key. This will be 0 if no session key was requested.

Security	Audit Success	12544	2015-04-23 07:23:44	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: LTRANPHD$ Account Domain: WORKGROUP Logon ID: 0x3e7 Logon Type: 5 Impersonation Level: %%1833 New Logon: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Logon ID: 0x3e7 Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x230 Process Name: C:\Windows\System32\services.exe Network Information: Workstation Name: Source Network Address: - Source Port: - Detailed Authentication Information: Logon Process: Advapi Authentication Package: Negotiate Transited Services: - Package Name (NTLM only): - Key Length: 0 This event is generated when a logon session is created. It is generated on the computer that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service such as the Server service, or a local process such as Winlogon.exe or Services.exe. The logon type field indicates the kind of logon that occurred. The most common types are 2 (interactive) and 3 (network). The New Logon fields indicate the account for whom the new logon was created, i.e. the account that was logged on. The network fields indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impersonation level field indicates the extent to which a process in the logon session can impersonate. The authentication information fields provide detailed information about this specific logon request. - Logon GUID is a unique identifier that can be used to correlate this event with a KDC event. - Transited services indicate which intermediate services have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indicates the length of the generated session key. This will be 0 if no session key was requested.
Security	Audit Success	12544	2015-04-23 07:23:44	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: LTRANPHD$ Account Domain: WORKGROUP Logon ID: 0x3e7 Logon Type: 5 Impersonation Level: %%1833 New Logon: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Logon ID: 0x3e7 Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x230 Process Name: C:\Windows\System32\services.exe Network Information: Workstation Name: Source Network Address: - Source Port: - Detailed Authentication Information: Logon Process: Advapi Authentication Package: Negotiate Transited Services: - Package Name (NTLM only): - Key Length: 0 This event is generated when a logon session is created. It is generated on the computer that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service such as the Server service, or a local process such as Winlogon.exe or Services.exe. The logon type field indicates the kind of logon that occurred. The most common types are 2 (interactive) and 3 (network). The New Logon fields indicate the account for whom the new logon was created, i.e. the account that was logged on. The network fields indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impersonation level field indicates the extent to which a process in the logon session can impersonate. The authentication information fields provide detailed information about this specific logon request. - Logon GUID is a unique identifier that can be used to correlate this event with a KDC event. - Transited services indicate which intermediate services have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indicates the length of the generated session key. This will be 0 if no session key was requested.
Security	Audit Success	12548	2015-04-23 07:23:44	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Logon ID: 0x3e7 Privileges: SeAssignPrimaryTokenPrivilege SeTcbPrivilege SeSecurityPrivilege SeTakeOwnershipPrivilege SeLoadDriverPrivilege SeBackupPrivilege SeRestorePrivilege SeDebugPrivilege SeAuditPrivilege SeSystemEnvironmentPrivilege SeImpersonatePrivilege
Security	Audit Success	12548	2015-04-23 07:23:44	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-20 Account Name: NETWORK SERVICE Account Domain: NT AUTHORITY Logon ID: 0x3e4 Privileges: SeAssignPrimaryTokenPrivilege SeAuditPrivilege SeImpersonatePrivilege
Security	Audit Success	12548	2015-04-23 07:23:44	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-90-1 Account Name: DWM-1 Account Domain: Window Manager Logon ID: 0xc3a8 Privileges: SeAssignPrimaryTokenPrivilege SeAuditPrivilege SeImpersonatePrivilege
Security	Audit Success	12548	2015-04-23 07:23:44	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-90-1 Account Name: DWM-1 Account Domain: Window Manager Logon ID: 0xc3c4 Privileges: SeAssignPrimaryTokenPrivilege SeAuditPrivilege
Security	Audit Success	12548	2015-04-23 07:23:44	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-19 Account Name: LOCAL SERVICE Account Domain: NT AUTHORITY Logon ID: 0x3e5 Privileges: SeAssignPrimaryTokenPrivilege SeAuditPrivilege SeImpersonatePrivilege
Security	Audit Success	12548	2015-04-23 07:23:44	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Logon ID: 0x3e7 Privileges: SeAssignPrimaryTokenPrivilege SeTcbPrivilege SeSecurityPrivilege SeTakeOwnershipPrivilege SeLoadDriverPrivilege SeBackupPrivilege SeRestorePrivilege SeDebugPrivilege SeAuditPrivilege SeSystemEnvironmentPrivilege SeImpersonatePrivilege
Security	Audit Success	12548	2015-04-23 07:23:44	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Logon ID: 0x3e7 Privileges: SeAssignPrimaryTokenPrivilege SeTcbPrivilege SeSecurityPrivilege SeTakeOwnershipPrivilege SeLoadDriverPrivilege SeBackupPrivilege SeRestorePrivilege SeDebugPrivilege SeAuditPrivilege SeSystemEnvironmentPrivilege SeImpersonatePrivilege
Security	Audit Success	13568	2015-04-23 07:23:44	Microsoft-Windows-Security-Auditing	4902: The Per-user audit policy table was created. Number of Elements: 0 Policy ID: 0x7441

Security	Audit Success	12292	2015-04-23 07:23:45	Microsoft-Windows-Security-Auditing	5033: The Windows Firewall Driver started successfully.
Security	Audit Success	12544	2015-04-23 07:23:45	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: LTRANPHD$ Account Domain: WORKGROUP Logon ID: 0x3e7 Logon Type: 5 Impersonation Level: %%1833 New Logon: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Logon ID: 0x3e7 Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x230 Process Name: C:\Windows\System32\services.exe Network Information: Workstation Name: Source Network Address: - Source Port: - Detailed Authentication Information: Logon Process: Advapi Authentication Package: Negotiate Transited Services: - Package Name (NTLM only): - Key Length: 0 This event is generated when a logon session is created. It is generated on the computer that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service such as the Server service, or a local process such as Winlogon.exe or Services.exe. The logon type field indicates the kind of logon that occurred. The most common types are 2 (interactive) and 3 (network). The New Logon fields indicate the account for whom the new logon was created, i.e. the account that was logged on. The network fields indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impersonation level field indicates the extent to which a process in the logon session can impersonate. The authentication information fields provide detailed information about this specific logon request. - Logon GUID is a unique identifier that can be used to correlate this event with a KDC event. - Transited services indicate which intermediate services have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indicates the length of the generated session key. This will be 0 if no session key was requested.
Security	Audit Success	12544	2015-04-23 07:23:45	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: LTRANPHD$ Account Domain: WORKGROUP Logon ID: 0x3e7 Logon Type: 5 Impersonation Level: %%1833 New Logon: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Logon ID: 0x3e7 Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x230 Process Name: C:\Windows\System32\services.exe Network Information: Workstation Name: Source Network Address: - Source Port: - Detailed Authentication Information: Logon Process: Advapi Authentication Package: Negotiate Transited Services: - Package Name (NTLM only): - Key Length: 0 This event is generated when a logon session is created. It is generated on the computer that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service such as the Server service, or a local process such as Winlogon.exe or Services.exe. The logon type field indicates the kind of logon that occurred. The most common types are 2 (interactive) and 3 (network). The New Logon fields indicate the account for whom the new logon was created, i.e. the account that was logged on. The network fields indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impersonation level field indicates the extent to which a process in the logon session can impersonate. The authentication information fields provide detailed information about this specific logon request. - Logon GUID is a unique identifier that can be used to correlate this event with a KDC event. - Transited services indicate which intermediate services have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indicates the length of the generated session key. This will be 0 if no session key was requested.
Security	Audit Success	12548	2015-04-23 07:23:45	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Logon ID: 0x3e7 Privileges: SeAssignPrimaryTokenPrivilege SeTcbPrivilege SeSecurityPrivilege SeTakeOwnershipPrivilege SeLoadDriverPrivilege SeBackupPrivilege SeRestorePrivilege SeDebugPrivilege SeAuditPrivilege SeSystemEnvironmentPrivilege SeImpersonatePrivilege
Security	Audit Success	12548	2015-04-23 07:23:45	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Logon ID: 0x3e7 Privileges: SeAssignPrimaryTokenPrivilege SeTcbPrivilege SeSecurityPrivilege SeTakeOwnershipPrivilege SeLoadDriverPrivilege SeBackupPrivilege SeRestorePrivilege SeDebugPrivilege SeAuditPrivilege SeSystemEnvironmentPrivilege SeImpersonatePrivilege
Security	Audit Success	12292	2015-04-23 07:23:46	Microsoft-Windows-Security-Auditing	5024: The Windows Firewall service started successfully.
Security	Audit Success	12544	2015-04-23 07:23:46	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: LTRANPHD$ Account Domain: WORKGROUP Logon ID: 0x3e7 Logon Type: 5 Impersonation Level: %%1833 New Logon: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Logon ID: 0x3e7 Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x230 Process Name: C:\Windows\System32\services.exe Network Information: Workstation Name: Source Network Address: - Source Port: - Detailed Authentication Information: Logon Process: Advapi Authentication Package: Negotiate Transited Services: - Package Name (NTLM only): - Key Length: 0 This event is generated when a logon session is created. It is generated on the computer that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service such as the Server service, or a local process such as Winlogon.exe or Services.exe. The logon type field indicates the kind of logon that occurred. The most common types are 2 (interactive) and 3 (network). The New Logon fields indicate the account for whom the new logon was created, i.e. the account that was logged on. The network fields indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impersonation level field indicates the extent to which a process in the logon session can

					impersonate. The authentication information fields provide detailed information about this specific logon request. - Logon GUID is a unique identifier that can be used to correlate this event with a KDC event. - Transited services indicate which intermediate services have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indicates the length of the generated session key. This will be 0 if no session key was requested.
Security	Audit Success	12544	2015-04-23 07:23:46	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-0-0 Account Name: - Account Domain: - Logon ID: 0x0 Logon Type: 3 Impersonation Level: %%1833 New Logon: Security ID: S-1-5-7 Account Name: ANONYMOUS LOGON Account Domain: NT AUTHORITY Logon ID: 0x17697 Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x0 Process Name: - Network Information: Workstation Name: Source Network Address: - Source Port: - Detailed Authentication Information: Logon Process: NtLmSsp Authentication Package: NTLM Transited Services: - Package Name (NTLM only): NTLM V1 Key Length: 0 This event is generated when a logon session is created. It is generated on the computer that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service such as the Server service, or a local process such as Winlogon.exe or Services.exe. The logon type field indicates the kind of logon that occurred. The most common types are 2 (interactive) and 3 (network). The New Logon fields indicate the account for whom the new logon was created, i.e. the account that was logged on. The network fields indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impersonation level field indicates the extent to which a process in the logon session can impersonate. The authentication information fields provide detailed information about this specific logon request. - Logon GUID is a unique identifier that can be used to correlate this event with a KDC event. - Transited services indicate which intermediate services have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indicates the length of the generated session key. This will be 0 if no session key was requested.
Security	Audit Success	12548	2015-04-23 07:23:46	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Logon ID: 0x3e7 Privileges: SeAssignPrimaryTokenPrivilege SeTcbPrivilege SeSecurityPrivilege SeTakeOwnershipPrivilege SeLoadDriverPrivilege SeBackupPrivilege SeRestorePrivilege SeDebugPrivilege SeAuditPrivilege SeSystemEnvironmentPrivilege SeImpersonatePrivilege
Security	Audit Success	12544	2015-04-23 07:23:48	Microsoft-Windows-Security-Auditing	4648: A logon was attempted using explicit credentials. Subject: Security ID: S-1-5-18 Account Name: LTRANPHD$ Account Domain: WORKGROUP Logon ID: 0x3e7 Logon GUID: {00000000-0000-0000-0000-000000000000} Account Whose Credentials Were Used: Account Name: Liem Account Domain: LTRANPHD Logon GUID: {00000000-0000-0000-0000-000000000000} Target Server: Target Server Name: localhost Additional Information: localhost Process Information: Process ID: 0x200 Process Name: C:\Windows\System32\winlogon.exe Network Information: Network Address: 127.0.0.1 Port: 0 This event is generated when a process attempts to log on an account by explicitly specifying that account's credentials. This most commonly occurs in batch-type configurations such as scheduled tasks, or when using the RUNAS command.
Security	Audit Success	12544	2015-04-23 07:23:48	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: LTRANPHD$ Account Domain: WORKGROUP Logon ID: 0x3e7 Logon Type: 2 Impersonation Level: %%1833 New Logon: Security ID: S-1-5-21-1888849264-3803429180-4108621888-1001 Account Name: Liem Account Domain: LTRANPHD Logon ID: 0x18dca Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x200 Process Name: C:\Windows\System32\winlogon.exe Network Information: Workstation Name: LTRANPHD Source Network Address: 127.0.0.1 Source Port: 0 Detailed Authentication Information: Logon Process: User32 Authentication Package: Negotiate Transited Services: - Package Name (NTLM only): - Key Length: 0 This event is generated when a logon session is created. It is generated on the computer that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service such as the Server service, or a local process such as Winlogon.exe or Services.exe. The logon type field indicates the kind of logon that occurred. The most common types are 2 (interactive) and 3 (network). The New Logon fields indicate the account for whom the new logon was created, i.e. the account that was logged on. The network fields indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impersonation level field indicates the extent to which a process in the logon session can impersonate. The authentication information fields provide detailed information about this specific logon request. - Logon GUID is a unique identifier that can be used to correlate this event with a KDC event. - Transited services indicate which intermediate services have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indicates the length of the generated session key. This will be 0 if no session key was requested.
Security	Audit Success	12544	2015-04-23 07:23:48	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: LTRANPHD$ Account Domain: WORKGROUP Logon ID: 0x3e7 Logon Type: 2 Impersonation Level: %%1833 New Logon: Security ID: S-1-5-21-1888849264-3803429180-4108621888-1001 Account Name: Liem Account Domain: LTRANPHD Logon ID: 0x18dfd Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x200 Process Name: C:\Windows\System32\winlogon.exe Network Information: Workstation Name: LTRANPHD Source Network Address: 127.0.0.1 Source Port: 0 Detailed Authentication Information: Logon Process: User32 Authentication Package: Negotiate Transited Services: - Package Name (NTLM only): - Key Length: 0 This event is generated when a logon session is created. It is generated on the computer that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service such as the Server service, or a local process such as Winlogon.exe or Services.exe. The logon type field indicates the kind of logon that occurred. The most common types are 2 (interactive) and 3

					(network). The New Logon fields indicate the account for whom the new logon was created, i.e. the account that was logged on. The network fields indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impersonation level field indicates the extent to which a process in the logon session can impersonate. The authentication information fields provide detailed information about this specific logon request. - Logon GUID is a unique identifier that can be used to correlate this event with a KDC event. - Transited services indicate which intermediate services have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indicates the length of the generated session key. This will be 0 if no session key was requested.
Security	Audit Success	12548	2015-04-23 07:23:48	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-21-1888849264-3803429180-4108621888-1001 Account Name: Liem Account Domain: LTRANPHD Logon ID: 0x18dca Privileges: SeSecurityPrivilege SeTakeOwnershipPrivilege SeLoadDriverPrivilege SeBackupPrivilege SeRestorePrivilege SeDebugPrivilege SeSystemEnvironmentPrivilege SeImpersonatePrivilege
Security	Audit Success	12544	2015-04-23 07:23:49	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: LTRANPHD$ Account Domain: WORKGROUP Logon ID: 0x3e7 Logon Type: 5 Impersonation Level: %%1833 New Logon: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Logon ID: 0x3e7 Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x230 Process Name: C:\Windows\System32\services.exe Network Information: Workstation Name: Source Network Address: - Source Port: - Detailed Authentication Information: Logon Process: Advapi Authentication Package: Negotiate Transited Services: - Package Name (NTLM only): - Key Length: 0 This event is generated when a logon session is created. It is generated on the computer that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service such as the Server service, or a local process such as Winlogon.exe or Services.exe. The logon type field indicates the kind of logon that occurred. The most common types are 2 (interactive) and 3 (network). The New Logon fields indicate the account for whom the new logon was created, i.e. the account that was logged on. The network fields indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impersonation level field indicates the extent to which a process in the logon session can impersonate. The authentication information fields provide detailed information about this specific logon request. - Logon GUID is a unique identifier that can be used to correlate this event with a KDC event. - Transited services indicate which intermediate services have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indicates the length of the generated session key. This will be 0 if no session key was requested.
Security	Audit Success	12548	2015-04-23 07:23:49	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Logon ID: 0x3e7 Privileges: SeAssignPrimaryTokenPrivilege SeTcbPrivilege SeSecurityPrivilege SeTakeOwnershipPrivilege SeLoadDriverPrivilege SeBackupPrivilege SeRestorePrivilege SeDebugPrivilege SeAuditPrivilege SeSystemEnvironmentPrivilege SeImpersonatePrivilege
Security	Audit Success	13824	2015-04-23 07:23:51	Microsoft-Windows-Security-Auditing	4797: An attempt was made to query the existence of a blank password for an account. Subject: Security ID: S-1-5-21-1888849264-3803429180-4108621888-1001 Account Name: Liem Account Domain: LTRANPHD Logon ID: 0x18dfd Additional Information: Caller Workstation: LTRANPHD Target Account Name: Administrator Target Account Domain: LTRANPHD
Security	Audit Success	13824	2015-04-23 07:23:51	Microsoft-Windows-Security-Auditing	4797: An attempt was made to query the existence of a blank password for an account. Subject: Security ID: S-1-5-21-1888849264-3803429180-4108621888-1001 Account Name: Liem Account Domain: LTRANPHD Logon ID: 0x18dfd Additional Information: Caller Workstation: LTRANPHD Target Account Name: Guest Target Account Domain: LTRANPHD
Security	Audit Success	13824	2015-04-23 07:23:51	Microsoft-Windows-Security-Auditing	4797: An attempt was made to query the existence of a blank password for an account. Subject: Security ID: S-1-5-21-1888849264-3803429180-4108621888-1001 Account Name: Liem Account Domain: LTRANPHD Logon ID: 0x18dfd Additional Information: Caller Workstation: LTRANPHD Target Account Name: Administrator Target Account Domain: LTRANPHD
Security	Audit Success	13824	2015-04-23 07:23:51	Microsoft-Windows-Security-Auditing	4797: An attempt was made to query the existence of a blank password for an account. Subject: Security ID: S-1-5-21-1888849264-3803429180-4108621888-1001 Account Name: Liem Account Domain: LTRANPHD Logon ID: 0x18dfd Additional Information: Caller Workstation: LTRANPHD Target Account Name: Guest Target Account Domain: LTRANPHD
Security	Audit Success	13824	2015-04-23 07:23:52	Microsoft-Windows-Security-Auditing	4797: An attempt was made to query the existence of a blank password for an account. Subject: Security ID: S-1-5-19 Account Name: LOCAL SERVICE Account Domain: NT AUTHORITY Logon ID: 0x3e5 Additional Information: Caller Workstation: LTRANPHD Target Account Name: Administrator Target Account Domain: LTRANPHD
Security	Audit Success	13824	2015-04-23 07:23:52	Microsoft-Windows-Security-Auditing	4797: An attempt was made to query the existence of a blank password for an account. Subject: Security ID: S-1-5-19 Account Name: LOCAL SERVICE Account Domain: NT AUTHORITY Logon ID: 0x3e5 Additional Information: Caller Workstation: LTRANPHD Target Account Name: Guest Target Account Domain: LTRANPHD
Security	Audit Success	13824	2015-04-23 07:23:52	Microsoft-Windows-Security-Auditing	4797: An attempt was made to query the existence of a blank password for an account. Subject: Security ID: S-1-5-19 Account Name: LOCAL SERVICE Account Domain: NT AUTHORITY Logon ID: 0x3e5 Additional Information: Caller Workstation: LTRANPHD Target Account Name: Liem Target Account Domain: LTRANPHD
Security	Audit Success	13824	2015-04-23 07:23:52	Microsoft-Windows-Security-Auditing	4797: An attempt was made to query the existence of a blank password for an account. Subject: Security ID: S-1-5-19 Account Name: LOCAL SERVICE Account Domain: NT AUTHORITY Logon ID: 0x3e5 Additional Information: Caller Workstation: LTRANPHD Target Account Name: Liem Target Account Domain: LTRANPHD
					4797: An attempt was made to query the existence of a blank password for an account. Subject: Security ID:

Security	Audit Success	13824	2015-04-23 07:23:52	Microsoft-Windows-Security-Auditing	S-1-5-19 Account Name: LOCAL SERVICE Account Domain: NT AUTHORITY Logon ID: 0x3e5 Additional Information: Caller Workstation: LTRANPHD Target Account Name: Administrator Target Account Domain: LTRANPHD
Security	Audit Success	13824	2015-04-23 07:23:52	Microsoft-Windows-Security-Auditing	4797: An attempt was made to query the existence of a blank password for an account. Subject: Security ID: S-1-5-19 Account Name: LOCAL SERVICE Account Domain: NT AUTHORITY Logon ID: 0x3e5 Additional Information: Caller Workstation: LTRANPHD Target Account Name: Guest Target Account Domain: LTRANPHD
Security	Audit Success	13824	2015-04-23 07:23:52	Microsoft-Windows-Security-Auditing	4797: An attempt was made to query the existence of a blank password for an account. Subject: Security ID: S-1-5-19 Account Name: LOCAL SERVICE Account Domain: NT AUTHORITY Logon ID: 0x3e5 Additional Information: Caller Workstation: LTRANPHD Target Account Name: Liem Target Account Domain: LTRANPHD
Security	Audit Success	13824	2015-04-23 07:23:52	Microsoft-Windows-Security-Auditing	4797: An attempt was made to query the existence of a blank password for an account. Subject: Security ID: S-1-5-19 Account Name: LOCAL SERVICE Account Domain: NT AUTHORITY Logon ID: 0x3e5 Additional Information: Caller Workstation: LTRANPHD Target Account Name: Liem Target Account Domain: LTRANPHD
Security	Audit Success	12544	2015-04-23 07:26:47	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: LTRANPHD$ Account Domain: WORKGROUP Logon ID: 0x3e7 Logon Type: 5 Impersonation Level: %%1833 New Logon: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Logon ID: 0x3e7 Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x230 Process Name: C:\Windows\System32\services.exe Network Information: Workstation Name: Source Network Address: - Source Port: - Detailed Authentication Information: Logon Process: Advapi Authentication Package: Negotiate Transited Services: - Package Name (NTLM only): - Key Length: 0 This event is generated when a logon session is created. It is generated on the computer that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service such as the Server service, or a local process such as Winlogon.exe or Services.exe. The logon type field indicates the kind of logon that occurred. The most common types are 2 (interactive) and 3 (network). The New Logon fields indicate the account for whom the new logon was created, i.e. the account that was logged on. The network fields indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impersonation level field indicates the extent to which a process in the logon session can impersonate. The authentication information fields provide detailed information about this specific logon request. - Logon GUID is a unique identifier that can be used to correlate this event with a KDC event. - Transited services indicate which intermediate services have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indicates the length of the generated session key. This will be 0 if no session key was requested.
Security	Audit Success	12548	2015-04-23 07:26:47	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Logon ID: 0x3e7 Privileges: SeAssignPrimaryTokenPrivilege SeTcbPrivilege SeSecurityPrivilege SeTakeOwnershipPrivilege SeLoadDriverPrivilege SeBackupPrivilege SeRestorePrivilege SeDebugPrivilege SeAuditPrivilege SeSystemEnvironmentPrivilege SeImpersonatePrivilege
Security	Audit Success	12544	2015-04-23 07:26:48	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: LTRANPHD$ Account Domain: WORKGROUP Logon ID: 0x3e7 Logon Type: 5 Impersonation Level: %%1833 New Logon: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Logon ID: 0x3e7 Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x230 Process Name: C:\Windows\System32\services.exe Network Information: Workstation Name: Source Network Address: - Source Port: - Detailed Authentication Information: Logon Process: Advapi Authentication Package: Negotiate Transited Services: - Package Name (NTLM only): - Key Length: 0 This event is generated when a logon session is created. It is generated on the computer that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service such as the Server service, or a local process such as Winlogon.exe or Services.exe. The logon type field indicates the kind of logon that occurred. The most common types are 2 (interactive) and 3 (network). The New Logon fields indicate the account for whom the new logon was created, i.e. the account that was logged on. The network fields indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impersonation level field indicates the extent to which a process in the logon session can impersonate. The authentication information fields provide detailed information about this specific logon request. - Logon GUID is a unique identifier that can be used to correlate this event with a KDC event. - Transited services indicate which intermediate services have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indicates the length of the generated session key. This will be 0 if no session key was requested.
Security	Audit Success	12548	2015-04-23 07:26:48	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Logon ID: 0x3e7 Privileges: SeAssignPrimaryTokenPrivilege SeTcbPrivilege SeSecurityPrivilege SeTakeOwnershipPrivilege SeLoadDriverPrivilege SeBackupPrivilege SeRestorePrivilege SeDebugPrivilege SeAuditPrivilege SeSystemEnvironmentPrivilege SeImpersonatePrivilege
					4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: LTRANPHD$ Account Domain: WORKGROUP Logon ID: 0x3e7 Logon Type: 5 Impersonation Level: %%1833 New Logon: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Logon ID: 0x3e7 Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x230 Process Name: C:\Windows\System32\services.exe Network Information: Workstation Name: Source Network Address: - Source Port: - Detailed Authentication Information: Logon Process: Advapi Authentication Package: Negotiate Transited Services: - Package Name (NTLM only): - Key Length: 0 This event is generated when a logon session is

Security	Audit Success	12544	2015-04-23 07:41:09	Microsoft-Windows-Security-Auditing	created. It is generated on the computer that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service such as the Server service, or a local process such as Winlogon.exe or Services.exe. The logon type field indicates the kind of logon that occurred. The most common types are 2 (interactive) and 3 (network). The New Logon fields indicate the account for whom the new logon was created, i.e. the account that was logged on. The network fields indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impersonation level field indicates the extent to which a process in the logon session can impersonate. The authentication information fields provide detailed information about this specific logon request. - Logon GUID is a unique identifier that can be used to correlate this event with a KDC event. - Transited services indicate which intermediate services have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indicates the length of the generated session key. This will be 0 if no session key was requested.
Security	Audit Success	12548	2015-04-23 07:41:09	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Logon ID: 0x3e7 Privileges: SeAssignPrimaryTokenPrivilege SeTcbPrivilege SeSecurityPrivilege SeTakeOwnershipPrivilege SeLoadDriverPrivilege SeBackupPrivilege SeRestorePrivilege SeDebugPrivilege SeAuditPrivilege SeSystemEnvironmentPrivilege SeImpersonatePrivilege
Security	Audit Success	12544	2015-04-23 08:27:32	Microsoft-Windows-Security-Auditing	4648: A logon was attempted using explicit credentials. Subject: Security ID: S-1-5-18 Account Name: LTRANPHD$ Account Domain: WORKGROUP Logon ID: 0x3e7 Logon GUID: {00000000-0000-0000-0000-000000000000} Account Whose Credentials Were Used: Account Name: Liem Account Domain: LTRANPHD Logon GUID: {00000000-0000-0000-0000-000000000000} Target Server: Target Server Name: localhost Additional Information: localhost Process Information: Process ID: 0x200 Process Name: C:\Windows\System32\winlogon.exe Network Information: Network Address: 127.0.0.1 Port: 0 This event is generated when a process attempts to log on an account by explicitly specifying that account's credentials. This most commonly occurs in batch-type configurations such as scheduled tasks, or when using the RUNAS command.
Security	Audit Success	12544	2015-04-23 08:27:32	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: LTRANPHD$ Account Domain: WORKGROUP Logon ID: 0x3e7 Logon Type: 7 Impersonation Level: %%1833 New Logon: Security ID: S-1-5-21-1888849264-3803429180-4108621888-1001 Account Name: Liem Account Domain: LTRANPHD Logon ID: 0x5613ec Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x200 Process Name: C:\Windows\System32\winlogon.exe Network Information: Workstation Name: LTRANPHD Source Network Address: 127.0.0.1 Source Port: 0 Detailed Authentication Information: Logon Process: User32 Authentication Package: Negotiate Transited Services: - Package Name (NTLM only): - Key Length: 0 This event is generated when a logon session is created. It is generated on the computer that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service such as the Server service, or a local process such as Winlogon.exe or Services.exe. The logon type field indicates the kind of logon that occurred. The most common types are 2 (interactive) and 3 (network). The New Logon fields indicate the account for whom the new logon was created, i.e. the account that was logged on. The network fields indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impersonation level field indicates the extent to which a process in the logon session can impersonate. The authentication information fields provide detailed information about this specific logon request. - Logon GUID is a unique identifier that can be used to correlate this event with a KDC event. - Transited services indicate which intermediate services have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indicates the length of the generated session key. This will be 0 if no session key was requested.
Security	Audit Success	12544	2015-04-23 08:27:32	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: LTRANPHD$ Account Domain: WORKGROUP Logon ID: 0x3e7 Logon Type: 7 Impersonation Level: %%1833 New Logon: Security ID: S-1-5-21-1888849264-3803429180-4108621888-1001 Account Name: Liem Account Domain: LTRANPHD Logon ID: 0x561407 Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x200 Process Name: C:\Windows\System32\winlogon.exe Network Information: Workstation Name: LTRANPHD Source Network Address: 127.0.0.1 Source Port: 0 Detailed Authentication Information: Logon Process: User32 Authentication Package: Negotiate Transited Services: - Package Name (NTLM only): - Key Length: 0 This event is generated when a logon session is created. It is generated on the computer that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service such as the Server service, or a local process such as Winlogon.exe or Services.exe. The logon type field indicates the kind of logon that occurred. The most common types are 2 (interactive) and 3 (network). The New Logon fields indicate the account for whom the new logon was created, i.e. the account that was logged on. The network fields indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impersonation level field indicates the extent to which a process in the logon session can impersonate. The authentication information fields provide detailed information about this specific logon request. - Logon GUID is a unique identifier that can be used to correlate this event with a KDC event. - Transited services indicate which intermediate services have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indicates the length of the generated session key. This will be 0 if no session key was requested.
			2015-04-		4634: An account was logged off. Subject: Security ID: S-1-5-21-1888849264-3803429180-4108621888-1001

Security	Audit Success	12545	23 08:27:32	Microsoft-Windows-Security-Auditing	Account Name: Liem Account Domain: LTRANPHD Logon ID: 0x561407 Logon Type: 7 This event is generated when a logon session is destroyed. It may be positively correlated with a logon event using the Logon ID value. Logon IDs are only unique between reboots on the same computer.
Security	Audit Success	12545	2015-04-23 08:27:32	Microsoft-Windows-Security-Auditing	4634: An account was logged off. Subject: Security ID: S-1-5-21-1888849264-3803429180-4108621888-1001 Account Name: Liem Account Domain: LTRANPHD Logon ID: 0x5613ec Logon Type: 7 This event is generated when a logon session is destroyed. It may be positively correlated with a logon event using the Logon ID value. Logon IDs are only unique between reboots on the same computer.
Security	Audit Success	12548	2015-04-23 08:27:32	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-21-1888849264-3803429180-4108621888-1001 Account Name: Liem Account Domain: LTRANPHD Logon ID: 0x5613ec Privileges: SeSecurityPrivilege SeTakeOwnershipPrivilege SeLoadDriverPrivilege SeBackupPrivilege SeRestorePrivilege SeDebugPrivilege SeSystemEnvironmentPrivilege SeImpersonatePrivilege
Security	Audit Success	12288	2015-04-23 08:53:11	Microsoft-Windows-Security-Auditing	4608: Windows is starting up. This event is logged when LSASS.EXE starts and the auditing subsystem is initialized.
Security	Audit Success	12544	2015-04-23 08:53:11	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-0-0 Account Name: - Account Domain: - Logon ID: 0x0 Logon Type: 0 Impersonation Level: - New Logon: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Logon ID: 0x3e7 Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x4 Process Name: Network Information: Workstation Name: - Source Network Address: - Source Port: - Detailed Authentication Information: Logon Process: - Authentication Package: - Transited Services: - Package Name (NTLM only): - Key Length: 0 This event is generated when a logon session is created. It is generated on the computer that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service such as the Server service, or a local process such as Winlogon.exe or Services.exe. The logon type field indicates the kind of logon that occurred. The most common types are 2 (interactive) and 3 (network). The New Logon fields indicate the account for whom the new logon was created, i.e. the account that was logged on. The network fields indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impersonation level field indicates the extent to which a process in the logon session can impersonate. The authentication information fields provide detailed information about this specific logon request. - Logon GUID is a unique identifier that can be used to correlate this event with a KDC event. - Transited services indicate which intermediate services have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indicates the length of the generated session key. This will be 0 if no session key was requested.
Security	Audit Success	12544	2015-04-23 08:53:11	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: LTRANPHD$ Account Domain: WORKGROUP Logon ID: 0x3e7 Logon Type: 5 Impersonation Level: %%1833 New Logon: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Logon ID: 0x3e7 Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x230 Process Name: C:\Windows\System32\services.exe Network Information: Workstation Name: Source Network Address: - Source Port: - Detailed Authentication Information: Logon Process: Advapi Authentication Package: Negotiate Transited Services: - Package Name (NTLM only): - Key Length: 0 This event is generated when a logon session is created. It is generated on the computer that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service such as the Server service, or a local process such as Winlogon.exe or Services.exe. The logon type field indicates the kind of logon that occurred. The most common types are 2 (interactive) and 3 (network). The New Logon fields indicate the account for whom the new logon was created, i.e. the account that was logged on. The network fields indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impersonation level field indicates the extent to which a process in the logon session can impersonate. The authentication information fields provide detailed information about this specific logon request. - Logon GUID is a unique identifier that can be used to correlate this event with a KDC event. - Transited services indicate which intermediate services have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indicates the length of the generated session key. This will be 0 if no session key was requested.
Security	Audit Success	12544	2015-04-23 08:53:11	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: LTRANPHD$ Account Domain: WORKGROUP Logon ID: 0x3e7 Logon Type: 5 Impersonation Level: %%1833 New Logon: Security ID: S-1-5-20 Account Name: NETWORK SERVICE Account Domain: NT AUTHORITY Logon ID: 0x3e4 Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x230 Process Name: C:\Windows\System32\services.exe Network Information: Workstation Name: Source Network Address: - Source Port: - Detailed Authentication Information: Logon Process: Advapi Authentication Package: Negotiate Transited Services: - Package Name (NTLM only): - Key Length: 0 This event is generated when a logon session is created. It is generated on the computer that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service such as the Server service, or a local process such as Winlogon.exe or Services.exe. The logon type field indicates the kind of logon that occurred. The most common types are 2 (interactive) and 3 (network). The New Logon fields indicate the account for whom the new logon was created, i.e. the account that was logged on. The network fields indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impersonation level field indicates the extent to which a process in the logon session can impersonate. The authentication information fields provide detailed information about this specific logon request.

					- Logon GUID is a unique identifier that can be used to correlate this event with a KDC event. - Transited services indicate which intermediate services have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indicates the length of the generated session key. This will be 0 if no session key was requested.
Security	Audit Success	12544	2015-04-23 08:53:11	Microsoft-Windows-Security-Auditing	4648: A logon was attempted using explicit credentials. Subject: Security ID: S-1-5-18 Account Name: LTRANPHD$ Account Domain: WORKGROUP Logon ID: 0x3e7 Logon GUID: {00000000-0000-0000-0000-000000000000} Account Whose Credentials Were Used: Account Name: DWM-1 Account Domain: Window Manager Logon GUID: {00000000-0000-0000-0000-000000000000} Target Server: Target Server Name: localhost Additional Information: localhost Process Information: Process ID: 0x208 Process Name: C:\Windows\System32\winlogon.exe Network Information: Network Address: - Port: - This event is generated when a process attempts to log on an account by explicitly specifying that account's credentials. This most commonly occurs in batch-type configurations such as scheduled tasks, or when using the RUNAS command.
Security	Audit Success	12544	2015-04-23 08:53:11	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: LTRANPHD$ Account Domain: WORKGROUP Logon ID: 0x3e7 Logon Type: 2 Impersonation Level: %%1833 New Logon: Security ID: S-1-5-90-1 Account Name: DWM-1 Account Domain: Window Manager Logon ID: 0xf54d Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x208 Process Name: C:\Windows\System32\winlogon.exe Network Information: Workstation Name: Source Network Address: - Source Port: - Detailed Authentication Information: Logon Process: Advapi Authentication Package: Negotiate Transited Services: - Package Name (NTLM only): - Key Length: 0 This event is generated when a logon session is created. It is generated on the computer that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service such as the Server service, or a local process such as Winlogon.exe or Services.exe. The logon type field indicates the kind of logon that occurred. The most common types are 2 (interactive) and 3 (network). The New Logon fields indicate the account for whom the new logon was created, i.e. the account that was logged on. The network fields indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impersonation level field indicates the extent to which a process in the logon session can impersonate. The authentication information fields provide detailed information about this specific logon request. - Logon GUID is a unique identifier that can be used to correlate this event with a KDC event. - Transited services indicate which intermediate services have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indicates the length of the generated session key. This will be 0 if no session key was requested.
Security	Audit Success	12544	2015-04-23 08:53:11	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: LTRANPHD$ Account Domain: WORKGROUP Logon ID: 0x3e7 Logon Type: 2 Impersonation Level: %%1833 New Logon: Security ID: S-1-5-90-1 Account Name: DWM-1 Account Domain: Window Manager Logon ID: 0xf566 Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x208 Process Name: C:\Windows\System32\winlogon.exe Network Information: Workstation Name: Source Network Address: - Source Port: - Detailed Authentication Information: Logon Process: Advapi Authentication Package: Negotiate Transited Services: - Package Name (NTLM only): - Key Length: 0 This event is generated when a logon session is created. It is generated on the computer that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service such as the Server service, or a local process such as Winlogon.exe or Services.exe. The logon type field indicates the kind of logon that occurred. The most common types are 2 (interactive) and 3 (network). The New Logon fields indicate the account for whom the new logon was created, i.e. the account that was logged on. The network fields indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impersonation level field indicates the extent to which a process in the logon session can impersonate. The authentication information fields provide detailed information about this specific logon request. - Logon GUID is a unique identifier that can be used to correlate this event with a KDC event. - Transited services indicate which intermediate services have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indicates the length of the generated session key. This will be 0 if no session key was requested.
Security	Audit Success	12544	2015-04-23 08:53:11	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: LTRANPHD$ Account Domain: WORKGROUP Logon ID: 0x3e7 Logon Type: 5 Impersonation Level: %%1833 New Logon: Security ID: S-1-5-19 Account Name: LOCAL SERVICE Account Domain: NT AUTHORITY Logon ID: 0x3e5 Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x230 Process Name: C:\Windows\System32\services.exe Network Information: Workstation Name: Source Network Address: - Source Port: - Detailed Authentication Information: Logon Process: Advapi Authentication Package: Negotiate Transited Services: - Package Name (NTLM only): - Key Length: 0 This event is generated when a logon session is created. It is generated on the computer that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service such as the Server service, or a local process such as Winlogon.exe or Services.exe. The logon type field indicates the kind of logon that occurred. The most common types are 2 (interactive) and 3 (network). The New Logon fields indicate the account for whom the new logon was created, i.e. the account that was logged on. The network fields indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impersonation level field indicates the extent to which a process in the logon session can impersonate. The authentication information fields provide detailed information about this specific logon request. - Logon GUID is a unique identifier that can be used to correlate this event with a KDC event. - Transited services indicate which intermediate services have participated in this logon request. - Package name indicates

					which sub-protocol was used among the NTLM protocols. - Key length indicates the length of the generated session key. This will be 0 if no session key was requested.
Security	Audit Success	12544	2015-04-23 08:53:11	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: LTRANPHD$ Account Domain: WORKGROUP Logon ID: 0x3e7 Logon Type: 5 Impersonation Level: %%1833 New Logon: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Logon ID: 0x3e7 Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x230 Process Name: C:\Windows\System32\services.exe Network Information: Workstation Name: Source Network Address: - Source Port: - Detailed Authentication Information: Logon Process: Advapi Authentication Package: Negotiate Transited Services: - Package Name (NTLM only): - Key Length: 0 This event is generated when a logon session is created. It is generated on the computer that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service such as the Server service, or a local process such as Winlogon.exe or Services.exe. The logon type field indicates the kind of logon that occurred. The most common types are 2 (interactive) and 3 (network). The New Logon fields indicate the account for whom the new logon was created, i.e. the account that was logged on. The network fields indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impersonation level field indicates the extent to which a process in the logon session can impersonate. The authentication information fields provide detailed information about this specific logon request. - Logon GUID is a unique identifier that can be used to correlate this event with a KDC event. - Transited services indicate which intermediate services have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indicates the length of the generated session key. This will be 0 if no session key was requested.
Security	Audit Success	12544	2015-04-23 08:53:11	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: LTRANPHD$ Account Domain: WORKGROUP Logon ID: 0x3e7 Logon Type: 5 Impersonation Level: %%1833 New Logon: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Logon ID: 0x3e7 Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x230 Process Name: C:\Windows\System32\services.exe Network Information: Workstation Name: Source Network Address: - Source Port: - Detailed Authentication Information: Logon Process: Advapi Authentication Package: Negotiate Transited Services: - Package Name (NTLM only): - Key Length: 0 This event is generated when a logon session is created. It is generated on the computer that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service such as the Server service, or a local process such as Winlogon.exe or Services.exe. The logon type field indicates the kind of logon that occurred. The most common types are 2 (interactive) and 3 (network). The New Logon fields indicate the account for whom the new logon was created, i.e. the account that was logged on. The network fields indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impersonation level field indicates the extent to which a process in the logon session can impersonate. The authentication information fields provide detailed information about this specific logon request. - Logon GUID is a unique identifier that can be used to correlate this event with a KDC event. - Transited services indicate which intermediate services have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indicates the length of the generated session key. This will be 0 if no session key was requested.
Security	Audit Success	12548	2015-04-23 08:53:11	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Logon ID: 0x3e7 Privileges: SeAssignPrimaryTokenPrivilege SeTcbPrivilege SeSecurityPrivilege SeTakeOwnershipPrivilege SeLoadDriverPrivilege SeBackupPrivilege SeRestorePrivilege SeDebugPrivilege SeAuditPrivilege SeSystemEnvironmentPrivilege SeImpersonatePrivilege
Security	Audit Success	12548	2015-04-23 08:53:11	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-20 Account Name: NETWORK SERVICE Account Domain: NT AUTHORITY Logon ID: 0x3e4 Privileges: SeAssignPrimaryTokenPrivilege SeAuditPrivilege SeImpersonatePrivilege
Security	Audit Success	12548	2015-04-23 08:53:11	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-90-1 Account Name: DWM-1 Account Domain: Window Manager Logon ID: 0xf54d Privileges: SeAssignPrimaryTokenPrivilege SeAuditPrivilege SeImpersonatePrivilege
Security	Audit Success	12548	2015-04-23 08:53:11	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-90-1 Account Name: DWM-1 Account Domain: Window Manager Logon ID: 0xf566 Privileges: SeAssignPrimaryTokenPrivilege SeAuditPrivilege
Security	Audit Success	12548	2015-04-23 08:53:11	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-19 Account Name: LOCAL SERVICE Account Domain: NT AUTHORITY Logon ID: 0x3e5 Privileges: SeAssignPrimaryTokenPrivilege SeAuditPrivilege SeImpersonatePrivilege
Security	Audit Success	12548	2015-04-23 08:53:11	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Logon ID: 0x3e7 Privileges: SeAssignPrimaryTokenPrivilege SeTcbPrivilege SeSecurityPrivilege SeTakeOwnershipPrivilege SeLoadDriverPrivilege SeBackupPrivilege SeRestorePrivilege SeDebugPrivilege SeAuditPrivilege SeSystemEnvironmentPrivilege SeImpersonatePrivilege
Security	Audit Success	12548	2015-04-23 08:53:11	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Logon ID: 0x3e7 Privileges: SeAssignPrimaryTokenPrivilege SeTcbPrivilege SeSecurityPrivilege SeTakeOwnershipPrivilege SeLoadDriverPrivilege SeBackupPrivilege SeRestorePrivilege SeDebugPrivilege SeAuditPrivilege SeSystemEnvironmentPrivilege SeImpersonatePrivilege
	Audit		2015-04-	Microsoft-Windows-Security-	

Security	Success	13568	23 08:53:11	Auditing	4902: The Per-user audit policy table was created. Number of Elements: 0 Policy ID: 0x9d28
Security	Audit Success	12292	2015-04- 23 08:53:12	Microsoft-Windows-Security- Auditing	5033: The Windows Firewall Driver started successfully.
Security	Audit Success	12292	2015-04- 23 08:53:12	Microsoft-Windows-Security- Auditing	5024: The Windows Firewall service started successfully.
Security	Audit Success	12544	2015-04- 23 08:53:12	Microsoft-Windows-Security- Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: LTRANPHD$ Account Domain: WORKGROUP Logon ID: 0x3e7 Logon Type: 5 Impersonation Level: %%1833 New Logon: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Logon ID: 0x3e7 Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x230 Process Name: C:\Windows\System32\services.exe Network Information: Workstation Name: Source Network Address: - Source Port: - Detailed Authentication Information: Logon Process: Advapi Authentication Package: Negotiate Transited Services: - Package Name (NTLM only): - Key Length: 0 This event is generated when a logon session is created. It is generated on the computer that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service such as the Server service, or a local process such as Winlogon.exe or Services.exe. The logon type field indicates the kind of logon that occurred. The most common types are 2 (interactive) and 3 (network). The New Logon fields indicate the account for whom the new logon was created, i.e. the account that was logged on. The network fields indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impersonation level field indicates the extent to which a process in the logon session can impersonate. The authentication information fields provide detailed information about this specific logon request. - Logon GUID is a unique identifier that can be used to correlate this event with a KDC event. - Transited services indicate which intermediate services have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indicates the length of the generated session key. This will be 0 if no session key was requested.
Security	Audit Success	12544	2015-04- 23 08:53:12	Microsoft-Windows-Security- Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: LTRANPHD$ Account Domain: WORKGROUP Logon ID: 0x3e7 Logon Type: 5 Impersonation Level: %%1833 New Logon: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Logon ID: 0x3e7 Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x230 Process Name: C:\Windows\System32\services.exe Network Information: Workstation Name: Source Network Address: - Source Port: - Detailed Authentication Information: Logon Process: Advapi Authentication Package: Negotiate Transited Services: - Package Name (NTLM only): - Key Length: 0 This event is generated when a logon session is created. It is generated on the computer that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service such as the Server service, or a local process such as Winlogon.exe or Services.exe. The logon type field indicates the kind of logon that occurred. The most common types are 2 (interactive) and 3 (network). The New Logon fields indicate the account for whom the new logon was created, i.e. the account that was logged on. The network fields indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impersonation level field indicates the extent to which a process in the logon session can impersonate. The authentication information fields provide detailed information about this specific logon request. - Logon GUID is a unique identifier that can be used to correlate this event with a KDC event. - Transited services indicate which intermediate services have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indicates the length of the generated session key. This will be 0 if no session key was requested.
Security	Audit Success	12544	2015-04- 23 08:53:12	Microsoft-Windows-Security- Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: LTRANPHD$ Account Domain: WORKGROUP Logon ID: 0x3e7 Logon Type: 5 Impersonation Level: %%1833 New Logon: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Logon ID: 0x3e7 Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x230 Process Name: C:\Windows\System32\services.exe Network Information: Workstation Name: Source Network Address: - Source Port: - Detailed Authentication Information: Logon Process: Advapi Authentication Package: Negotiate Transited Services: - Package Name (NTLM only): - Key Length: 0 This event is generated when a logon session is created. It is generated on the computer that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service such as the Server service, or a local process such as Winlogon.exe or Services.exe. The logon type field indicates the kind of logon that occurred. The most common types are 2 (interactive) and 3 (network). The New Logon fields indicate the account for whom the new logon was created, i.e. the account that was logged on. The network fields indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impersonation level field indicates the extent to which a process in the logon session can impersonate. The authentication information fields provide detailed information about this specific logon request. - Logon GUID is a unique identifier that can be used to correlate this event with a KDC event. - Transited services indicate which intermediate services have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indicates the length of the generated session key. This will be 0 if no session key was requested.
					4624: An account was successfully logged on. Subject: Security ID: S-1-0-0 Account Name: - Account Domain:

Security	Audit Success	12544	2015-04-23 08:53:12	Microsoft-Windows-Security-Auditing	- Logon ID: 0x0 Logon Type: 3 Impersonation Level: %%1833 New Logon: Security ID: S-1-5-7 Account Name: ANONYMOUS LOGON Account Domain: NT AUTHORITY Logon ID: 0x19580 Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x0 Process Name: - Network Information: Workstation Name: Source Network Address: - Source Port: - Detailed Authentication Information: Logon Process: NtLmSsp Authentication Package: NTLM Transited Services: - Package Name (NTLM only): NTLM V1 Key Length: 0 This event is generated when a logon session is created. It is generated on the computer that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service such as the Server service, or a local process such as Winlogon.exe or Services.exe. The logon type field indicates the kind of logon that occurred. The most common types are 2 (interactive) and 3 (network). The New Logon fields indicate the account for whom the new logon was created, i.e. the account that was logged on. The network fields indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impersonation level field indicates the extent to which a process in the logon session can impersonate. The authentication information fields provide detailed information about this specific logon request. - Logon GUID is a unique identifier that can be used to correlate this event with a KDC event. - Transited services indicate which intermediate services have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indicates the length of the generated session key. This will be 0 if no session key was requested.
Security	Audit Success	12548	2015-04-23 08:53:12	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Logon ID: 0x3e7 Privileges: SeAssignPrimaryTokenPrivilege SeTcbPrivilege SeSecurityPrivilege SeTakeOwnershipPrivilege SeLoadDriverPrivilege SeBackupPrivilege SeRestorePrivilege SeDebugPrivilege SeAuditPrivilege SeSystemEnvironmentPrivilege SeImpersonatePrivilege
Security	Audit Success	12548	2015-04-23 08:53:12	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Logon ID: 0x3e7 Privileges: SeAssignPrimaryTokenPrivilege SeTcbPrivilege SeSecurityPrivilege SeTakeOwnershipPrivilege SeLoadDriverPrivilege SeBackupPrivilege SeRestorePrivilege SeDebugPrivilege SeAuditPrivilege SeSystemEnvironmentPrivilege SeImpersonatePrivilege
Security	Audit Success	12548	2015-04-23 08:53:12	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Logon ID: 0x3e7 Privileges: SeAssignPrimaryTokenPrivilege SeTcbPrivilege SeSecurityPrivilege SeTakeOwnershipPrivilege SeLoadDriverPrivilege SeBackupPrivilege SeRestorePrivilege SeDebugPrivilege SeAuditPrivilege SeSystemEnvironmentPrivilege SeImpersonatePrivilege
Security	Audit Success	12544	2015-04-23 08:53:23	Microsoft-Windows-Security-Auditing	4648: A logon was attempted using explicit credentials. Subject: Security ID: S-1-5-18 Account Name: LTRANPHD$ Account Domain: WORKGROUP Logon ID: 0x3e7 Logon GUID: {00000000-0000-0000-0000-000000000000} Account Whose Credentials Were Used: Account Name: Liem Account Domain: LTRANPHD Logon GUID: {00000000-0000-0000-0000-000000000000} Target Server: Target Server Name: localhost Additional Information: localhost Process Information: Process ID: 0x208 Process Name: C:\Windows\System32\winlogon.exe Network Information: Network Address: 127.0.0.1 Port: 0 This event is generated when a process attempts to log on an account by explicitly specifying that account's credentials. This most commonly occurs in batch-type configurations such as scheduled tasks, or when using the RUNAS command.
Security	Audit Success	12544	2015-04-23 08:53:23	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: LTRANPHD$ Account Domain: WORKGROUP Logon ID: 0x3e7 Logon Type: 2 Impersonation Level: %%1833 New Logon: Security ID: S-1-5-21-1888849264-3803429180-4108621888-1001 Account Name: Liem Account Domain: LTRANPHD Logon ID: 0x22958 Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x208 Process Name: C:\Windows\System32\winlogon.exe Network Information: Workstation Name: LTRANPHD Source Network Address: 127.0.0.1 Source Port: 0 Detailed Authentication Information: Logon Process: User32 Authentication Package: Negotiate Transited Services: - Package Name (NTLM only): - Key Length: 0 This event is generated when a logon session is created. It is generated on the computer that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service such as the Server service, or a local process such as Winlogon.exe or Services.exe. The logon type field indicates the kind of logon that occurred. The most common types are 2 (interactive) and 3 (network). The New Logon fields indicate the account for whom the new logon was created, i.e. the account that was logged on. The network fields indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impersonation level field indicates the extent to which a process in the logon session can impersonate. The authentication information fields provide detailed information about this specific logon request. - Logon GUID is a unique identifier that can be used to correlate this event with a KDC event. - Transited services indicate which intermediate services have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indicates the length of the generated session key. This will be 0 if no session key was requested.
	Audit		2015-04-	Microsoft-Windows-Security-	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: LTRANPHD$ Account Domain: WORKGROUP Logon ID: 0x3e7 Logon Type: 2 Impersonation Level: %%1833 New Logon: Security ID: S-1-5-21-1888849264-3803429180-4108621888-1001 Account Name: Liem Account Domain: LTRANPHD Logon ID: 0x229b1 Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x208 Process Name: C:\Windows\System32\winlogon.exe Network Information: Workstation Name: LTRANPHD Source Network Address: 127.0.0.1 Source Port: 0 Detailed Authentication Information: Logon Process: User32 Authentication Package: Negotiate Transited Services: - Package Name (NTLM only): - Key Length: 0 This event is generated when a logon session is created. It is generated on the computer that was accessed. The subject fields indicate the account on the local system which requested the logon. This is

Security	Success	12544	23 08:53:23	Auditing	most commonly a service such as the Server service, or a local process such as Winlogon.exe or Services.exe. The logon type field indicates the kind of logon that occurred. The most common types are 2 (interactive) and 3 (network). The New Logon fields indicate the account for whom the new logon was created, i.e. the account that was logged on. The network fields indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impersonation level field indicates the extent to which a process in the logon session can impersonate. The authentication information fields provide detailed information about this specific logon request. - Logon GUID is a unique identifier that can be used to correlate this event with a KDC event. - Transited services indicate which intermediate services have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indicates the length of the generated session key. This will be 0 if no session key was requested.
Security	Audit Success	12548	2015-04-23 08:53:23	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-21-1888849264-3803429180-4108621888-1001 Account Name: Liem Account Domain: LTRANPHD Logon ID: 0x22958 Privileges: SeSecurityPrivilege SeTakeOwnershipPrivilege SeLoadDriverPrivilege SeBackupPrivilege SeRestorePrivilege SeDebugPrivilege SeSystemEnvironmentPrivilege SeImpersonatePrivilege
Security	Audit Success	12544	2015-04-23 08:53:24	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: LTRANPHD$ Account Domain: WORKGROUP Logon ID: 0x3e7 Logon Type: 5 Impersonation Level: %%1833 New Logon: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Logon ID: 0x3e7 Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x230 Process Name: C:\Windows\System32\services.exe Network Information: Workstation Name: Source Network Address: - Source Port: - Detailed Authentication Information: Logon Process: Advapi Authentication Package: Negotiate Transited Services: - Package Name (NTLM only): - Key Length: 0 This event is generated when a logon session is created. It is generated on the computer that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service such as the Server service, or a local process such as Winlogon.exe or Services.exe. The logon type field indicates the kind of logon that occurred. The most common types are 2 (interactive) and 3 (network). The New Logon fields indicate the account for whom the new logon was created, i.e. the account that was logged on. The network fields indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impersonation level field indicates the extent to which a process in the logon session can impersonate. The authentication information fields provide detailed information about this specific logon request. - Logon GUID is a unique identifier that can be used to correlate this event with a KDC event. - Transited services indicate which intermediate services have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indicates the length of the generated session key. This will be 0 if no session key was requested.
Security	Audit Success	12548	2015-04-23 08:53:24	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Logon ID: 0x3e7 Privileges: SeAssignPrimaryTokenPrivilege SeTcbPrivilege SeSecurityPrivilege SeTakeOwnershipPrivilege SeLoadDriverPrivilege SeBackupPrivilege SeRestorePrivilege SeDebugPrivilege SeAuditPrivilege SeSystemEnvironmentPrivilege SeImpersonatePrivilege
Security	Audit Success	12544	2015-04-23 08:53:25	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: LTRANPHD$ Account Domain: WORKGROUP Logon ID: 0x3e7 Logon Type: 5 Impersonation Level: %%1833 New Logon: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Logon ID: 0x3e7 Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x230 Process Name: C:\Windows\System32\services.exe Network Information: Workstation Name: Source Network Address: - Source Port: - Detailed Authentication Information: Logon Process: Advapi Authentication Package: Negotiate Transited Services: - Package Name (NTLM only): - Key Length: 0 This event is generated when a logon session is created. It is generated on the computer that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service such as the Server service, or a local process such as Winlogon.exe or Services.exe. The logon type field indicates the kind of logon that occurred. The most common types are 2 (interactive) and 3 (network). The New Logon fields indicate the account for whom the new logon was created, i.e. the account that was logged on. The network fields indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impersonation level field indicates the extent to which a process in the logon session can impersonate. The authentication information fields provide detailed information about this specific logon request. - Logon GUID is a unique identifier that can be used to correlate this event with a KDC event. - Transited services indicate which intermediate services have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indicates the length of the generated session key. This will be 0 if no session key was requested.
Security	Audit Success	12548	2015-04-23 08:53:25	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Logon ID: 0x3e7 Privileges: SeAssignPrimaryTokenPrivilege SeTcbPrivilege SeSecurityPrivilege SeTakeOwnershipPrivilege SeLoadDriverPrivilege SeBackupPrivilege SeRestorePrivilege SeDebugPrivilege SeAuditPrivilege SeSystemEnvironmentPrivilege SeImpersonatePrivilege
Security	Audit Success	13824	2015-04-23 08:53:25	Microsoft-Windows-Security-Auditing	4797: An attempt was made to query the existence of a blank password for an account. Subject: Security ID: S-1-5-19 Account Name: LOCAL SERVICE Account Domain: NT AUTHORITY Logon ID: 0x3e5 Additional Information: Caller Workstation: LTRANPHD Target Account Name: Administrator Target Account Domain: LTRANPHD
Security	Audit	13824	2015-04-23	Microsoft-Windows-Security-	4797: An attempt was made to query the existence of a blank password for an account. Subject: Security ID: S-1-5-19 Account Name: LOCAL SERVICE Account Domain: NT AUTHORITY Logon ID: 0x3e5 Additional

	Success		08:53:25	Auditing	Information: Caller Workstation: LTRANPHD Target Account Name: Guest Target Account Domain: LTRANPHD
Security	Audit Success	13824	2015-04-23 08:53:25	Microsoft-Windows-Security-Auditing	4797: An attempt was made to query the existence of a blank password for an account. Subject: Security ID: S-1-5-19 Account Name: LOCAL SERVICE Account Domain: NT AUTHORITY Logon ID: 0x3e5 Additional Information: Caller Workstation: LTRANPHD Target Account Name: Liem Target Account Domain: LTRANPHD
Security	Audit Success	13824	2015-04-23 08:53:25	Microsoft-Windows-Security-Auditing	4797: An attempt was made to query the existence of a blank password for an account. Subject: Security ID: S-1-5-19 Account Name: LOCAL SERVICE Account Domain: NT AUTHORITY Logon ID: 0x3e5 Additional Information: Caller Workstation: LTRANPHD Target Account Name: Liem Target Account Domain: LTRANPHD
Security	Audit Success	13824	2015-04-23 08:53:25	Microsoft-Windows-Security-Auditing	4797: An attempt was made to query the existence of a blank password for an account. Subject: Security ID: S-1-5-19 Account Name: LOCAL SERVICE Account Domain: NT AUTHORITY Logon ID: 0x3e5 Additional Information: Caller Workstation: LTRANPHD Target Account Name: Administrator Target Account Domain: LTRANPHD
Security	Audit Success	13824	2015-04-23 08:53:25	Microsoft-Windows-Security-Auditing	4797: An attempt was made to query the existence of a blank password for an account. Subject: Security ID: S-1-5-19 Account Name: LOCAL SERVICE Account Domain: NT AUTHORITY Logon ID: 0x3e5 Additional Information: Caller Workstation: LTRANPHD Target Account Name: Guest Target Account Domain: LTRANPHD
Security	Audit Success	13824	2015-04-23 08:53:25	Microsoft-Windows-Security-Auditing	4797: An attempt was made to query the existence of a blank password for an account. Subject: Security ID: S-1-5-19 Account Name: LOCAL SERVICE Account Domain: NT AUTHORITY Logon ID: 0x3e5 Additional Information: Caller Workstation: LTRANPHD Target Account Name: Liem Target Account Domain: LTRANPHD
Security	Audit Success	13824	2015-04-23 08:53:25	Microsoft-Windows-Security-Auditing	4797: An attempt was made to query the existence of a blank password for an account. Subject: Security ID: S-1-5-19 Account Name: LOCAL SERVICE Account Domain: NT AUTHORITY Logon ID: 0x3e5 Additional Information: Caller Workstation: LTRANPHD Target Account Name: Administrator Target Account Domain: LTRANPHD
Security	Audit Success	13824	2015-04-23 08:53:25	Microsoft-Windows-Security-Auditing	4797: An attempt was made to query the existence of a blank password for an account. Subject: Security ID: S-1-5-19 Account Name: LOCAL SERVICE Account Domain: NT AUTHORITY Logon ID: 0x3e5 Additional Information: Caller Workstation: LTRANPHD Target Account Name: Liem Target Account Domain: LTRANPHD
Security	Audit Success	13824	2015-04-23 08:53:25	Microsoft-Windows-Security-Auditing	4797: An attempt was made to query the existence of a blank password for an account. Subject: Security ID: S-1-5-19 Account Name: LOCAL SERVICE Account Domain: NT AUTHORITY Logon ID: 0x3e5 Additional Information: Caller Workstation: LTRANPHD Target Account Name: Administrator Target Account Domain: LTRANPHD
Security	Audit Success	13824	2015-04-23 08:53:25	Microsoft-Windows-Security-Auditing	4797: An attempt was made to query the existence of a blank password for an account. Subject: Security ID: S-1-5-19 Account Name: LOCAL SERVICE Account Domain: NT AUTHORITY Logon ID: 0x3e5 Additional Information: Caller Workstation: LTRANPHD Target Account Name: Guest Target Account Domain: LTRANPHD
Security	Audit Success	13824	2015-04-23 08:53:25	Microsoft-Windows-Security-Auditing	4797: An attempt was made to query the existence of a blank password for an account. Subject: Security ID: S-1-5-19 Account Name: LOCAL SERVICE Account Domain: NT AUTHORITY Logon ID: 0x3e5 Additional Information: Caller Workstation: LTRANPHD Target Account Name: Liem Target Account Domain: LTRANPHD
Security	Audit Success	13824	2015-04-23 08:53:25	Microsoft-Windows-Security-Auditing	4797: An attempt was made to query the existence of a blank password for an account. Subject: Security ID: S-1-5-19 Account Name: LOCAL SERVICE Account Domain: NT AUTHORITY Logon ID: 0x3e5 Additional Information: Caller Workstation: LTRANPHD Target Account Name: Liem Target Account Domain: LTRANPHD
Security	Audit Success	13824	2015-04-23 08:53:25	Microsoft-Windows-Security-Auditing	4797: An attempt was made to query the existence of a blank password for an account. Subject: Security ID: S-1-5-19 Account Name: LOCAL SERVICE Account Domain: NT AUTHORITY Logon ID: 0x3e5 Additional Information: Caller Workstation: LTRANPHD Target Account Name: Administrator Target Account Domain: LTRANPHD
Security	Audit Success	13824	2015-04-23 08:53:25	Microsoft-Windows-Security-Auditing	4797: An attempt was made to query the existence of a blank password for an account. Subject: Security ID: S-1-5-19 Account Name: LOCAL SERVICE Account Domain: NT AUTHORITY Logon ID: 0x3e5 Additional Information: Caller Workstation: LTRANPHD Target Account Name: Guest Target Account Domain: LTRANPHD
Security	Audit Success	13824	2015-04-23 08:53:25	Microsoft-Windows-Security-Auditing	4797: An attempt was made to query the existence of a blank password for an account. Subject: Security ID: S-1-5-19 Account Name: LOCAL SERVICE Account Domain: NT AUTHORITY Logon ID: 0x3e5 Additional Information: Caller Workstation: LTRANPHD Target Account Name: Liem Target Account Domain: LTRANPHD
Security	Audit Success	13824	2015-04-23 08:53:25	Microsoft-Windows-Security-Auditing	4797: An attempt was made to query the existence of a blank password for an account. Subject: Security ID: S-1-5-19 Account Name: LOCAL SERVICE Account Domain: NT AUTHORITY Logon ID: 0x3e5 Additional Information: Caller Workstation: LTRANPHD Target Account Name: Liem Target Account Domain: LTRANPHD
Security	Audit Success	13824	2015-04-23 08:53:26	Microsoft-Windows-Security-Auditing	4797: An attempt was made to query the existence of a blank password for an account. Subject: Security ID: S-1-5-21-1888849264-3803429180-4108621888-1001 Account Name: Liem Account Domain: LTRANPHD Logon ID: 0x229b1 Additional Information: Caller Workstation: LTRANPHD Target Account Name: Administrator Target Account Domain: LTRANPHD
Security	Audit Success	13824	2015-04-23 08:53:26	Microsoft-Windows-Security-Auditing	4797: An attempt was made to query the existence of a blank password for an account. Subject: Security ID: S-1-5-21-1888849264-3803429180-4108621888-1001 Account Name: Liem Account Domain: LTRANPHD Logon ID: 0x229b1 Additional Information: Caller Workstation: LTRANPHD Target Account Name: Guest Target Account Domain: LTRANPHD
Security	Audit Success	13824	2015-04-23 08:53:26	Microsoft-Windows-Security-Auditing	4797: An attempt was made to query the existence of a blank password for an account. Subject: Security ID: S-1-5-21-1888849264-3803429180-4108621888-1001 Account Name: Liem Account Domain: LTRANPHD Logon ID: 0x229b1 Additional Information: Caller Workstation: LTRANPHD Target Account Name: Administrator Target Account Domain: LTRANPHD

Security	Audit Success	13824	2015-04-23 08:53:26	Microsoft-Windows-Security-Auditing	4797: An attempt was made to query the existence of a blank password for an account. Subject: Security ID: S-1-5-21-1888849264-3803429180-4108621888-1001 Account Name: Liem Account Domain: LTRANPHD Logon ID: 0x229b1 Additional Information: Caller Workstation: LTRANPHD Target Account Name: Guest Target Account Domain: LTRANPHD
Security	Audit Success	12544	2015-04-23 08:53:55	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: LTRANPHD$ Account Domain: WORKGROUP Logon ID: 0x3e7 Logon Type: 5 Impersonation Level: %%1833 New Logon: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Logon ID: 0x3e7 Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x230 Process Name: C:\Windows\System32\services.exe Network Information: Workstation Name: Source Network Address: - Source Port: - Detailed Authentication Information: Logon Process: Advapi Authentication Package: Negotiate Transited Services: - Package Name (NTLM only): - Key Length: 0 This event is generated when a logon session is created. It is generated on the computer that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service such as the Server service, or a local process such as Winlogon.exe or Services.exe. The logon type field indicates the kind of logon that occurred. The most common types are 2 (interactive) and 3 (network). The New Logon fields indicate the account for whom the new logon was created, i.e. the account that was logged on. The network fields indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impersonation level field indicates the extent to which a process in the logon session can impersonate. The authentication information fields provide detailed information about this specific logon request. - Logon GUID is a unique identifier that can be used to correlate this event with a KDC event. - Transited services indicate which intermediate services have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indicates the length of the generated session key. This will be 0 if no session key was requested.
Security	Audit Success	12548	2015-04-23 08:53:55	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Logon ID: 0x3e7 Privileges: SeAssignPrimaryTokenPrivilege SeTcbPrivilege SeSecurityPrivilege SeTakeOwnershipPrivilege SeLoadDriverPrivilege SeBackupPrivilege SeRestorePrivilege SeDebugPrivilege SeAuditPrivilege SeSystemEnvironmentPrivilege SeImpersonatePrivilege
Security	Audit Success	12544	2015-04-23 08:53:57	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: LTRANPHD$ Account Domain: WORKGROUP Logon ID: 0x3e7 Logon Type: 5 Impersonation Level: %%1833 New Logon: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Logon ID: 0x3e7 Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x230 Process Name: C:\Windows\System32\services.exe Network Information: Workstation Name: Source Network Address: - Source Port: - Detailed Authentication Information: Logon Process: Advapi Authentication Package: Negotiate Transited Services: - Package Name (NTLM only): - Key Length: 0 This event is generated when a logon session is created. It is generated on the computer that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service such as the Server service, or a local process such as Winlogon.exe or Services.exe. The logon type field indicates the kind of logon that occurred. The most common types are 2 (interactive) and 3 (network). The New Logon fields indicate the account for whom the new logon was created, i.e. the account that was logged on. The network fields indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impersonation level field indicates the extent to which a process in the logon session can impersonate. The authentication information fields provide detailed information about this specific logon request. - Logon GUID is a unique identifier that can be used to correlate this event with a KDC event. - Transited services indicate which intermediate services have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indicates the length of the generated session key. This will be 0 if no session key was requested.
Security	Audit Success	12548	2015-04-23 08:53:57	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Logon ID: 0x3e7 Privileges: SeAssignPrimaryTokenPrivilege SeTcbPrivilege SeSecurityPrivilege SeTakeOwnershipPrivilege SeLoadDriverPrivilege SeBackupPrivilege SeRestorePrivilege SeDebugPrivilege SeAuditPrivilege SeSystemEnvironmentPrivilege SeImpersonatePrivilege
Security	Audit Success	12288	2015-04-23 12:32:58	Microsoft-Windows-Security-Auditing	4608: Windows is starting up. This event is logged when LSASS.EXE starts and the auditing subsystem is initialized.
Security	Audit Success	12544	2015-04-23 12:32:58	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-0-0 Account Name: - Account Domain: - Logon ID: 0x0 Logon Type: 0 Impersonation Level: - New Logon: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Logon ID: 0x3e7 Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x4 Process Name: Network Information: Workstation Name: - Source Network Address: - Source Port: - Detailed Authentication Information: Logon Process: - Authentication Package: - Transited Services: - Package Name (NTLM only): - Key Length: 0 This event is generated when a logon session is created. It is generated on the computer that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service such as the Server service, or a local process such as Winlogon.exe or Services.exe. The logon type field indicates the kind of logon that occurred. The most common types are 2 (interactive) and 3 (network). The New Logon fields indicate the account for whom the new logon was created, i.e. the account that was logged on. The network fields indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impersonation level field indicates the extent to which a

					process in the logon session can impersonate. The authentication information fields provide detailed information about this specific logon request. - Logon GUID is a unique identifier that can be used to correlate this event with a KDC event. - Transited services indicate which intermediate services have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indicates the length of the generated session key. This will be 0 if no session key was requested.
Security	Audit Success	12544	2015-04-23 12:32:58	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: LTRANPHD$ Account Domain: WORKGROUP Logon ID: 0x3e7 Logon Type: 5 Impersonation Level: %%1833 New Logon: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Logon ID: 0x3e7 Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x22c Process Name: C:\Windows\System32\services.exe Network Information: Workstation Name: Source Network Address: - Source Port: - Detailed Authentication Information: Logon Process: Advapi Authentication Package: Negotiate Transited Services: - Package Name (NTLM only): - Key Length: 0 This event is generated when a logon session is created. It is generated on the computer that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service such as the Server service, or a local process such as Winlogon.exe or Services.exe. The logon type field indicates the kind of logon that occurred. The most common types are 2 (interactive) and 3 (network). The New Logon fields indicate the account for whom the new logon was created, i.e. the account that was logged on. The network fields indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impersonation level field indicates the extent to which a process in the logon session can impersonate. The authentication information fields provide detailed information about this specific logon request. - Logon GUID is a unique identifier that can be used to correlate this event with a KDC event. - Transited services indicate which intermediate services have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indicates the length of the generated session key. This will be 0 if no session key was requested.
Security	Audit Success	12544	2015-04-23 12:32:58	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: LTRANPHD$ Account Domain: WORKGROUP Logon ID: 0x3e7 Logon Type: 5 Impersonation Level: %%1833 New Logon: Security ID: S-1-5-20 Account Name: NETWORK SERVICE Account Domain: NT AUTHORITY Logon ID: 0x3e4 Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x22c Process Name: C:\Windows\System32\services.exe Network Information: Workstation Name: Source Network Address: - Source Port: - Detailed Authentication Information: Logon Process: Advapi Authentication Package: Negotiate Transited Services: - Package Name (NTLM only): - Key Length: 0 This event is generated when a logon session is created. It is generated on the computer that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service such as the Server service, or a local process such as Winlogon.exe or Services.exe. The logon type field indicates the kind of logon that occurred. The most common types are 2 (interactive) and 3 (network). The New Logon fields indicate the account for whom the new logon was created, i.e. the account that was logged on. The network fields indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impersonation level field indicates the extent to which a process in the logon session can impersonate. The authentication information fields provide detailed information about this specific logon request. - Logon GUID is a unique identifier that can be used to correlate this event with a KDC event. - Transited services indicate which intermediate services have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indicates the length of the generated session key. This will be 0 if no session key was requested.
Security	Audit Success	12544	2015-04-23 12:32:58	Microsoft-Windows-Security-Auditing	4648: A logon was attempted using explicit credentials. Subject: Security ID: S-1-5-18 Account Name: LTRANPHD$ Account Domain: WORKGROUP Logon ID: 0x3e7 Logon GUID: {00000000-0000-0000-0000-000000000000} Account Whose Credentials Were Used: Account Name: DWM-1 Account Domain: Window Manager Logon GUID: {00000000-0000-0000-0000-000000000000} Target Server: Target Server Name: localhost Additional Information: localhost Process Information: Process ID: 0x204 Process Name: C:\Windows\System32\winlogon.exe Network Information: Network Address: - Port: - This event is generated when a process attempts to log on an account by explicitly specifying that account's credentials. This most commonly occurs in batch-type configurations such as scheduled tasks, or when using the RUNAS command.
Security	Audit Success	12544	2015-04-23 12:32:58	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: LTRANPHD$ Account Domain: WORKGROUP Logon ID: 0x3e7 Logon Type: 2 Impersonation Level: %%1833 New Logon: Security ID: S-1-5-90-1 Account Name: DWM-1 Account Domain: Window Manager Logon ID: 0xe387 Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x204 Process Name: C:\Windows\System32\winlogon.exe Network Information: Workstation Name: Source Network Address: - Source Port: - Detailed Authentication Information: Logon Process: Advapi Authentication Package: Negotiate Transited Services: - Package Name (NTLM only): - Key Length: 0 This event is generated when a logon session is created. It is generated on the computer that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service such as the Server service, or a local process such as Winlogon.exe or Services.exe. The logon type field indicates the kind of logon that occurred. The most common types are 2 (interactive) and 3 (network). The New Logon fields indicate the account for whom the new logon was created, i.e. the account that was logged on. The network fields indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impersonation level field indicates the extent to which a process in the logon session can impersonate. The authentication information fields provide detailed information about this specific logon request. - Logon GUID is a unique identifier that can be used to correlate this event with a KDC event. - Transited

					services indicate which intermediate services have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indicates the length of the generated session key. This will be 0 if no session key was requested.
Security	Audit Success	12544	2015-04-23 12:32:58	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: LTRANPHD$ Account Domain: WORKGROUP Logon ID: 0x3e7 Logon Type: 2 Impersonation Level: %%1833 New Logon: Security ID: S-1-5-90-1 Account Name: DWM-1 Account Domain: Window Manager Logon ID: 0xe39c Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x204 Process Name: C:\Windows\System32\winlogon.exe Network Information: Workstation Name: Source Network Address: - Source Port: - Detailed Authentication Information: Logon Process: Advapi Authentication Package: Negotiate Transited Services: - Package Name (NTLM only): - Key Length: 0 This event is generated when a logon session is created. It is generated on the computer that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service such as the Server service, or a local process such as Winlogon.exe or Services.exe. The logon type field indicates the kind of logon that occurred. The most common types are 2 (interactive) and 3 (network). The New Logon fields indicate the account for whom the new logon was created, i.e. the account that was logged on. The network fields indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impersonation level field indicates the extent to which a process in the logon session can impersonate. The authentication information fields provide detailed information about this specific logon request. - Logon GUID is a unique identifier that can be used to correlate this event with a KDC event. - Transited services indicate which intermediate services have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indicates the length of the generated session key. This will be 0 if no session key was requested.
Security	Audit Success	12544	2015-04-23 12:32:58	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: LTRANPHD$ Account Domain: WORKGROUP Logon ID: 0x3e7 Logon Type: 5 Impersonation Level: %%1833 New Logon: Security ID: S-1-5-19 Account Name: LOCAL SERVICE Account Domain: NT AUTHORITY Logon ID: 0x3e5 Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x22c Process Name: C:\Windows\System32\services.exe Network Information: Workstation Name: Source Network Address: - Source Port: - Detailed Authentication Information: Logon Process: Advapi Authentication Package: Negotiate Transited Services: - Package Name (NTLM only): - Key Length: 0 This event is generated when a logon session is created. It is generated on the computer that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service such as the Server service, or a local process such as Winlogon.exe or Services.exe. The logon type field indicates the kind of logon that occurred. The most common types are 2 (interactive) and 3 (network). The New Logon fields indicate the account for whom the new logon was created, i.e. the account that was logged on. The network fields indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impersonation level field indicates the extent to which a process in the logon session can impersonate. The authentication information fields provide detailed information about this specific logon request. - Logon GUID is a unique identifier that can be used to correlate this event with a KDC event. - Transited services indicate which intermediate services have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indicates the length of the generated session key. This will be 0 if no session key was requested.
Security	Audit Success	12544	2015-04-23 12:32:58	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: LTRANPHD$ Account Domain: WORKGROUP Logon ID: 0x3e7 Logon Type: 5 Impersonation Level: %%1833 New Logon: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Logon ID: 0x3e7 Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x22c Process Name: C:\Windows\System32\services.exe Network Information: Workstation Name: Source Network Address: - Source Port: - Detailed Authentication Information: Logon Process: Advapi Authentication Package: Negotiate Transited Services: - Package Name (NTLM only): - Key Length: 0 This event is generated when a logon session is created. It is generated on the computer that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service such as the Server service, or a local process such as Winlogon.exe or Services.exe. The logon type field indicates the kind of logon that occurred. The most common types are 2 (interactive) and 3 (network). The New Logon fields indicate the account for whom the new logon was created, i.e. the account that was logged on. The network fields indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impersonation level field indicates the extent to which a process in the logon session can impersonate. The authentication information fields provide detailed information about this specific logon request. - Logon GUID is a unique identifier that can be used to correlate this event with a KDC event. - Transited services indicate which intermediate services have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indicates the length of the generated session key. This will be 0 if no session key was requested.
					4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: LTRANPHD$ Account Domain: WORKGROUP Logon ID: 0x3e7 Logon Type: 5 Impersonation Level: %%1833 New Logon: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Logon ID: 0x3e7 Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x22c Process Name: C:\Windows\System32\services.exe Network Information: Workstation Name: Source Network Address: - Source Port: - Detailed Authentication Information: Logon Process: Advapi Authentication Package: Negotiate Transited Services: - Package Name (NTLM only): - Key Length: 0 This event is generated when a logon session is

Security	Audit Success	12544	2015-04-23 12:32:58	Microsoft-Windows-Security-Auditing	created. It is generated on the computer that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service such as the Server service, or a local process such as Winlogon.exe or Services.exe. The logon type field indicates the kind of logon that occurred. The most common types are 2 (interactive) and 3 (network). The New Logon fields indicate the account for whom the new logon was created, i.e. the account that was logged on. The network fields indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impersonation level field indicates the extent to which a process in the logon session can impersonate. The authentication information fields provide detailed information about this specific logon request. - Logon GUID is a unique identifier that can be used to correlate this event with a KDC event. - Transited services indicate which intermediate services have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indicates the length of the generated session key. This will be 0 if no session key was requested.
Security	Audit Success	12548	2015-04-23 12:32:58	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Logon ID: 0x3e7 Privileges: SeAssignPrimaryTokenPrivilege SeTcbPrivilege SeSecurityPrivilege SeTakeOwnershipPrivilege SeLoadDriverPrivilege SeBackupPrivilege SeRestorePrivilege SeDebugPrivilege SeAuditPrivilege SeSystemEnvironmentPrivilege SeImpersonatePrivilege
Security	Audit Success	12548	2015-04-23 12:32:58	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-20 Account Name: NETWORK SERVICE Account Domain: NT AUTHORITY Logon ID: 0x3e4 Privileges: SeAssignPrimaryTokenPrivilege SeAuditPrivilege SeImpersonatePrivilege
Security	Audit Success	12548	2015-04-23 12:32:58	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-90-1 Account Name: DWM-1 Account Domain: Window Manager Logon ID: 0xe387 Privileges: SeAssignPrimaryTokenPrivilege SeAuditPrivilege SeImpersonatePrivilege
Security	Audit Success	12548	2015-04-23 12:32:58	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-90-1 Account Name: DWM-1 Account Domain: Window Manager Logon ID: 0xe39c Privileges: SeAssignPrimaryTokenPrivilege SeAuditPrivilege
Security	Audit Success	12548	2015-04-23 12:32:58	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-19 Account Name: LOCAL SERVICE Account Domain: NT AUTHORITY Logon ID: 0x3e5 Privileges: SeAssignPrimaryTokenPrivilege SeAuditPrivilege SeImpersonatePrivilege
Security	Audit Success	12548	2015-04-23 12:32:58	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Logon ID: 0x3e7 Privileges: SeAssignPrimaryTokenPrivilege SeTcbPrivilege SeSecurityPrivilege SeTakeOwnershipPrivilege SeLoadDriverPrivilege SeBackupPrivilege SeRestorePrivilege SeDebugPrivilege SeAuditPrivilege SeSystemEnvironmentPrivilege SeImpersonatePrivilege
Security	Audit Success	12548	2015-04-23 12:32:58	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Logon ID: 0x3e7 Privileges: SeAssignPrimaryTokenPrivilege SeTcbPrivilege SeSecurityPrivilege SeTakeOwnershipPrivilege SeLoadDriverPrivilege SeBackupPrivilege SeRestorePrivilege SeDebugPrivilege SeAuditPrivilege SeSystemEnvironmentPrivilege SeImpersonatePrivilege
Security	Audit Success	13568	2015-04-23 12:32:58	Microsoft-Windows-Security-Auditing	4902: The Per-user audit policy table was created. Number of Elements: 0 Policy ID: 0x80ff
Security	Audit Success	12292	2015-04-23 12:32:59	Microsoft-Windows-Security-Auditing	5033: The Windows Firewall Driver started successfully.
Security	Audit Success	12544	2015-04-23 12:32:59	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: LTRANPHD$ Account Domain: WORKGROUP Logon ID: 0x3e7 Logon Type: 5 Impersonation Level: %%1833 New Logon: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Logon ID: 0x3e7 Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x22c Process Name: C:\Windows\System32\services.exe Network Information: Workstation Name: Source Network Address: - Source Port: - Detailed Authentication Information: Logon Process: Advapi Authentication Package: Negotiate Transited Services: - Package Name (NTLM only): - Key Length: 0 This event is generated when a logon session is created. It is generated on the computer that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service such as the Server service, or a local process such as Winlogon.exe or Services.exe. The logon type field indicates the kind of logon that occurred. The most common types are 2 (interactive) and 3 (network). The New Logon fields indicate the account for whom the new logon was created, i.e. the account that was logged on. The network fields indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impersonation level field indicates the extent to which a process in the logon session can impersonate. The authentication information fields provide detailed information about this specific logon request. - Logon GUID is a unique identifier that can be used to correlate this event with a KDC event. - Transited services indicate which intermediate services have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indicates the length of the generated session key. This will be 0 if no session key was requested.
					4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: LTRANPHD$ Account Domain: WORKGROUP Logon ID: 0x3e7 Logon Type: 5 Impersonation Level: %%1833 New Logon: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Logon ID: 0x3e7 Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x22c Process Name:

Security	Audit Success	12544	2015-04-23 12:32:59	Microsoft-Windows-Security-Auditing	C:\Windows\System32\services.exe Network Information: Workstation Name: Source Network Address: - Source Port: - Detailed Authentication Information: Logon Process: Advapi Authentication Package: Negotiate Transited Services: - Package Name (NTLM only): - Key Length: 0 This event is generated when a logon session is created. It is generated on the computer that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service such as the Server service, or a local process such as Winlogon.exe or Services.exe. The logon type field indicates the kind of logon that occurred. The most common types are 2 (interactive) and 3 (network). The New Logon fields indicate the account for whom the new logon was created, i.e. the account that was logged on. The network fields indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impersonation level field indicates the extent to which a process in the logon session can impersonate. The authentication information fields provide detailed information about this specific logon request. - Logon GUID is a unique identifier that can be used to correlate this event with a KDC event. - Transited services indicate which intermediate services have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indicates the length of the generated session key. This will be 0 if no session key was requested.
Security	Audit Success	12548	2015-04-23 12:32:59	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Logon ID: 0x3e7 Privileges: SeAssignPrimaryTokenPrivilege SeTcbPrivilege SeSecurityPrivilege SeTakeOwnershipPrivilege SeLoadDriverPrivilege SeBackupPrivilege SeRestorePrivilege SeDebugPrivilege SeAuditPrivilege SeSystemEnvironmentPrivilege SeImpersonatePrivilege
Security	Audit Success	12548	2015-04-23 12:32:59	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Logon ID: 0x3e7 Privileges: SeAssignPrimaryTokenPrivilege SeTcbPrivilege SeSecurityPrivilege SeTakeOwnershipPrivilege SeLoadDriverPrivilege SeBackupPrivilege SeRestorePrivilege SeDebugPrivilege SeAuditPrivilege SeSystemEnvironmentPrivilege SeImpersonatePrivilege
Security	Audit Success	12292	2015-04-23 12:33:01	Microsoft-Windows-Security-Auditing	5024: The Windows Firewall service started successfully.
Security	Audit Success	12544	2015-04-23 12:33:01	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: LTRANPHD$ Account Domain: WORKGROUP Logon ID: 0x3e7 Logon Type: 5 Impersonation Level: %%1833 New Logon: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Logon ID: 0x3e7 Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x22c Process Name: C:\Windows\System32\services.exe Network Information: Workstation Name: Source Network Address: - Source Port: - Detailed Authentication Information: Logon Process: Advapi Authentication Package: Negotiate Transited Services: - Package Name (NTLM only): - Key Length: 0 This event is generated when a logon session is created. It is generated on the computer that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service such as the Server service, or a local process such as Winlogon.exe or Services.exe. The logon type field indicates the kind of logon that occurred. The most common types are 2 (interactive) and 3 (network). The New Logon fields indicate the account for whom the new logon was created, i.e. the account that was logged on. The network fields indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impersonation level field indicates the extent to which a process in the logon session can impersonate. The authentication information fields provide detailed information about this specific logon request. - Logon GUID is a unique identifier that can be used to correlate this event with a KDC event. - Transited services indicate which intermediate services have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indicates the length of the generated session key. This will be 0 if no session key was requested.
Security	Audit Success	12544	2015-04-23 12:33:01	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-0-0 Account Name: - Account Domain: - Logon ID: 0x0 Logon Type: 3 Impersonation Level: %%1833 New Logon: Security ID: S-1-5-7 Account Name: ANONYMOUS LOGON Account Domain: NT AUTHORITY Logon ID: 0x18dfb Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x0 Process Name: - Network Information: Workstation Name: Source Network Address: - Source Port: - Detailed Authentication Information: Logon Process: NtLmSsp Authentication Package: NTLM Transited Services: - Package Name (NTLM only): NTLM V1 Key Length: 0 This event is generated when a logon session is created. It is generated on the computer that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service such as the Server service, or a local process such as Winlogon.exe or Services.exe. The logon type field indicates the kind of logon that occurred. The most common types are 2 (interactive) and 3 (network). The New Logon fields indicate the account for whom the new logon was created, i.e. the account that was logged on. The network fields indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impersonation level field indicates the extent to which a process in the logon session can impersonate. The authentication information fields provide detailed information about this specific logon request. - Logon GUID is a unique identifier that can be used to correlate this event with a KDC event. - Transited services indicate which intermediate services have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indicates the length of the generated session key. This will be 0 if no session key was requested.
Security	Audit Success	12548	2015-04-23 12:33:01	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Logon ID: 0x3e7 Privileges: SeAssignPrimaryTokenPrivilege SeTcbPrivilege SeSecurityPrivilege SeTakeOwnershipPrivilege SeLoadDriverPrivilege SeBackupPrivilege SeRestorePrivilege

					SeDebugPrivilege SeAuditPrivilege SeSystemEnvironmentPrivilege SeImpersonatePrivilege
Security	Audit Success	12544	2015-04-23 12:33:04	Microsoft-Windows-Security-Auditing	4648: A logon was attempted using explicit credentials. Subject: Security ID: S-1-5-18 Account Name: LTRANPHD$ Account Domain: WORKGROUP Logon ID: 0x3e7 Logon GUID: {00000000-0000-0000-0000-000000000000} Account Whose Credentials Were Used: Account Name: Liem Account Domain: LTRANPHD Logon GUID: {00000000-0000-0000-0000-000000000000} Target Server: Target Server Name: localhost Additional Information: localhost Process Information: Process ID: 0x204 Process Name: C:\Windows\System32\winlogon.exe Network Information: Network Address: 127.0.0.1 Port: 0 This event is generated when a process attempts to log on an account by explicitly specifying that account's credentials. This most commonly occurs in batch-type configurations such as scheduled tasks, or when using the RUNAS command.
Security	Audit Success	12544	2015-04-23 12:33:04	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: LTRANPHD$ Account Domain: WORKGROUP Logon ID: 0x3e7 Logon Type: 2 Impersonation Level: %%1833 New Logon: Security ID: S-1-5-21-1888849264-3803429180-4108621888-1001 Account Name: Liem Account Domain: LTRANPHD Logon ID: 0x1bc5d Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x204 Process Name: C:\Windows\System32\winlogon.exe Network Information: Workstation Name: LTRANPHD Source Network Address: 127.0.0.1 Source Port: 0 Detailed Authentication Information: Logon Process: User32 Authentication Package: Negotiate Transited Services: - Package Name (NTLM only): - Key Length: 0 This event is generated when a logon session is created. It is generated on the computer that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service such as the Server service, or a local process such as Winlogon.exe or Services.exe. The logon type field indicates the kind of logon that occurred. The most common types are 2 (interactive) and 3 (network). The New Logon fields indicate the account for whom the new logon was created, i.e. the account that was logged on. The network fields indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impersonation level field indicates the extent to which a process in the logon session can impersonate. The authentication information fields provide detailed information about this specific logon request. - Logon GUID is a unique identifier that can be used to correlate this event with a KDC event. - Transited services indicate which intermediate services have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indicates the length of the generated session key. This will be 0 if no session key was requested.
Security	Audit Success	12544	2015-04-23 12:33:04	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: LTRANPHD$ Account Domain: WORKGROUP Logon ID: 0x3e7 Logon Type: 2 Impersonation Level: %%1833 New Logon: Security ID: S-1-5-21-1888849264-3803429180-4108621888-1001 Account Name: Liem Account Domain: LTRANPHD Logon ID: 0x1bc8c Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x204 Process Name: C:\Windows\System32\winlogon.exe Network Information: Workstation Name: LTRANPHD Source Network Address: 127.0.0.1 Source Port: 0 Detailed Authentication Information: Logon Process: User32 Authentication Package: Negotiate Transited Services: - Package Name (NTLM only): - Key Length: 0 This event is generated when a logon session is created. It is generated on the computer that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service such as the Server service, or a local process such as Winlogon.exe or Services.exe. The logon type field indicates the kind of logon that occurred. The most common types are 2 (interactive) and 3 (network). The New Logon fields indicate the account for whom the new logon was created, i.e. the account that was logged on. The network fields indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impersonation level field indicates the extent to which a process in the logon session can impersonate. The authentication information fields provide detailed information about this specific logon request. - Logon GUID is a unique identifier that can be used to correlate this event with a KDC event. - Transited services indicate which intermediate services have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indicates the length of the generated session key. This will be 0 if no session key was requested.
Security	Audit Success	12548	2015-04-23 12:33:04	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-21-1888849264-3803429180-4108621888-1001 Account Name: Liem Account Domain: LTRANPHD Logon ID: 0x1bc5d Privileges: SeSecurityPrivilege SeTakeOwnershipPrivilege SeLoadDriverPrivilege SeBackupPrivilege SeRestorePrivilege SeDebugPrivilege SeSystemEnvironmentPrivilege SeImpersonatePrivilege
Security	Audit Success	12544	2015-04-23 12:33:05	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: LTRANPHD$ Account Domain: WORKGROUP Logon ID: 0x3e7 Logon Type: 5 Impersonation Level: %%1833 New Logon: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Logon ID: 0x3e7 Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x22c Process Name: C:\Windows\System32\services.exe Network Information: Workstation Name: Source Network Address: - Source Port: - Detailed Authentication Information: Logon Process: Advapi Authentication Package: Negotiate Transited Services: - Package Name (NTLM only): - Key Length: 0 This event is generated when a logon session is created. It is generated on the computer that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service such as the Server service, or a local process such as Winlogon.exe or Services.exe. The logon type field indicates the kind of logon that occurred. The most common types are 2 (interactive) and 3 (network). The New Logon fields indicate the account for whom the new logon was created, i.e. the account that was logged on. The network fields indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impersonation level field indicates the extent to which a process in the logon session can

					impersonate. The authentication information fields provide detailed information about this specific logon request. - Logon GUID is a unique identifier that can be used to correlate this event with a KDC event. - Transited services indicate which intermediate services have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indicates the length of the generated session key. This will be 0 if no session key was requested.
Security	Audit Success	12548	2015-04-23 12:33:05	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Logon ID: 0x3e7 Privileges: SeAssignPrimaryTokenPrivilege SeTcbPrivilege SeSecurityPrivilege SeTakeOwnershipPrivilege SeLoadDriverPrivilege SeBackupPrivilege SeRestorePrivilege SeDebugPrivilege SeAuditPrivilege SeSystemEnvironmentPrivilege SeImpersonatePrivilege
Security	Audit Success	13824	2015-04-23 12:33:07	Microsoft-Windows-Security-Auditing	4797: An attempt was made to query the existence of a blank password for an account. Subject: Security ID: S-1-5-21-1888849264-3803429180-4108621888-1001 Account Name: Liem Account Domain: LTRANPHD Logon ID: 0x1bc8c Additional Information: Caller Workstation: LTRANPHD Target Account Name: Administrator Target Account Domain: LTRANPHD
Security	Audit Success	13824	2015-04-23 12:33:07	Microsoft-Windows-Security-Auditing	4797: An attempt was made to query the existence of a blank password for an account. Subject: Security ID: S-1-5-21-1888849264-3803429180-4108621888-1001 Account Name: Liem Account Domain: LTRANPHD Logon ID: 0x1bc8c Additional Information: Caller Workstation: LTRANPHD Target Account Name: Guest Target Account Domain: LTRANPHD
Security	Audit Success	13824	2015-04-23 12:33:07	Microsoft-Windows-Security-Auditing	4797: An attempt was made to query the existence of a blank password for an account. Subject: Security ID: S-1-5-21-1888849264-3803429180-4108621888-1001 Account Name: Liem Account Domain: LTRANPHD Logon ID: 0x1bc8c Additional Information: Caller Workstation: LTRANPHD Target Account Name: Administrator Target Account Domain: LTRANPHD
Security	Audit Success	13824	2015-04-23 12:33:07	Microsoft-Windows-Security-Auditing	4797: An attempt was made to query the existence of a blank password for an account. Subject: Security ID: S-1-5-21-1888849264-3803429180-4108621888-1001 Account Name: Liem Account Domain: LTRANPHD Logon ID: 0x1bc8c Additional Information: Caller Workstation: LTRANPHD Target Account Name: Guest Target Account Domain: LTRANPHD
Security	Audit Success	13824	2015-04-23 12:33:49	Microsoft-Windows-Security-Auditing	4797: An attempt was made to query the existence of a blank password for an account. Subject: Security ID: S-1-5-21-1888849264-3803429180-4108621888-1001 Account Name: Liem Account Domain: LTRANPHD Logon ID: 0x1bc8c Additional Information: Caller Workstation: LTRANPHD Target Account Name: Administrator Target Account Domain: LTRANPHD
Security	Audit Success	13824	2015-04-23 12:33:49	Microsoft-Windows-Security-Auditing	4797: An attempt was made to query the existence of a blank password for an account. Subject: Security ID: S-1-5-21-1888849264-3803429180-4108621888-1001 Account Name: Liem Account Domain: LTRANPHD Logon ID: 0x1bc8c Additional Information: Caller Workstation: LTRANPHD Target Account Name: Guest Target Account Domain: LTRANPHD
Security	Audit Success	13824	2015-04-23 12:33:49	Microsoft-Windows-Security-Auditing	4797: An attempt was made to query the existence of a blank password for an account. Subject: Security ID: S-1-5-21-1888849264-3803429180-4108621888-1001 Account Name: Liem Account Domain: LTRANPHD Logon ID: 0x1bc8c Additional Information: Caller Workstation: LTRANPHD Target Account Name: Administrator Target Account Domain: LTRANPHD
Security	Audit Success	13824	2015-04-23 12:33:49	Microsoft-Windows-Security-Auditing	4797: An attempt was made to query the existence of a blank password for an account. Subject: Security ID: S-1-5-21-1888849264-3803429180-4108621888-1001 Account Name: Liem Account Domain: LTRANPHD Logon ID: 0x1bc8c Additional Information: Caller Workstation: LTRANPHD Target Account Name: Guest Target Account Domain: LTRANPHD
Security	Audit Success	13824	2015-04-23 12:45:53	Microsoft-Windows-Security-Auditing	4797: An attempt was made to query the existence of a blank password for an account. Subject: Security ID: S-1-5-21-1888849264-3803429180-4108621888-1001 Account Name: Liem Account Domain: LTRANPHD Logon ID: 0x1bc8c Additional Information: Caller Workstation: LTRANPHD Target Account Name: Administrator Target Account Domain: LTRANPHD
Security	Audit Success	13824	2015-04-23 12:45:53	Microsoft-Windows-Security-Auditing	4797: An attempt was made to query the existence of a blank password for an account. Subject: Security ID: S-1-5-21-1888849264-3803429180-4108621888-1001 Account Name: Liem Account Domain: LTRANPHD Logon ID: 0x1bc8c Additional Information: Caller Workstation: LTRANPHD Target Account Name: Guest Target Account Domain: LTRANPHD
Security	Audit Success	12545	2015-04-23 12:46:09	Microsoft-Windows-Security-Auditing	4647: User initiated logoff: Subject: Security ID: S-1-5-21-1888849264-3803429180-4108621888-1001 Account Name: Liem Account Domain: LTRANPHD Logon ID: 0x1bc8c This event is generated when a logoff is initiated. No further user-initiated activity can occur. This event can be interpreted as a logoff event.
Security	Audit Success	103	2015-04-23 12:46:15	Microsoft-Windows-Eventlog	1100: The event logging service has shut down.
Security	Audit Success	12288	2015-04-24 17:31:51	Microsoft-Windows-Security-Auditing	4616: The system time was changed. Subject: Security ID: S-1-5-19 Account Name: LOCAL SERVICE Account Domain: NT AUTHORITY Logon ID: 0x3e5 Process Information: Process ID: 0x3dc Name: C:\Windows\System32\svchost.exe Previous Time: 2015-03-22T22:31:56.207163300Z New Time: 2015-04-25T00:31:51.590482400Z This event is generated when the system time is changed. It is normal for the Windows Time Service, which runs with System privilege, to change the system time on a regular basis. Other system time changes may be indicative of attempts to tamper with the computer.
	Audit		2015-04-	Microsoft-Windows-Security-	4616: The system time was changed. Subject: Security ID: S-1-5-19 Account Name: LOCAL SERVICE Account Domain: NT AUTHORITY Logon ID: 0x3e5 Process Information: Process ID: 0x3dc Name: C:\Windows\System32\svchost.exe Previous Time: 2015-04-25T00:31:51.578990700Z New Time: 2015-04-

Security	Success	12288	24 17:31:51	Auditing	25T00:31:51.575000000Z This event is generated when the system time is changed. It is normal for the Windows Time Service, which runs with System privilege, to change the system time on a regular basis. Other system time changes may be indicative of attempts to tamper with the computer.
Security	Audit Success	12544	2015-04-24 17:31:52	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: LTRANPHD$ Account Domain: WORKGROUP Logon ID: 0x3e7 Logon Type: 5 Impersonation Level: %%1833 New Logon: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Logon ID: 0x3e7 Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x230 Process Name: C:\Windows\System32\services.exe Network Information: Workstation Name: Source Network Address: - Source Port: - Detailed Authentication Information: Logon Process: Advapi Authentication Package: Negotiate Transited Services: - Package Name (NTLM only): - Key Length: 0 This event is generated when a logon session is created. It is generated on the computer that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service such as the Server service, or a local process such as Winlogon.exe or Services.exe. The logon type field indicates the kind of logon that occurred. The most common types are 2 (interactive) and 3 (network). The New Logon fields indicate the account for whom the new logon was created, i.e. the account that was logged on. The network fields indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impersonation level field indicates the extent to which a process in the logon session can impersonate. The authentication information fields provide detailed information about this specific logon request. - Logon GUID is a unique identifier that can be used to correlate this event with a KDC event. - Transited services indicate which intermediate services have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indicates the length of the generated session key. This will be 0 if no session key was requested.
Security	Audit Success	12548	2015-04-24 17:31:52	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Logon ID: 0x3e7 Privileges: SeAssignPrimaryTokenPrivilege SeTcbPrivilege SeSecurityPrivilege SeTakeOwnershipPrivilege SeLoadDriverPrivilege SeBackupPrivilege SeRestorePrivilege SeDebugPrivilege SeAuditPrivilege SeSystemEnvironmentPrivilege SeImpersonatePrivilege
Security	Audit Success	12544	2015-04-24 17:31:54	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: LTRANPHD$ Account Domain: WORKGROUP Logon ID: 0x3e7 Logon Type: 5 Impersonation Level: %%1833 New Logon: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Logon ID: 0x3e7 Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x230 Process Name: C:\Windows\System32\services.exe Network Information: Workstation Name: Source Network Address: - Source Port: - Detailed Authentication Information: Logon Process: Advapi Authentication Package: Negotiate Transited Services: - Package Name (NTLM only): - Key Length: 0 This event is generated when a logon session is created. It is generated on the computer that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service such as the Server service, or a local process such as Winlogon.exe or Services.exe. The logon type field indicates the kind of logon that occurred. The most common types are 2 (interactive) and 3 (network). The New Logon fields indicate the account for whom the new logon was created, i.e. the account that was logged on. The network fields indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impersonation level field indicates the extent to which a process in the logon session can impersonate. The authentication information fields provide detailed information about this specific logon request. - Logon GUID is a unique identifier that can be used to correlate this event with a KDC event. - Transited services indicate which intermediate services have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indicates the length of the generated session key. This will be 0 if no session key was requested.
Security	Audit Success	12548	2015-04-24 17:31:54	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Logon ID: 0x3e7 Privileges: SeAssignPrimaryTokenPrivilege SeTcbPrivilege SeSecurityPrivilege SeTakeOwnershipPrivilege SeLoadDriverPrivilege SeBackupPrivilege SeRestorePrivilege SeDebugPrivilege SeAuditPrivilege SeSystemEnvironmentPrivilege SeImpersonatePrivilege
Security	Audit Success	12288	2015-04-24 17:58:32	Microsoft-Windows-Security-Auditing	4608: Windows is starting up. This event is logged when LSASS.EXE starts and the auditing subsystem is initialized.
Security	Audit Success	12544	2015-04-24 17:58:32	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-0-0 Account Name: - Account Domain: - Logon ID: 0x0 Logon Type: 0 Impersonation Level: - New Logon: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Logon ID: 0x3e7 Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x4 Process Name: Network Information: Workstation Name: - Source Network Address: - Source Port: - Detailed Authentication Information: Logon Process: - Authentication Package: - Transited Services: - Package Name (NTLM only): - Key Length: 0 This event is generated when a logon session is created. It is generated on the computer that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service such as the Server service, or a local process such as Winlogon.exe or Services.exe. The logon type field indicates the kind of logon that occurred. The most common types are 2 (interactive) and 3 (network). The New Logon fields indicate the account for whom the new logon was created, i.e. the account that was logged on. The network fields indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impersonation level field indicates the extent to which a process in the logon session can impersonate. The authentication information fields provide detailed information

					about this specific logon request. - Logon GUID is a unique identifier that can be used to correlate this event with a KDC event. - Transited services indicate which intermediate services have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indicates the length of the generated session key. This will be 0 if no session key was requested.
Security	Audit Success	12544	2015-04-24 17:58:32	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: LTRANPHD$ Account Domain: WORKGROUP Logon ID: 0x3e7 Logon Type: 5 Impersonation Level: %%1833 New Logon: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Logon ID: 0x3e7 Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x22c Process Name: C:\Windows\System32\services.exe Network Information: Workstation Name: Source Network Address: - Source Port: - Detailed Authentication Information: Logon Process: Advapi Authentication Package: Negotiate Transited Services: - Package Name (NTLM only): - Key Length: 0 This event is generated when a logon session is created. It is generated on the computer that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service such as the Server service, or a local process such as Winlogon.exe or Services.exe. The logon type field indicates the kind of logon that occurred. The most common types are 2 (interactive) and 3 (network). The New Logon fields indicate the account for whom the new logon was created, i.e. the account that was logged on. The network fields indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impersonation level field indicates the extent to which a process in the logon session can impersonate. The authentication information fields provide detailed information about this specific logon request. - Logon GUID is a unique identifier that can be used to correlate this event with a KDC event. - Transited services indicate which intermediate services have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indicates the length of the generated session key. This will be 0 if no session key was requested.
Security	Audit Success	12544	2015-04-24 17:58:32	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: LTRANPHD$ Account Domain: WORKGROUP Logon ID: 0x3e7 Logon Type: 5 Impersonation Level: %%1833 New Logon: Security ID: S-1-5-20 Account Name: NETWORK SERVICE Account Domain: NT AUTHORITY Logon ID: 0x3e4 Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x22c Process Name: C:\Windows\System32\services.exe Network Information: Workstation Name: Source Network Address: - Source Port: - Detailed Authentication Information: Logon Process: Advapi Authentication Package: Negotiate Transited Services: - Package Name (NTLM only): - Key Length: 0 This event is generated when a logon session is created. It is generated on the computer that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service such as the Server service, or a local process such as Winlogon.exe or Services.exe. The logon type field indicates the kind of logon that occurred. The most common types are 2 (interactive) and 3 (network). The New Logon fields indicate the account for whom the new logon was created, i.e. the account that was logged on. The network fields indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impersonation level field indicates the extent to which a process in the logon session can impersonate. The authentication information fields provide detailed information about this specific logon request. - Logon GUID is a unique identifier that can be used to correlate this event with a KDC event. - Transited services indicate which intermediate services have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indicates the length of the generated session key. This will be 0 if no session key was requested.
Security	Audit Success	12544	2015-04-24 17:58:32	Microsoft-Windows-Security-Auditing	4648: A logon was attempted using explicit credentials. Subject: Security ID: S-1-5-18 Account Name: LTRANPHD$ Account Domain: WORKGROUP Logon ID: 0x3e7 Logon GUID: {00000000-0000-0000-0000-000000000000} Account Whose Credentials Were Used: Account Name: DWM-1 Account Domain: Window Manager Logon GUID: {00000000-0000-0000-0000-000000000000} Target Server: Target Server Name: localhost Additional Information: localhost Process Information: Process ID: 0x214 Process Name: C:\Windows\System32\winlogon.exe Network Information: Network Address: - Port: - This event is generated when a process attempts to log on an account by explicitly specifying that account's credentials. This most commonly occurs in batch-type configurations such as scheduled tasks, or when using the RUNAS command.
Security	Audit Success	12544	2015-04-24 17:58:32	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: LTRANPHD$ Account Domain: WORKGROUP Logon ID: 0x3e7 Logon Type: 2 Impersonation Level: %%1833 New Logon: Security ID: S-1-5-90-1 Account Name: DWM-1 Account Domain: Window Manager Logon ID: 0xd624 Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x214 Process Name: C:\Windows\System32\winlogon.exe Network Information: Workstation Name: Source Network Address: - Source Port: - Detailed Authentication Information: Logon Process: Advapi Authentication Package: Negotiate Transited Services: - Package Name (NTLM only): - Key Length: 0 This event is generated when a logon session is created. It is generated on the computer that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service such as the Server service, or a local process such as Winlogon.exe or Services.exe. The logon type field indicates the kind of logon that occurred. The most common types are 2 (interactive) and 3 (network). The New Logon fields indicate the account for whom the new logon was created, i.e. the account that was logged on. The network fields indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impersonation level field indicates the extent to which a process in the logon session can impersonate. The authentication information fields provide detailed information about this specific logon request. - Logon GUID is a unique identifier that can be used to correlate this event with a KDC event. - Transited services indicate which intermediate services have participated in this logon request. - Package name indicates

					which sub-protocol was used among the NTLM protocols. - Key length indicates the length of the generated session key. This will be 0 if no session key was requested.
Security	Audit Success	12544	2015-04-24 17:58:32	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: LTRANPHD$ Account Domain: WORKGROUP Logon ID: 0x3e7 Logon Type: 2 Impersonation Level: %%1833 New Logon: Security ID: S-1-5-90-1 Account Name: DWM-1 Account Domain: Window Manager Logon ID: 0xd639 Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x214 Process Name: C:\Windows\System32\winlogon.exe Network Information: Workstation Name: Source Network Address: - Source Port: - Detailed Authentication Information: Logon Process: Advapi Authentication Package: Negotiate Transited Services: - Package Name (NTLM only): - Key Length: 0 This event is generated when a logon session is created. It is generated on the computer that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service such as the Server service, or a local process such as Winlogon.exe or Services.exe. The logon type field indicates the kind of logon that occurred. The most common types are 2 (interactive) and 3 (network). The New Logon fields indicate the account for whom the new logon was created, i.e. the account that was logged on. The network fields indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impersonation level field indicates the extent to which a process in the logon session can impersonate. The authentication information fields provide detailed information about this specific logon request. - Logon GUID is a unique identifier that can be used to correlate this event with a KDC event. - Transited services indicate which intermediate services have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indicates the length of the generated session key. This will be 0 if no session key was requested.
Security	Audit Success	12548	2015-04-24 17:58:32	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Logon ID: 0x3e7 Privileges: SeAssignPrimaryTokenPrivilege SeTcbPrivilege SeSecurityPrivilege SeTakeOwnershipPrivilege SeLoadDriverPrivilege SeBackupPrivilege SeRestorePrivilege SeDebugPrivilege SeAuditPrivilege SeSystemEnvironmentPrivilege SeImpersonatePrivilege
Security	Audit Success	12548	2015-04-24 17:58:32	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-20 Account Name: NETWORK SERVICE Account Domain: NT AUTHORITY Logon ID: 0x3e4 Privileges: SeAssignPrimaryTokenPrivilege SeAuditPrivilege SeImpersonatePrivilege
Security	Audit Success	12548	2015-04-24 17:58:32	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-90-1 Account Name: DWM-1 Account Domain: Window Manager Logon ID: 0xd624 Privileges: SeAssignPrimaryTokenPrivilege SeAuditPrivilege SeImpersonatePrivilege
Security	Audit Success	12548	2015-04-24 17:58:32	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-90-1 Account Name: DWM-1 Account Domain: Window Manager Logon ID: 0xd639 Privileges: SeAssignPrimaryTokenPrivilege SeAuditPrivilege
Security	Audit Success	13568	2015-04-24 17:58:32	Microsoft-Windows-Security-Auditing	4902: The Per-user audit policy table was created. Number of Elements: 0 Policy ID: 0x9d80
Security	Audit Success	12544	2015-04-24 17:58:33	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: LTRANPHD$ Account Domain: WORKGROUP Logon ID: 0x3e7 Logon Type: 5 Impersonation Level: %%1833 New Logon: Security ID: S-1-5-19 Account Name: LOCAL SERVICE Account Domain: NT AUTHORITY Logon ID: 0x3e5 Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x22c Process Name: C:\Windows\System32\services.exe Network Information: Workstation Name: Source Network Address: - Source Port: - Detailed Authentication Information: Logon Process: Advapi Authentication Package: Negotiate Transited Services: - Package Name (NTLM only): - Key Length: 0 This event is generated when a logon session is created. It is generated on the computer that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service such as the Server service, or a local process such as Winlogon.exe or Services.exe. The logon type field indicates the kind of logon that occurred. The most common types are 2 (interactive) and 3 (network). The New Logon fields indicate the account for whom the new logon was created, i.e. the account that was logged on. The network fields indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impersonation level field indicates the extent to which a process in the logon session can impersonate. The authentication information fields provide detailed information about this specific logon request. - Logon GUID is a unique identifier that can be used to correlate this event with a KDC event. - Transited services indicate which intermediate services have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indicates the length of the generated session key. This will be 0 if no session key was requested.
Security	Audit	12544	2015-04-24	Microsoft-Windows-Security-	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: LTRANPHD$ Account Domain: WORKGROUP Logon ID: 0x3e7 Logon Type: 5 Impersonation Level: %%1833 New Logon: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Logon ID: 0x3e7 Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x22c Process Name: C:\Windows\System32\services.exe Network Information: Workstation Name: Source Network Address: - Source Port: - Detailed Authentication Information: Logon Process: Advapi Authentication Package: Negotiate Transited Services: - Package Name (NTLM only): - Key Length: 0 This event is generated when a logon session is created. It is generated on the computer that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service such as the Server service, or a local process such as Winlogon.exe or Services.exe. The logon type field indicates the kind of logon that occurred.

	Success		17:58:33	Auditing	The most common types are 2 (interactive) and 3 (network). The New Logon fields indicate the account for whom the new logon was created, i.e. the account that was logged on. The network fields indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impersonation level field indicates the extent to which a process in the logon session can impersonate. The authentication information fields provide detailed information about this specific logon request. - Logon GUID is a unique identifier that can be used to correlate this event with a KDC event. - Transited services indicate which intermediate services have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indicates the length of the generated session key. This will be 0 if no session key was requested.
Security	Audit Success	12544	2015-04-24 17:58:33	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: LTRANPHD$ Account Domain: WORKGROUP Logon ID: 0x3e7 Logon Type: 5 Impersonation Level: %%1833 New Logon: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Logon ID: 0x3e7 Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x22c Process Name: C:\Windows\System32\services.exe Network Information: Workstation Name: Source Network Address: - Source Port: - Detailed Authentication Information: Logon Process: Advapi Authentication Package: Negotiate Transited Services: - Package Name (NTLM only): - Key Length: 0 This event is generated when a logon session is created. It is generated on the computer that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service such as the Server service, or a local process such as Winlogon.exe or Services.exe. The logon type field indicates the kind of logon that occurred. The most common types are 2 (interactive) and 3 (network). The New Logon fields indicate the account for whom the new logon was created, i.e. the account that was logged on. The network fields indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impersonation level field indicates the extent to which a process in the logon session can impersonate. The authentication information fields provide detailed information about this specific logon request. - Logon GUID is a unique identifier that can be used to correlate this event with a KDC event. - Transited services indicate which intermediate services have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indicates the length of the generated session key. This will be 0 if no session key was requested.
Security	Audit Success	12548	2015-04-24 17:58:33	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-19 Account Name: LOCAL SERVICE Account Domain: NT AUTHORITY Logon ID: 0x3e5 Privileges: SeAssignPrimaryTokenPrivilege SeAuditPrivilege SeImpersonatePrivilege
Security	Audit Success	12548	2015-04-24 17:58:33	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Logon ID: 0x3e7 Privileges: SeAssignPrimaryTokenPrivilege SeTcbPrivilege SeSecurityPrivilege SeTakeOwnershipPrivilege SeLoadDriverPrivilege SeBackupPrivilege SeRestorePrivilege SeDebugPrivilege SeAuditPrivilege SeSystemEnvironmentPrivilege SeImpersonatePrivilege
Security	Audit Success	12548	2015-04-24 17:58:33	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Logon ID: 0x3e7 Privileges: SeAssignPrimaryTokenPrivilege SeTcbPrivilege SeSecurityPrivilege SeTakeOwnershipPrivilege SeLoadDriverPrivilege SeBackupPrivilege SeRestorePrivilege SeDebugPrivilege SeAuditPrivilege SeSystemEnvironmentPrivilege SeImpersonatePrivilege
Security	Audit Success	12292	2015-04-24 17:58:34	Microsoft-Windows-Security-Auditing	5033: The Windows Firewall Driver started successfully.
Security	Audit Success	12544	2015-04-24 17:58:34	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: LTRANPHD$ Account Domain: WORKGROUP Logon ID: 0x3e7 Logon Type: 5 Impersonation Level: %%1833 New Logon: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Logon ID: 0x3e7 Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x22c Process Name: C:\Windows\System32\services.exe Network Information: Workstation Name: Source Network Address: - Source Port: - Detailed Authentication Information: Logon Process: Advapi Authentication Package: Negotiate Transited Services: - Package Name (NTLM only): - Key Length: 0 This event is generated when a logon session is created. It is generated on the computer that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service such as the Server service, or a local process such as Winlogon.exe or Services.exe. The logon type field indicates the kind of logon that occurred. The most common types are 2 (interactive) and 3 (network). The New Logon fields indicate the account for whom the new logon was created, i.e. the account that was logged on. The network fields indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impersonation level field indicates the extent to which a process in the logon session can impersonate. The authentication information fields provide detailed information about this specific logon request. - Logon GUID is a unique identifier that can be used to correlate this event with a KDC event. - Transited services indicate which intermediate services have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indicates the length of the generated session key. This will be 0 if no session key was requested.
					4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: LTRANPHD$ Account Domain: WORKGROUP Logon ID: 0x3e7 Logon Type: 5 Impersonation Level: %%1833 New Logon: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Logon ID: 0x3e7 Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x22c Process Name:

Security	Audit Success	12544	2015-04-24 17:58:34	Microsoft-Windows-Security-Auditing	C:\Windows\System32\services.exe Network Information: Workstation Name: Source Network Address: - Source Port: - Detailed Authentication Information: Logon Process: Advapi Authentication Package: Negotiate Transited Services: - Package Name (NTLM only): - Key Length: 0 This event is generated when a logon session is created. It is generated on the computer that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service such as the Server service, or a local process such as Winlogon.exe or Services.exe. The logon type field indicates the kind of logon that occurred. The most common types are 2 (interactive) and 3 (network). The New Logon fields indicate the account for whom the new logon was created, i.e. the account that was logged on. The network fields indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impersonation level field indicates the extent to which a process in the logon session can impersonate. The authentication information fields provide detailed information about this specific logon request. - Logon GUID is a unique identifier that can be used to correlate this event with a KDC event. - Transited services indicate which intermediate services have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indicates the length of the generated session key. This will be 0 if no session key was requested.
Security	Audit Success	12548	2015-04-24 17:58:34	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Logon ID: 0x3e7 Privileges: SeAssignPrimaryTokenPrivilege SeTcbPrivilege SeSecurityPrivilege SeTakeOwnershipPrivilege SeLoadDriverPrivilege SeBackupPrivilege SeRestorePrivilege SeDebugPrivilege SeAuditPrivilege SeSystemEnvironmentPrivilege SeImpersonatePrivilege
Security	Audit Success	12548	2015-04-24 17:58:34	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Logon ID: 0x3e7 Privileges: SeAssignPrimaryTokenPrivilege SeTcbPrivilege SeSecurityPrivilege SeTakeOwnershipPrivilege SeLoadDriverPrivilege SeBackupPrivilege SeRestorePrivilege SeDebugPrivilege SeAuditPrivilege SeSystemEnvironmentPrivilege SeImpersonatePrivilege
Security	Audit Success	12292	2015-04-24 17:58:35	Microsoft-Windows-Security-Auditing	5024: The Windows Firewall service started successfully.
Security	Audit Success	12544	2015-04-24 17:58:35	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: LTRANPHD$ Account Domain: WORKGROUP Logon ID: 0x3e7 Logon Type: 5 Impersonation Level: %%1833 New Logon: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Logon ID: 0x3e7 Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x22c Process Name: C:\Windows\System32\services.exe Network Information: Workstation Name: Source Network Address: - Source Port: - Detailed Authentication Information: Logon Process: Advapi Authentication Package: Negotiate Transited Services: - Package Name (NTLM only): - Key Length: 0 This event is generated when a logon session is created. It is generated on the computer that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service such as the Server service, or a local process such as Winlogon.exe or Services.exe. The logon type field indicates the kind of logon that occurred. The most common types are 2 (interactive) and 3 (network). The New Logon fields indicate the account for whom the new logon was created, i.e. the account that was logged on. The network fields indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impersonation level field indicates the extent to which a process in the logon session can impersonate. The authentication information fields provide detailed information about this specific logon request. - Logon GUID is a unique identifier that can be used to correlate this event with a KDC event. - Transited services indicate which intermediate services have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indicates the length of the generated session key. This will be 0 if no session key was requested.
Security	Audit Success	12548	2015-04-24 17:58:35	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Logon ID: 0x3e7 Privileges: SeAssignPrimaryTokenPrivilege SeTcbPrivilege SeSecurityPrivilege SeTakeOwnershipPrivilege SeLoadDriverPrivilege SeBackupPrivilege SeRestorePrivilege SeDebugPrivilege SeAuditPrivilege SeSystemEnvironmentPrivilege SeImpersonatePrivilege
Security	Audit Success	12544	2015-04-24 17:58:36	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-0-0 Account Name: - Account Domain: - Logon ID: 0x0 Logon Type: 3 Impersonation Level: %%1833 New Logon: Security ID: S-1-5-7 Account Name: ANONYMOUS LOGON Account Domain: NT AUTHORITY Logon ID: 0x1ab2d Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x0 Process Name: - Network Information: Workstation Name: Source Network Address: - Source Port: - Detailed Authentication Information: Logon Process: NtLmSsp Authentication Package: NTLM Transited Services: - Package Name (NTLM only): NTLM V1 Key Length: 0 This event is generated when a logon session is created. It is generated on the computer that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service such as the Server service, or a local process such as Winlogon.exe or Services.exe. The logon type field indicates the kind of logon that occurred. The most common types are 2 (interactive) and 3 (network). The New Logon fields indicate the account for whom the new logon was created, i.e. the account that was logged on. The network fields indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impersonation level field indicates the extent to which a process in the logon session can impersonate. The authentication information fields provide detailed information about this specific logon request. - Logon GUID is a unique identifier that can be used to correlate this event with a KDC event. - Transited services indicate which intermediate services have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length

					indicates the length of the generated session key. This will be 0 if no session key was requested.
Security	Audit Success	12544	2015-04-24 17:58:37	Microsoft-Windows-Security-Auditing	4648: A logon was attempted using explicit credentials. Subject: Security ID: S-1-5-18 Account Name: LTRANPHD$ Account Domain: WORKGROUP Logon ID: 0x3e7 Logon GUID: {00000000-0000-0000-0000-000000000000} Account Whose Credentials Were Used: Account Name: Liem Account Domain: LTRANPHD Logon GUID: {00000000-0000-0000-0000-000000000000} Target Server: Target Server Name: localhost Additional Information: localhost Process Information: Process ID: 0x214 Process Name: C:\Windows\System32\winlogon.exe Network Information: Network Address: 127.0.0.1 Port: 0 This event is generated when a process attempts to log on an account by explicitly specifying that account's credentials. This most commonly occurs in batch-type configurations such as scheduled tasks, or when using the RUNAS command.
Security	Audit Success	12544	2015-04-24 17:58:37	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: LTRANPHD$ Account Domain: WORKGROUP Logon ID: 0x3e7 Logon Type: 2 Impersonation Level: %%1833 New Logon: Security ID: S-1-5-21-1888849264-3803429180-4108621888-1001 Account Name: Liem Account Domain: LTRANPHD Logon ID: 0x1ba74 Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x214 Process Name: C:\Windows\System32\winlogon.exe Network Information: Workstation Name: LTRANPHD Source Network Address: 127.0.0.1 Source Port: 0 Detailed Authentication Information: Logon Process: User32 Authentication Package: Negotiate Transited Services: - Package Name (NTLM only): - Key Length: 0 This event is generated when a logon session is created. It is generated on the computer that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service such as the Server service, or a local process such as Winlogon.exe or Services.exe. The logon type field indicates the kind of logon that occurred. The most common types are 2 (interactive) and 3 (network). The New Logon fields indicate the account for whom the new logon was created, i.e. the account that was logged on. The network fields indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impersonation level field indicates the extent to which a process in the logon session can impersonate. The authentication information fields provide detailed information about this specific logon request. - Logon GUID is a unique identifier that can be used to correlate this event with a KDC event. - Transited services indicate which intermediate services have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indicates the length of the generated session key. This will be 0 if no session key was requested.
Security	Audit Success	12544	2015-04-24 17:58:37	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: LTRANPHD$ Account Domain: WORKGROUP Logon ID: 0x3e7 Logon Type: 2 Impersonation Level: %%1833 New Logon: Security ID: S-1-5-21-1888849264-3803429180-4108621888-1001 Account Name: Liem Account Domain: LTRANPHD Logon ID: 0x1baa3 Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x214 Process Name: C:\Windows\System32\winlogon.exe Network Information: Workstation Name: LTRANPHD Source Network Address: 127.0.0.1 Source Port: 0 Detailed Authentication Information: Logon Process: User32 Authentication Package: Negotiate Transited Services: - Package Name (NTLM only): - Key Length: 0 This event is generated when a logon session is created. It is generated on the computer that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service such as the Server service, or a local process such as Winlogon.exe or Services.exe. The logon type field indicates the kind of logon that occurred. The most common types are 2 (interactive) and 3 (network). The New Logon fields indicate the account for whom the new logon was created, i.e. the account that was logged on. The network fields indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impersonation level field indicates the extent to which a process in the logon session can impersonate. The authentication information fields provide detailed information about this specific logon request. - Logon GUID is a unique identifier that can be used to correlate this event with a KDC event. - Transited services indicate which intermediate services have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indicates the length of the generated session key. This will be 0 if no session key was requested.
Security	Audit Success	12548	2015-04-24 17:58:37	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-21-1888849264-3803429180-4108621888-1001 Account Name: Liem Account Domain: LTRANPHD Logon ID: 0x1ba74 Privileges: SeSecurityPrivilege SeTakeOwnershipPrivilege SeLoadDriverPrivilege SeBackupPrivilege SeRestorePrivilege SeDebugPrivilege SeSystemEnvironmentPrivilege SeImpersonatePrivilege
Security	Audit Success	12544	2015-04-24 17:58:39	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: LTRANPHD$ Account Domain: WORKGROUP Logon ID: 0x3e7 Logon Type: 5 Impersonation Level: %%1833 New Logon: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Logon ID: 0x3e7 Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x22c Process Name: C:\Windows\System32\services.exe Network Information: Workstation Name: Source Network Address: - Source Port: - Detailed Authentication Information: Logon Process: Advapi Authentication Package: Negotiate Transited Services: - Package Name (NTLM only): - Key Length: 0 This event is generated when a logon session is created. It is generated on the computer that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service such as the Server service, or a local process such as Winlogon.exe or Services.exe. The logon type field indicates the kind of logon that occurred. The most common types are 2 (interactive) and 3 (network). The New Logon fields indicate the account for whom the new logon was created, i.e. the account that was logged on. The network fields indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impersonation level field indicates the extent to which a process in the logon session can

					impersonate. The authentication information fields provide detailed information about this specific logon request. - Logon GUID is a unique identifier that can be used to correlate this event with a KDC event. - Transited services indicate which intermediate services have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indicates the length of the generated session key. This will be 0 if no session key was requested.
Security	Audit Success	12548	2015-04-24 17:58:39	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Logon ID: 0x3e7 Privileges: SeAssignPrimaryTokenPrivilege SeTcbPrivilege SeSecurityPrivilege SeTakeOwnershipPrivilege SeLoadDriverPrivilege SeBackupPrivilege SeRestorePrivilege SeDebugPrivilege SeAuditPrivilege SeSystemEnvironmentPrivilege SeImpersonatePrivilege
Security	Audit Success	13824	2015-04-24 17:58:42	Microsoft-Windows-Security-Auditing	4797: An attempt was made to query the existence of a blank password for an account. Subject: Security ID: S-1-5-19 Account Name: LOCAL SERVICE Account Domain: NT AUTHORITY Logon ID: 0x3e5 Additional Information: Caller Workstation: LTRANPHD Target Account Name: Administrator Target Account Domain: LTRANPHD
Security	Audit Success	13824	2015-04-24 17:58:42	Microsoft-Windows-Security-Auditing	4797: An attempt was made to query the existence of a blank password for an account. Subject: Security ID: S-1-5-19 Account Name: LOCAL SERVICE Account Domain: NT AUTHORITY Logon ID: 0x3e5 Additional Information: Caller Workstation: LTRANPHD Target Account Name: Guest Target Account Domain: LTRANPHD
Security	Audit Success	13824	2015-04-24 17:58:42	Microsoft-Windows-Security-Auditing	4797: An attempt was made to query the existence of a blank password for an account. Subject: Security ID: S-1-5-19 Account Name: LOCAL SERVICE Account Domain: NT AUTHORITY Logon ID: 0x3e5 Additional Information: Caller Workstation: LTRANPHD Target Account Name: Liem Target Account Domain: LTRANPHD
Security	Audit Success	13824	2015-04-24 17:58:42	Microsoft-Windows-Security-Auditing	4797: An attempt was made to query the existence of a blank password for an account. Subject: Security ID: S-1-5-19 Account Name: LOCAL SERVICE Account Domain: NT AUTHORITY Logon ID: 0x3e5 Additional Information: Caller Workstation: LTRANPHD Target Account Name: Liem Target Account Domain: LTRANPHD
Security	Audit Success	13824	2015-04-24 17:58:42	Microsoft-Windows-Security-Auditing	4797: An attempt was made to query the existence of a blank password for an account. Subject: Security ID: S-1-5-19 Account Name: LOCAL SERVICE Account Domain: NT AUTHORITY Logon ID: 0x3e5 Additional Information: Caller Workstation: LTRANPHD Target Account Name: Administrator Target Account Domain: LTRANPHD
Security	Audit Success	13824	2015-04-24 17:58:42	Microsoft-Windows-Security-Auditing	4797: An attempt was made to query the existence of a blank password for an account. Subject: Security ID: S-1-5-19 Account Name: LOCAL SERVICE Account Domain: NT AUTHORITY Logon ID: 0x3e5 Additional Information: Caller Workstation: LTRANPHD Target Account Name: Guest Target Account Domain: LTRANPHD
Security	Audit Success	13824	2015-04-24 17:58:42	Microsoft-Windows-Security-Auditing	4797: An attempt was made to query the existence of a blank password for an account. Subject: Security ID: S-1-5-19 Account Name: LOCAL SERVICE Account Domain: NT AUTHORITY Logon ID: 0x3e5 Additional Information: Caller Workstation: LTRANPHD Target Account Name: Liem Target Account Domain: LTRANPHD
Security	Audit Success	13824	2015-04-24 17:58:42	Microsoft-Windows-Security-Auditing	4797: An attempt was made to query the existence of a blank password for an account. Subject: Security ID: S-1-5-19 Account Name: LOCAL SERVICE Account Domain: NT AUTHORITY Logon ID: 0x3e5 Additional Information: Caller Workstation: LTRANPHD Target Account Name: Liem Target Account Domain: LTRANPHD
Security	Audit Success	13824	2015-04-24 17:58:42	Microsoft-Windows-Security-Auditing	4797: An attempt was made to query the existence of a blank password for an account. Subject: Security ID: S-1-5-21-1888849264-3803429180-4108621888-1001 Account Name: Liem Account Domain: LTRANPHD Logon ID: 0x1baa3 Additional Information: Caller Workstation: LTRANPHD Target Account Name: Administrator Target Account Domain: LTRANPHD
Security	Audit Success	13824	2015-04-24 17:58:42	Microsoft-Windows-Security-Auditing	4797: An attempt was made to query the existence of a blank password for an account. Subject: Security ID: S-1-5-21-1888849264-3803429180-4108621888-1001 Account Name: Liem Account Domain: LTRANPHD Logon ID: 0x1baa3 Additional Information: Caller Workstation: LTRANPHD Target Account Name: Guest Target Account Domain: LTRANPHD
Security	Audit Success	13824	2015-04-24 17:58:42	Microsoft-Windows-Security-Auditing	4797: An attempt was made to query the existence of a blank password for an account. Subject: Security ID: S-1-5-21-1888849264-3803429180-4108621888-1001 Account Name: Liem Account Domain: LTRANPHD Logon ID: 0x1baa3 Additional Information: Caller Workstation: LTRANPHD Target Account Name: Administrator Target Account Domain: LTRANPHD
Security	Audit Success	13824	2015-04-24 17:58:42	Microsoft-Windows-Security-Auditing	4797: An attempt was made to query the existence of a blank password for an account. Subject: Security ID: S-1-5-21-1888849264-3803429180-4108621888-1001 Account Name: Liem Account Domain: LTRANPHD Logon ID: 0x1baa3 Additional Information: Caller Workstation: LTRANPHD Target Account Name: Guest Target Account Domain: LTRANPHD
Security	Audit Success	12544	2015-04-24 17:58:57	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: LTRANPHD$ Account Domain: WORKGROUP Logon ID: 0x3e7 Logon Type: 5 Impersonation Level: %%1833 New Logon: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Logon ID: 0x3e7 Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x22c Process Name: C:\Windows\System32\services.exe Network Information: Workstation Name: Source Network Address: - Source Port: - Detailed Authentication Information: Logon Process: Advapi Authentication Package: Negotiate Transited Services: - Package Name (NTLM only): - Key Length: 0 This event is generated when a logon session is created. It is generated on the computer that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service such as the Server service, or a local process such as Winlogon.exe or Services.exe. The logon type field indicates the kind of logon that occurred. The most common types are 2 (interactive) and 3 (network). The New Logon fields indicate the account for whom the new logon was created, i.e. the account that was logged on. The network fields indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some

					cases. The impersonation level field indicates the extent to which a process in the logon session can impersonate. The authentication information fields provide detailed information about this specific logon request. - Logon GUID is a unique identifier that can be used to correlate this event with a KDC event. - Transited services indicate which intermediate services have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indicates the length of the generated session key. This will be 0 if no session key was requested.
Security	Audit Success	12548	2015-04-24 17:58:57	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Logon ID: 0x3e7 Privileges: SeAssignPrimaryTokenPrivilege SeTcbPrivilege SeSecurityPrivilege SeTakeOwnershipPrivilege SeLoadDriverPrivilege SeBackupPrivilege SeRestorePrivilege SeDebugPrivilege SeAuditPrivilege SeSystemEnvironmentPrivilege SeImpersonatePrivilege
Security	Audit Success	12544	2015-04-24 17:58:59	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: LTRANPHD$ Account Domain: WORKGROUP Logon ID: 0x3e7 Logon Type: 5 Impersonation Level: %%1833 New Logon: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Logon ID: 0x3e7 Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x22c Process Name: C:\Windows\System32\services.exe Network Information: Workstation Name: Source Network Address: - Source Port: - Detailed Authentication Information: Logon Process: Advapi Authentication Package: Negotiate Transited Services: - Package Name (NTLM only): - Key Length: 0 This event is generated when a logon session is created. It is generated on the computer that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service such as the Server service, or a local process such as Winlogon.exe or Services.exe. The logon type field indicates the kind of logon that occurred. The most common types are 2 (interactive) and 3 (network). The New Logon fields indicate the account for whom the new logon was created, i.e. the account that was logged on. The network fields indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impersonation level field indicates the extent to which a process in the logon session can impersonate. The authentication information fields provide detailed information about this specific logon request. - Logon GUID is a unique identifier that can be used to correlate this event with a KDC event. - Transited services indicate which intermediate services have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indicates the length of the generated session key. This will be 0 if no session key was requested.
Security	Audit Success	12548	2015-04-24 17:58:59	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Logon ID: 0x3e7 Privileges: SeAssignPrimaryTokenPrivilege SeTcbPrivilege SeSecurityPrivilege SeTakeOwnershipPrivilege SeLoadDriverPrivilege SeBackupPrivilege SeRestorePrivilege SeDebugPrivilege SeAuditPrivilege SeSystemEnvironmentPrivilege SeImpersonatePrivilege
Security	Audit Success	103	2015-04-24 18:00:28	Microsoft-Windows-Eventlog	1100: The event logging service has shut down.
Security	Audit Success	12545	2015-04-24 18:00:28	Microsoft-Windows-Security-Auditing	4647: User initiated logoff: Subject: Security ID: S-1-5-21-1888849264-3803429180-4108621888-1001 Account Name: Liem Account Domain: LTRANPHD Logon ID: 0x1baa3 This event is generated when a logoff is initiated. No further user-initiated activity can occur. This event can be interpreted as a logoff event.
Security	Audit Success	12288	2015-04-24 18:00:41	Microsoft-Windows-Security-Auditing	4608: Windows is starting up. This event is logged when LSASS.EXE starts and the auditing subsystem is initialized.
Security	Audit Success	12544	2015-04-24 18:00:41	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-0-0 Account Name: - Account Domain: - Logon ID: 0x0 Logon Type: 0 Impersonation Level: - New Logon: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Logon ID: 0x3e7 Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x4 Process Name: Network Information: Workstation Name: - Source Network Address: - Source Port: - Detailed Authentication Information: Logon Process: - Authentication Package: - Transited Services: - Package Name (NTLM only): - Key Length: 0 This event is generated when a logon session is created. It is generated on the computer that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service such as the Server service, or a local process such as Winlogon.exe or Services.exe. The logon type field indicates the kind of logon that occurred. The most common types are 2 (interactive) and 3 (network). The New Logon fields indicate the account for whom the new logon was created, i.e. the account that was logged on. The network fields indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impersonation level field indicates the extent to which a process in the logon session can impersonate. The authentication information fields provide detailed information about this specific logon request. - Logon GUID is a unique identifier that can be used to correlate this event with a KDC event. - Transited services indicate which intermediate services have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indicates the length of the generated session key. This will be 0 if no session key was requested.
					4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: LTRANPHD$ Account Domain: WORKGROUP Logon ID: 0x3e7 Logon Type: 5 Impersonation Level: %%1833 New Logon: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Logon ID: 0x3e7 Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x230 Process Name: C:\Windows\System32\services.exe Network Information: Workstation Name: Source Network Address: - Source Port: - Detailed Authentication Information: Logon Process: Advapi Authentication Package: Negotiate Transited

Security	Audit Success	12544	2015-04-24 18:00:41	Microsoft-Windows-Security-Auditing	Services: - Package Name (NTLM only): - Key Length: 0 This event is generated when a logon session is created. It is generated on the computer that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service such as the Server service, or a local process such as Winlogon.exe or Services.exe. The logon type field indicates the kind of logon that occurred. The most common types are 2 (interactive) and 3 (network). The New Logon fields indicate the account for whom the new logon was created, i.e. the account that was logged on. The network fields indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impersonation level field indicates the extent to which a process in the logon session can impersonate. The authentication information fields provide detailed information about this specific logon request. - Logon GUID is a unique identifier that can be used to correlate this event with a KDC event. - Transited services indicate which intermediate services have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indicates the length of the generated session key. This will be 0 if no session key was requested.
Security	Audit Success	12544	2015-04-24 18:00:41	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: LTRANPHD$ Account Domain: WORKGROUP Logon ID: 0x3e7 Logon Type: 5 Impersonation Level: %%1833 New Logon: Security ID: S-1-5-20 Account Name: NETWORK SERVICE Account Domain: NT AUTHORITY Logon ID: 0x3e4 Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x230 Process Name: C:\Windows\System32\services.exe Network Information: Workstation Name: Source Network Address: - Source Port: - Detailed Authentication Information: Logon Process: Advapi Authentication Package: Negotiate Transited Services: - Package Name (NTLM only): - Key Length: 0 This event is generated when a logon session is created. It is generated on the computer that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service such as the Server service, or a local process such as Winlogon.exe or Services.exe. The logon type field indicates the kind of logon that occurred. The most common types are 2 (interactive) and 3 (network). The New Logon fields indicate the account for whom the new logon was created, i.e. the account that was logged on. The network fields indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impersonation level field indicates the extent to which a process in the logon session can impersonate. The authentication information fields provide detailed information about this specific logon request. - Logon GUID is a unique identifier that can be used to correlate this event with a KDC event. - Transited services indicate which intermediate services have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indicates the length of the generated session key. This will be 0 if no session key was requested.
Security	Audit Success	12544	2015-04-24 18:00:41	Microsoft-Windows-Security-Auditing	4648: A logon was attempted using explicit credentials. Subject: Security ID: S-1-5-18 Account Name: LTRANPHD$ Account Domain: WORKGROUP Logon ID: 0x3e7 Logon GUID: {00000000-0000-0000-0000-000000000000} Account Whose Credentials Were Used: Account Name: DWM-1 Account Domain: Window Manager Logon GUID: {00000000-0000-0000-0000-000000000000} Target Server: Target Server Name: localhost Additional Information: localhost Process Information: Process ID: 0x200 Process Name: C:\Windows\System32\winlogon.exe Network Information: Network Address: - Port: - This event is generated when a process attempts to log on an account by explicitly specifying that account's credentials. This most commonly occurs in batch-type configurations such as scheduled tasks, or when using the RUNAS command.
Security	Audit Success	12544	2015-04-24 18:00:41	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: LTRANPHD$ Account Domain: WORKGROUP Logon ID: 0x3e7 Logon Type: 2 Impersonation Level: %%1833 New Logon: Security ID: S-1-5-90-1 Account Name: DWM-1 Account Domain: Window Manager Logon ID: 0xc355 Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x200 Process Name: C:\Windows\System32\winlogon.exe Network Information: Workstation Name: Source Network Address: - Source Port: - Detailed Authentication Information: Logon Process: Advapi Authentication Package: Negotiate Transited Services: - Package Name (NTLM only): - Key Length: 0 This event is generated when a logon session is created. It is generated on the computer that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service such as the Server service, or a local process such as Winlogon.exe or Services.exe. The logon type field indicates the kind of logon that occurred. The most common types are 2 (interactive) and 3 (network). The New Logon fields indicate the account for whom the new logon was created, i.e. the account that was logged on. The network fields indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impersonation level field indicates the extent to which a process in the logon session can impersonate. The authentication information fields provide detailed information about this specific logon request. - Logon GUID is a unique identifier that can be used to correlate this event with a KDC event. - Transited services indicate which intermediate services have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indicates the length of the generated session key. This will be 0 if no session key was requested.
					4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: LTRANPHD$ Account Domain: WORKGROUP Logon ID: 0x3e7 Logon Type: 2 Impersonation Level: %%1833 New Logon: Security ID: S-1-5-90-1 Account Name: DWM-1 Account Domain: Window Manager Logon ID: 0xc372 Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x200 Process Name: C:\Windows\System32\winlogon.exe Network Information: Workstation Name: Source Network Address: - Source Port: - Detailed Authentication Information: Logon Process: Advapi Authentication Package: Negotiate Transited Services: - Package Name (NTLM only): - Key Length: 0 This event is generated when a logon session is created. It is generated on the computer that was accessed. The subject fields indicate the account on the

Security	Audit Success	12544	2015-04-24 18:00:41	Microsoft-Windows-Security-Auditing	local system which requested the logon. This is most commonly a service such as the Server service, or a local process such as Winlogon.exe or Services.exe. The logon type field indicates the kind of logon that occurred. The most common types are 2 (interactive) and 3 (network). The New Logon fields indicate the account for whom the new logon was created, i.e. the account that was logged on. The network fields indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impersonation level field indicates the extent to which a process in the logon session can impersonate. The authentication information fields provide detailed information about this specific logon request. - Logon GUID is a unique identifier that can be used to correlate this event with a KDC event. - Transited services indicate which intermediate services have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indicates the length of the generated session key. This will be 0 if no session key was requested.
Security	Audit Success	12548	2015-04-24 18:00:41	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Logon ID: 0x3e7 Privileges: SeAssignPrimaryTokenPrivilege SeTcbPrivilege SeSecurityPrivilege SeTakeOwnershipPrivilege SeLoadDriverPrivilege SeBackupPrivilege SeRestorePrivilege SeDebugPrivilege SeAuditPrivilege SeSystemEnvironmentPrivilege SeImpersonatePrivilege
Security	Audit Success	12548	2015-04-24 18:00:41	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-20 Account Name: NETWORK SERVICE Account Domain: NT AUTHORITY Logon ID: 0x3e4 Privileges: SeAssignPrimaryTokenPrivilege SeAuditPrivilege SeImpersonatePrivilege
Security	Audit Success	12548	2015-04-24 18:00:41	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-90-1 Account Name: DWM-1 Account Domain: Window Manager Logon ID: 0xc355 Privileges: SeAssignPrimaryTokenPrivilege SeAuditPrivilege SeImpersonatePrivilege
Security	Audit Success	12548	2015-04-24 18:00:41	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-90-1 Account Name: DWM-1 Account Domain: Window Manager Logon ID: 0xc372 Privileges: SeAssignPrimaryTokenPrivilege SeAuditPrivilege
Security	Audit Success	13568	2015-04-24 18:00:41	Microsoft-Windows-Security-Auditing	4902: The Per-user audit policy table was created. Number of Elements: 0 Policy ID: 0x7462
Security	Audit Success	12292	2015-04-24 18:00:42	Microsoft-Windows-Security-Auditing	5033: The Windows Firewall Driver started successfully.
Security	Audit Success	12544	2015-04-24 18:00:42	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: LTRANPHD$ Account Domain: WORKGROUP Logon ID: 0x3e7 Logon Type: 5 Impersonation Level: %%1833 New Logon: Security ID: S-1-5-19 Account Name: LOCAL SERVICE Account Domain: NT AUTHORITY Logon ID: 0x3e5 Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x230 Process Name: C:\Windows\System32\services.exe Network Information: Workstation Name: Source Network Address: - Source Port: - Detailed Authentication Information: Logon Process: Advapi Authentication Package: Negotiate Transited Services: - Package Name (NTLM only): - Key Length: 0 This event is generated when a logon session is created. It is generated on the computer that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service such as the Server service, or a local process such as Winlogon.exe or Services.exe. The logon type field indicates the kind of logon that occurred. The most common types are 2 (interactive) and 3 (network). The New Logon fields indicate the account for whom the new logon was created, i.e. the account that was logged on. The network fields indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impersonation level field indicates the extent to which a process in the logon session can impersonate. The authentication information fields provide detailed information about this specific logon request. - Logon GUID is a unique identifier that can be used to correlate this event with a KDC event. - Transited services indicate which intermediate services have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indicates the length of the generated session key. This will be 0 if no session key was requested.
Security	Audit Success	12544	2015-04-24 18:00:42	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: LTRANPHD$ Account Domain: WORKGROUP Logon ID: 0x3e7 Logon Type: 5 Impersonation Level: %%1833 New Logon: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Logon ID: 0x3e7 Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x230 Process Name: C:\Windows\System32\services.exe Network Information: Workstation Name: Source Network Address: - Source Port: - Detailed Authentication Information: Logon Process: Advapi Authentication Package: Negotiate Transited Services: - Package Name (NTLM only): - Key Length: 0 This event is generated when a logon session is created. It is generated on the computer that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service such as the Server service, or a local process such as Winlogon.exe or Services.exe. The logon type field indicates the kind of logon that occurred. The most common types are 2 (interactive) and 3 (network). The New Logon fields indicate the account for whom the new logon was created, i.e. the account that was logged on. The network fields indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impersonation level field indicates the extent to which a process in the logon session can impersonate. The authentication information fields provide detailed information about this specific logon request. - Logon GUID is a unique identifier that can be used to correlate this event with a KDC event. - Transited services indicate which intermediate services have participated in this logon request. - Package name indicates

					which sub-protocol was used among the NTLM protocols. - Key length indicates the length of the generated session key. This will be 0 if no session key was requested.
Security	Audit Success	12544	2015-04-24 18:00:42	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: LTRANPHD$ Account Domain: WORKGROUP Logon ID: 0x3e7 Logon Type: 5 Impersonation Level: %%1833 New Logon: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Logon ID: 0x3e7 Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x230 Process Name: C:\Windows\System32\services.exe Network Information: Workstation Name: Source Network Address: - Source Port: - Detailed Authentication Information: Logon Process: Advapi Authentication Package: Negotiate Transited Services: - Package Name (NTLM only): - Key Length: 0 This event is generated when a logon session is created. It is generated on the computer that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service such as the Server service, or a local process such as Winlogon.exe or Services.exe. The logon type field indicates the kind of logon that occurred. The most common types are 2 (interactive) and 3 (network). The New Logon fields indicate the account for whom the new logon was created, i.e. the account that was logged on. The network fields indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impersonation level field indicates the extent to which a process in the logon session can impersonate. The authentication information fields provide detailed information about this specific logon request. - Logon GUID is a unique identifier that can be used to correlate this event with a KDC event. - Transited services indicate which intermediate services have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indicates the length of the generated session key. This will be 0 if no session key was requested.
Security	Audit Success	12544	2015-04-24 18:00:42	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: LTRANPHD$ Account Domain: WORKGROUP Logon ID: 0x3e7 Logon Type: 5 Impersonation Level: %%1833 New Logon: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Logon ID: 0x3e7 Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x230 Process Name: C:\Windows\System32\services.exe Network Information: Workstation Name: Source Network Address: - Source Port: - Detailed Authentication Information: Logon Process: Advapi Authentication Package: Negotiate Transited Services: - Package Name (NTLM only): - Key Length: 0 This event is generated when a logon session is created. It is generated on the computer that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service such as the Server service, or a local process such as Winlogon.exe or Services.exe. The logon type field indicates the kind of logon that occurred. The most common types are 2 (interactive) and 3 (network). The New Logon fields indicate the account for whom the new logon was created, i.e. the account that was logged on. The network fields indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impersonation level field indicates the extent to which a process in the logon session can impersonate. The authentication information fields provide detailed information about this specific logon request. - Logon GUID is a unique identifier that can be used to correlate this event with a KDC event. - Transited services indicate which intermediate services have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indicates the length of the generated session key. This will be 0 if no session key was requested.
Security	Audit Success	12544	2015-04-24 18:00:42	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: LTRANPHD$ Account Domain: WORKGROUP Logon ID: 0x3e7 Logon Type: 5 Impersonation Level: %%1833 New Logon: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Logon ID: 0x3e7 Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x230 Process Name: C:\Windows\System32\services.exe Network Information: Workstation Name: Source Network Address: - Source Port: - Detailed Authentication Information: Logon Process: Advapi Authentication Package: Negotiate Transited Services: - Package Name (NTLM only): - Key Length: 0 This event is generated when a logon session is created. It is generated on the computer that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service such as the Server service, or a local process such as Winlogon.exe or Services.exe. The logon type field indicates the kind of logon that occurred. The most common types are 2 (interactive) and 3 (network). The New Logon fields indicate the account for whom the new logon was created, i.e. the account that was logged on. The network fields indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impersonation level field indicates the extent to which a process in the logon session can impersonate. The authentication information fields provide detailed information about this specific logon request. - Logon GUID is a unique identifier that can be used to correlate this event with a KDC event. - Transited services indicate which intermediate services have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indicates the length of the generated session key. This will be 0 if no session key was requested.
					4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: LTRANPHD$ Account Domain: WORKGROUP Logon ID: 0x3e7 Logon Type: 5 Impersonation Level: %%1833 New Logon: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Logon ID: 0x3e7 Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x230 Process Name: C:\Windows\System32\services.exe Network Information: Workstation Name: Source Network Address: - Source Port: - Detailed Authentication Information: Logon Process: Advapi Authentication Package: Negotiate Transited Services: - Package Name (NTLM only): - Key Length: 0 This event is generated when a logon session is created. It is generated on the computer that was accessed. The subject fields indicate the account on the local

Security	Audit Success	12544	2015-04-24 18:00:42	Microsoft-Windows-Security-Auditing	system which requested the logon. This is most commonly a service such as the Server service, or a local process such as Winlogon.exe or Services.exe. The logon type field indicates the kind of logon that occurred. The most common types are 2 (interactive) and 3 (network). The New Logon fields indicate the account for whom the new logon was created, i.e. the account that was logged on. The network fields indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impersonation level field indicates the extent to which a process in the logon session can impersonate. The authentication information fields provide detailed information about this specific logon request. - Logon GUID is a unique identifier that can be used to correlate this event with a KDC event. - Transited services indicate which intermediate services have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indicates the length of the generated session key. This will be 0 if no session key was requested.
Security	Audit Success	12544	2015-04-24 18:00:42	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-0-0 Account Name: - Account Domain: - Logon ID: 0x0 Logon Type: 3 Impersonation Level: %%1833 New Logon: Security ID: S-1-5-7 Account Name: ANONYMOUS LOGON Account Domain: NT AUTHORITY Logon ID: 0x17ad7 Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x0 Process Name: - Network Information: Workstation Name: Source Network Address: - Source Port: - Detailed Authentication Information: Logon Process: NtLmSsp Authentication Package: NTLM Transited Services: - Package Name (NTLM only): NTLM V1 Key Length: 0 This event is generated when a logon session is created. It is generated on the computer that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service such as the Server service, or a local process such as Winlogon.exe or Services.exe. The logon type field indicates the kind of logon that occurred. The most common types are 2 (interactive) and 3 (network). The New Logon fields indicate the account for whom the new logon was created, i.e. the account that was logged on. The network fields indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impersonation level field indicates the extent to which a process in the logon session can impersonate. The authentication information fields provide detailed information about this specific logon request. - Logon GUID is a unique identifier that can be used to correlate this event with a KDC event. - Transited services indicate which intermediate services have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indicates the length of the generated session key. This will be 0 if no session key was requested.
Security	Audit Success	12548	2015-04-24 18:00:42	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-19 Account Name: LOCAL SERVICE Account Domain: NT AUTHORITY Logon ID: 0x3e5 Privileges: SeAssignPrimaryTokenPrivilege SeAuditPrivilege SeImpersonatePrivilege
Security	Audit Success	12548	2015-04-24 18:00:42	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Logon ID: 0x3e7 Privileges: SeAssignPrimaryTokenPrivilege SeTcbPrivilege SeSecurityPrivilege SeTakeOwnershipPrivilege SeLoadDriverPrivilege SeBackupPrivilege SeRestorePrivilege SeDebugPrivilege SeAuditPrivilege SeSystemEnvironmentPrivilege SeImpersonatePrivilege
Security	Audit Success	12548	2015-04-24 18:00:42	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Logon ID: 0x3e7 Privileges: SeAssignPrimaryTokenPrivilege SeTcbPrivilege SeSecurityPrivilege SeTakeOwnershipPrivilege SeLoadDriverPrivilege SeBackupPrivilege SeRestorePrivilege SeDebugPrivilege SeAuditPrivilege SeSystemEnvironmentPrivilege SeImpersonatePrivilege
Security	Audit Success	12548	2015-04-24 18:00:42	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Logon ID: 0x3e7 Privileges: SeAssignPrimaryTokenPrivilege SeTcbPrivilege SeSecurityPrivilege SeTakeOwnershipPrivilege SeLoadDriverPrivilege SeBackupPrivilege SeRestorePrivilege SeDebugPrivilege SeAuditPrivilege SeSystemEnvironmentPrivilege SeImpersonatePrivilege
Security	Audit Success	12548	2015-04-24 18:00:42	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Logon ID: 0x3e7 Privileges: SeAssignPrimaryTokenPrivilege SeTcbPrivilege SeSecurityPrivilege SeTakeOwnershipPrivilege SeLoadDriverPrivilege SeBackupPrivilege SeRestorePrivilege SeDebugPrivilege SeAuditPrivilege SeSystemEnvironmentPrivilege SeImpersonatePrivilege
Security	Audit Success	12548	2015-04-24 18:00:42	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Logon ID: 0x3e7 Privileges: SeAssignPrimaryTokenPrivilege SeTcbPrivilege SeSecurityPrivilege SeTakeOwnershipPrivilege SeLoadDriverPrivilege SeBackupPrivilege SeRestorePrivilege SeDebugPrivilege SeAuditPrivilege SeSystemEnvironmentPrivilege SeImpersonatePrivilege
Security	Audit Success	12292	2015-04-24 18:00:43	Microsoft-Windows-Security-Auditing	5024: The Windows Firewall service started successfully.
Security	Audit Success	12544	2015-04-24 18:00:45	Microsoft-Windows-Security-Auditing	4648: A logon was attempted using explicit credentials. Subject: Security ID: S-1-5-18 Account Name: LTRANPHD$ Account Domain: WORKGROUP Logon ID: 0x3e7 Logon GUID: {00000000-0000-0000-0000-000000000000} Account Whose Credentials Were Used: Account Name: Liem Account Domain: LTRANPHD Logon GUID: {00000000-0000-0000-0000-000000000000} Target Server: Target Server Name: localhost Additional Information: localhost Process Information: Process ID: 0x200 Process Name: C:\Windows\System32\winlogon.exe Network Information: Network Address: 127.0.0.1 Port: 0 This event is generated when a process attempts to log on an account by explicitly specifying that account's credentials. This most commonly occurs in batch-type configurations such as scheduled tasks, or when using the RUNAS command.
					4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: LTRANPHD$

Security	Audit Success	12544	2015-04-24 18:00:45	Microsoft-Windows-Security-Auditing	Account Domain: WORKGROUP Logon ID: 0x3e7 Logon Type: 2 Impersonation Level: %%1833 New Logon: Security ID: S-1-5-21-1888849264-3803429180-4108621888-1001 Account Name: Liem Account Domain: LTRANPHD Logon ID: 0x1c3b6 Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x200 Process Name: C:\Windows\System32\winlogon.exe Network Information: Workstation Name: LTRANPHD Source Network Address: 127.0.0.1 Source Port: 0 Detailed Authentication Information: Logon Process: User32 Authentication Package: Negotiate Transited Services: - Package Name (NTLM only): - Key Length: 0 This event is generated when a logon session is created. It is generated on the computer that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service such as the Server service, or a local process such as Winlogon.exe or Services.exe. The logon type field indicates the kind of logon that occurred. The most common types are 2 (interactive) and 3 (network). The New Logon fields indicate the account for whom the new logon was created, i.e. the account that was logged on. The network fields indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impersonation level field indicates the extent to which a process in the logon session can impersonate. The authentication information fields provide detailed information about this specific logon request. - Logon GUID is a unique identifier that can be used to correlate this event with a KDC event. - Transited services indicate which intermediate services have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indicates the length of the generated session key. This will be 0 if no session key was requested.
Security	Audit Success	12544	2015-04-24 18:00:45	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: LTRANPHD$ Account Domain: WORKGROUP Logon ID: 0x3e7 Logon Type: 2 Impersonation Level: %%1833 New Logon: Security ID: S-1-5-21-1888849264-3803429180-4108621888-1001 Account Name: Liem Account Domain: LTRANPHD Logon ID: 0x1c40a Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x200 Process Name: C:\Windows\System32\winlogon.exe Network Information: Workstation Name: LTRANPHD Source Network Address: 127.0.0.1 Source Port: 0 Detailed Authentication Information: Logon Process: User32 Authentication Package: Negotiate Transited Services: - Package Name (NTLM only): - Key Length: 0 This event is generated when a logon session is created. It is generated on the computer that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service such as the Server service, or a local process such as Winlogon.exe or Services.exe. The logon type field indicates the kind of logon that occurred. The most common types are 2 (interactive) and 3 (network). The New Logon fields indicate the account for whom the new logon was created, i.e. the account that was logged on. The network fields indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impersonation level field indicates the extent to which a process in the logon session can impersonate. The authentication information fields provide detailed information about this specific logon request. - Logon GUID is a unique identifier that can be used to correlate this event with a KDC event. - Transited services indicate which intermediate services have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indicates the length of the generated session key. This will be 0 if no session key was requested.
Security	Audit Success	12548	2015-04-24 18:00:45	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-21-1888849264-3803429180-4108621888-1001 Account Name: Liem Account Domain: LTRANPHD Logon ID: 0x1c3b6 Privileges: SeSecurityPrivilege SeTakeOwnershipPrivilege SeLoadDriverPrivilege SeBackupPrivilege SeRestorePrivilege SeDebugPrivilege SeSystemEnvironmentPrivilege SeImpersonatePrivilege
Security	Audit Success	12544	2015-04-24 18:00:46	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: LTRANPHD$ Account Domain: WORKGROUP Logon ID: 0x3e7 Logon Type: 5 Impersonation Level: %%1833 New Logon: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Logon ID: 0x3e7 Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x230 Process Name: C:\Windows\System32\services.exe Network Information: Workstation Name: Source Network Address: - Source Port: - Detailed Authentication Information: Logon Process: Advapi Authentication Package: Negotiate Transited Services: - Package Name (NTLM only): - Key Length: 0 This event is generated when a logon session is created. It is generated on the computer that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service such as the Server service, or a local process such as Winlogon.exe or Services.exe. The logon type field indicates the kind of logon that occurred. The most common types are 2 (interactive) and 3 (network). The New Logon fields indicate the account for whom the new logon was created, i.e. the account that was logged on. The network fields indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impersonation level field indicates the extent to which a process in the logon session can impersonate. The authentication information fields provide detailed information about this specific logon request. - Logon GUID is a unique identifier that can be used to correlate this event with a KDC event. - Transited services indicate which intermediate services have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indicates the length of the generated session key. This will be 0 if no session key was requested.
Security	Audit Success	12548	2015-04-24 18:00:46	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Logon ID: 0x3e7 Privileges: SeAssignPrimaryTokenPrivilege SeTcbPrivilege SeSecurityPrivilege SeTakeOwnershipPrivilege SeLoadDriverPrivilege SeBackupPrivilege SeRestorePrivilege SeDebugPrivilege SeAuditPrivilege SeSystemEnvironmentPrivilege SeImpersonatePrivilege
Security	Audit	13824	2015-04-24	Microsoft-Windows-Security-	4797: An attempt was made to query the existence of a blank password for an account. Subject: Security ID: S-1-5-21-1888849264-3803429180-4108621888-1001 Account Name: Liem Account Domain: LTRANPHD Logon

	Success		18:00:48	Auditing	ID: 0x1c40a Additional Information: Caller Workstation: LTRANPHD Target Account Name: Administrator Target Account Domain: LTRANPHD
Security	Audit Success	13824	2015-04-24 18:00:48	Microsoft-Windows-Security-Auditing	4797: An attempt was made to query the existence of a blank password for an account. Subject: Security ID: S-1-5-21-1888849264-3803429180-4108621888-1001 Account Name: Liem Account Domain: LTRANPHD Logon ID: 0x1c40a Additional Information: Caller Workstation: LTRANPHD Target Account Name: Guest Target Account Domain: LTRANPHD
Security	Audit Success	13824	2015-04-24 18:00:48	Microsoft-Windows-Security-Auditing	4797: An attempt was made to query the existence of a blank password for an account. Subject: Security ID: S-1-5-21-1888849264-3803429180-4108621888-1001 Account Name: Liem Account Domain: LTRANPHD Logon ID: 0x1c40a Additional Information: Caller Workstation: LTRANPHD Target Account Name: Administrator Target Account Domain: LTRANPHD
Security	Audit Success	13824	2015-04-24 18:00:48	Microsoft-Windows-Security-Auditing	4797: An attempt was made to query the existence of a blank password for an account. Subject: Security ID: S-1-5-21-1888849264-3803429180-4108621888-1001 Account Name: Liem Account Domain: LTRANPHD Logon ID: 0x1c40a Additional Information: Caller Workstation: LTRANPHD Target Account Name: Guest Target Account Domain: LTRANPHD
Security	Audit Success	13824	2015-04-24 18:00:50	Microsoft-Windows-Security-Auditing	4797: An attempt was made to query the existence of a blank password for an account. Subject: Security ID: S-1-5-19 Account Name: LOCAL SERVICE Account Domain: NT AUTHORITY Logon ID: 0x3e5 Additional Information: Caller Workstation: LTRANPHD Target Account Name: Administrator Target Account Domain: LTRANPHD
Security	Audit Success	13824	2015-04-24 18:00:50	Microsoft-Windows-Security-Auditing	4797: An attempt was made to query the existence of a blank password for an account. Subject: Security ID: S-1-5-19 Account Name: LOCAL SERVICE Account Domain: NT AUTHORITY Logon ID: 0x3e5 Additional Information: Caller Workstation: LTRANPHD Target Account Name: Administrator Target Account Domain: LTRANPHD
Security	Audit Success	13824	2015-04-24 18:00:50	Microsoft-Windows-Security-Auditing	4797: An attempt was made to query the existence of a blank password for an account. Subject: Security ID: S-1-5-19 Account Name: LOCAL SERVICE Account Domain: NT AUTHORITY Logon ID: 0x3e5 Additional Information: Caller Workstation: LTRANPHD Target Account Name: Guest Target Account Domain: LTRANPHD
Security	Audit Success	13824	2015-04-24 18:00:50	Microsoft-Windows-Security-Auditing	4797: An attempt was made to query the existence of a blank password for an account. Subject: Security ID: S-1-5-19 Account Name: LOCAL SERVICE Account Domain: NT AUTHORITY Logon ID: 0x3e5 Additional Information: Caller Workstation: LTRANPHD Target Account Name: Guest Target Account Domain: LTRANPHD
Security	Audit Success	13824	2015-04-24 18:00:50	Microsoft-Windows-Security-Auditing	4797: An attempt was made to query the existence of a blank password for an account. Subject: Security ID: S-1-5-19 Account Name: LOCAL SERVICE Account Domain: NT AUTHORITY Logon ID: 0x3e5 Additional Information: Caller Workstation: LTRANPHD Target Account Name: Liem Target Account Domain: LTRANPHD
Security	Audit Success	13824	2015-04-24 18:00:50	Microsoft-Windows-Security-Auditing	4797: An attempt was made to query the existence of a blank password for an account. Subject: Security ID: S-1-5-19 Account Name: LOCAL SERVICE Account Domain: NT AUTHORITY Logon ID: 0x3e5 Additional Information: Caller Workstation: LTRANPHD Target Account Name: Liem Target Account Domain: LTRANPHD
Security	Audit Success	13824	2015-04-24 18:00:50	Microsoft-Windows-Security-Auditing	4797: An attempt was made to query the existence of a blank password for an account. Subject: Security ID: S-1-5-19 Account Name: LOCAL SERVICE Account Domain: NT AUTHORITY Logon ID: 0x3e5 Additional Information: Caller Workstation: LTRANPHD Target Account Name: Liem Target Account Domain: LTRANPHD
Security	Audit Success	13824	2015-04-24 18:00:50	Microsoft-Windows-Security-Auditing	4797: An attempt was made to query the existence of a blank password for an account. Subject: Security ID: S-1-5-19 Account Name: LOCAL SERVICE Account Domain: NT AUTHORITY Logon ID: 0x3e5 Additional Information: Caller Workstation: LTRANPHD Target Account Name: Liem Target Account Domain: LTRANPHD
Security	Audit Success	103	2015-04-24 18:10:01	Microsoft-Windows-Eventlog	1100: The event logging service has shut down.
Security	Audit Success	12545	2015-04-24 18:10:01	Microsoft-Windows-Security-Auditing	4647: User initiated logoff: Subject: Security ID: S-1-5-21-1888849264-3803429180-4108621888-1001 Account Name: Liem Account Domain: LTRANPHD Logon ID: 0x1c40a This event is generated when a logoff is initiated. No further user-initiated activity can occur. This event can be interpreted as a logoff event.
Security	Audit Success	12288	2015-04-24 18:10:34	Microsoft-Windows-Security-Auditing	4608: Windows is starting up. This event is logged when LSASS.EXE starts and the auditing subsystem is initialized.
Security	Audit Success	12544	2015-04-24 18:10:34	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-0-0 Account Name: - Account Domain: - Logon ID: 0x0 Logon Type: 0 Impersonation Level: - New Logon: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Logon ID: 0x3e7 Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x4 Process Name: Network Information: Workstation Name: - Source Network Address: - Source Port: - Detailed Authentication Information: Logon Process: - Authentication Package: - Transited Services: - Package Name (NTLM only): - Key Length: 0 This event is generated when a logon session is created. It is generated on the computer that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service such as the Server service, or a local process such as Winlogon.exe or Services.exe. The logon type field indicates the kind of logon that occurred. The most common types are 2 (interactive) and 3 (network). The New Logon fields indicate the account for whom the new logon was created, i.e. the account that was logged on. The network fields indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impersonation level field indicates the extent to which a process in the logon session can impersonate. The authentication information fields provide detailed information about this specific logon request. - Logon GUID is a unique identifier that can be used to correlate this event

					with a KDC event. - Transited services indicate which intermediate services have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indicates the length of the generated session key. This will be 0 if no session key was requested.
Security	Audit Success	12544	2015-04-24 18:10:34	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: LTRANPHD$ Account Domain: WORKGROUP Logon ID: 0x3e7 Logon Type: 5 Impersonation Level: %%1833 New Logon: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Logon ID: 0x3e7 Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x230 Process Name: C:\Windows\System32\services.exe Network Information: Workstation Name: Source Network Address: - Source Port: - Detailed Authentication Information: Logon Process: Advapi Authentication Package: Negotiate Transited Services: - Package Name (NTLM only): - Key Length: 0 This event is generated when a logon session is created. It is generated on the computer that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service such as the Server service, or a local process such as Winlogon.exe or Services.exe. The logon type field indicates the kind of logon that occurred. The most common types are 2 (interactive) and 3 (network). The New Logon fields indicate the account for whom the new logon was created, i.e. the account that was logged on. The network fields indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impersonation level field indicates the extent to which a process in the logon session can impersonate. The authentication information fields provide detailed information about this specific logon request. - Logon GUID is a unique identifier that can be used to correlate this event with a KDC event. - Transited services indicate which intermediate services have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indicates the length of the generated session key. This will be 0 if no session key was requested.
Security	Audit Success	12544	2015-04-24 18:10:34	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: LTRANPHD$ Account Domain: WORKGROUP Logon ID: 0x3e7 Logon Type: 5 Impersonation Level: %%1833 New Logon: Security ID: S-1-5-20 Account Name: NETWORK SERVICE Account Domain: NT AUTHORITY Logon ID: 0x3e4 Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x230 Process Name: C:\Windows\System32\services.exe Network Information: Workstation Name: Source Network Address: - Source Port: - Detailed Authentication Information: Logon Process: Advapi Authentication Package: Negotiate Transited Services: - Package Name (NTLM only): - Key Length: 0 This event is generated when a logon session is created. It is generated on the computer that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service such as the Server service, or a local process such as Winlogon.exe or Services.exe. The logon type field indicates the kind of logon that occurred. The most common types are 2 (interactive) and 3 (network). The New Logon fields indicate the account for whom the new logon was created, i.e. the account that was logged on. The network fields indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impersonation level field indicates the extent to which a process in the logon session can impersonate. The authentication information fields provide detailed information about this specific logon request. - Logon GUID is a unique identifier that can be used to correlate this event with a KDC event. - Transited services indicate which intermediate services have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indicates the length of the generated session key. This will be 0 if no session key was requested.
Security	Audit Success	12544	2015-04-24 18:10:34	Microsoft-Windows-Security-Auditing	4648: A logon was attempted using explicit credentials. Subject: Security ID: S-1-5-18 Account Name: LTRANPHD$ Account Domain: WORKGROUP Logon ID: 0x3e7 Logon GUID: {00000000-0000-0000-0000-000000000000} Account Whose Credentials Were Used: Account Name: DWM-1 Account Domain: Window Manager Logon GUID: {00000000-0000-0000-0000-000000000000} Target Server: Target Server Name: localhost Additional Information: localhost Process Information: Process ID: 0x200 Process Name: C:\Windows\System32\winlogon.exe Network Information: Network Address: - Port: - This event is generated when a process attempts to log on an account by explicitly specifying that account's credentials. This most commonly occurs in batch-type configurations such as scheduled tasks, or when using the RUNAS command.
Security	Audit Success	12544	2015-04-24 18:10:34	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: LTRANPHD$ Account Domain: WORKGROUP Logon ID: 0x3e7 Logon Type: 2 Impersonation Level: %%1833 New Logon: Security ID: S-1-5-90-1 Account Name: DWM-1 Account Domain: Window Manager Logon ID: 0xc365 Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x200 Process Name: C:\Windows\System32\winlogon.exe Network Information: Workstation Name: Source Network Address: - Source Port: - Detailed Authentication Information: Logon Process: Advapi Authentication Package: Negotiate Transited Services: - Package Name (NTLM only): - Key Length: 0 This event is generated when a logon session is created. It is generated on the computer that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service such as the Server service, or a local process such as Winlogon.exe or Services.exe. The logon type field indicates the kind of logon that occurred. The most common types are 2 (interactive) and 3 (network). The New Logon fields indicate the account for whom the new logon was created, i.e. the account that was logged on. The network fields indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impersonation level field indicates the extent to which a process in the logon session can impersonate. The authentication information fields provide detailed information about this specific logon request. - Logon GUID is a unique identifier that can be used to correlate this event with a KDC event. - Transited services indicate which intermediate services have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indicates the length of the generated

					session key. This will be 0 if no session key was requested.
Security	Audit Success	12544	2015-04-24 18:10:34	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: LTRANPHD$ Account Domain: WORKGROUP Logon ID: 0x3e7 Logon Type: 2 Impersonation Level: %%1833 New Logon: Security ID: S-1-5-90-1 Account Name: DWM-1 Account Domain: Window Manager Logon ID: 0xc37d Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x200 Process Name: C:\Windows\System32\winlogon.exe Network Information: Workstation Name: Source Network Address: - Source Port: - Detailed Authentication Information: Logon Process: Advapi Authentication Package: Negotiate Transited Services: - Package Name (NTLM only): - Key Length: 0 This event is generated when a logon session is created. It is generated on the computer that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service such as the Server service, or a local process such as Winlogon.exe or Services.exe. The logon type field indicates the kind of logon that occurred. The most common types are 2 (interactive) and 3 (network). The New Logon fields indicate the account for whom the new logon was created, i.e. the account that was logged on. The network fields indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impersonation level field indicates the extent to which a process in the logon session can impersonate. The authentication information fields provide detailed information about this specific logon request. - Logon GUID is a unique identifier that can be used to correlate this event with a KDC event. - Transited services indicate which intermediate services have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indicates the length of the generated session key. This will be 0 if no session key was requested.
Security	Audit Success	12544	2015-04-24 18:10:34	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: LTRANPHD$ Account Domain: WORKGROUP Logon ID: 0x3e7 Logon Type: 5 Impersonation Level: %%1833 New Logon: Security ID: S-1-5-19 Account Name: LOCAL SERVICE Account Domain: NT AUTHORITY Logon ID: 0x3e5 Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x230 Process Name: C:\Windows\System32\services.exe Network Information: Workstation Name: Source Network Address: - Source Port: - Detailed Authentication Information: Logon Process: Advapi Authentication Package: Negotiate Transited Services: - Package Name (NTLM only): - Key Length: 0 This event is generated when a logon session is created. It is generated on the computer that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service such as the Server service, or a local process such as Winlogon.exe or Services.exe. The logon type field indicates the kind of logon that occurred. The most common types are 2 (interactive) and 3 (network). The New Logon fields indicate the account for whom the new logon was created, i.e. the account that was logged on. The network fields indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impersonation level field indicates the extent to which a process in the logon session can impersonate. The authentication information fields provide detailed information about this specific logon request. - Logon GUID is a unique identifier that can be used to correlate this event with a KDC event. - Transited services indicate which intermediate services have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indicates the length of the generated session key. This will be 0 if no session key was requested.
Security	Audit Success	12544	2015-04-24 18:10:34	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: LTRANPHD$ Account Domain: WORKGROUP Logon ID: 0x3e7 Logon Type: 5 Impersonation Level: %%1833 New Logon: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Logon ID: 0x3e7 Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x230 Process Name: C:\Windows\System32\services.exe Network Information: Workstation Name: Source Network Address: - Source Port: - Detailed Authentication Information: Logon Process: Advapi Authentication Package: Negotiate Transited Services: - Package Name (NTLM only): - Key Length: 0 This event is generated when a logon session is created. It is generated on the computer that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service such as the Server service, or a local process such as Winlogon.exe or Services.exe. The logon type field indicates the kind of logon that occurred. The most common types are 2 (interactive) and 3 (network). The New Logon fields indicate the account for whom the new logon was created, i.e. the account that was logged on. The network fields indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impersonation level field indicates the extent to which a process in the logon session can impersonate. The authentication information fields provide detailed information about this specific logon request. - Logon GUID is a unique identifier that can be used to correlate this event with a KDC event. - Transited services indicate which intermediate services have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indicates the length of the generated session key. This will be 0 if no session key was requested.
			2015-04-		4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: LTRANPHD$ Account Domain: WORKGROUP Logon ID: 0x3e7 Logon Type: 5 Impersonation Level: %%1833 New Logon: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Logon ID: 0x3e7 Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x230 Process Name: C:\Windows\System32\services.exe Network Information: Workstation Name: Source Network Address: - Source Port: - Detailed Authentication Information: Logon Process: Advapi Authentication Package: Negotiate Transited Services: - Package Name (NTLM only): - Key Length: 0 This event is generated when a logon session is created. It is generated on the computer that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service such as the Server service, or a local

Security	Audit Success	12544	24 18:10:34	Microsoft-Windows-Security-Auditing	process such as Winlogon.exe or Services.exe. The logon type field indicates the kind of logon that occurred. The most common types are 2 (interactive) and 3 (network). The New Logon fields indicate the account for whom the new logon was created, i.e. the account that was logged on. The network fields indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impersonation level field indicates the extent to which a process in the logon session can impersonate. The authentication information fields provide detailed information about this specific logon request. - Logon GUID is a unique identifier that can be used to correlate this event with a KDC event. - Transited services indicate which intermediate services have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indicates the length of the generated session key. This will be 0 if no session key was requested.
Security	Audit Success	12548	2015-04-24 18:10:34	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Logon ID: 0x3e7 Privileges: SeAssignPrimaryTokenPrivilege SeTcbPrivilege SeSecurityPrivilege SeTakeOwnershipPrivilege SeLoadDriverPrivilege SeBackupPrivilege SeRestorePrivilege SeDebugPrivilege SeAuditPrivilege SeSystemEnvironmentPrivilege SeImpersonatePrivilege
Security	Audit Success	12548	2015-04-24 18:10:34	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-20 Account Name: NETWORK SERVICE Account Domain: NT AUTHORITY Logon ID: 0x3e4 Privileges: SeAssignPrimaryTokenPrivilege SeAuditPrivilege SeImpersonatePrivilege
Security	Audit Success	12548	2015-04-24 18:10:34	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-90-1 Account Name: DWM-1 Account Domain: Window Manager Logon ID: 0xc365 Privileges: SeAssignPrimaryTokenPrivilege SeAuditPrivilege SeImpersonatePrivilege
Security	Audit Success	12548	2015-04-24 18:10:34	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-90-1 Account Name: DWM-1 Account Domain: Window Manager Logon ID: 0xc37d Privileges: SeAssignPrimaryTokenPrivilege SeAuditPrivilege
Security	Audit Success	12548	2015-04-24 18:10:34	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-19 Account Name: LOCAL SERVICE Account Domain: NT AUTHORITY Logon ID: 0x3e5 Privileges: SeAssignPrimaryTokenPrivilege SeAuditPrivilege SeImpersonatePrivilege
Security	Audit Success	12548	2015-04-24 18:10:34	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Logon ID: 0x3e7 Privileges: SeAssignPrimaryTokenPrivilege SeTcbPrivilege SeSecurityPrivilege SeTakeOwnershipPrivilege SeLoadDriverPrivilege SeBackupPrivilege SeRestorePrivilege SeDebugPrivilege SeAuditPrivilege SeSystemEnvironmentPrivilege SeImpersonatePrivilege
Security	Audit Success	12548	2015-04-24 18:10:34	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Logon ID: 0x3e7 Privileges: SeAssignPrimaryTokenPrivilege SeTcbPrivilege SeSecurityPrivilege SeTakeOwnershipPrivilege SeLoadDriverPrivilege SeBackupPrivilege SeRestorePrivilege SeDebugPrivilege SeAuditPrivilege SeSystemEnvironmentPrivilege SeImpersonatePrivilege
Security	Audit Success	13568	2015-04-24 18:10:34	Microsoft-Windows-Security-Auditing	4902: The Per-user audit policy table was created. Number of Elements: 0 Policy ID: 0x7459
Security	Audit Success	12292	2015-04-24 18:10:35	Microsoft-Windows-Security-Auditing	5033: The Windows Firewall Driver started successfully.
Security	Audit Success	12292	2015-04-24 18:10:35	Microsoft-Windows-Security-Auditing	5024: The Windows Firewall service started successfully.
Security	Audit Success	12544	2015-04-24 18:10:35	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: LTRANPHD$ Account Domain: WORKGROUP Logon ID: 0x3e7 Logon Type: 5 Impersonation Level: %%1833 New Logon: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Logon ID: 0x3e7 Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x230 Process Name: C:\Windows\System32\services.exe Network Information: Workstation Name: Source Network Address: - Source Port: - Detailed Authentication Information: Logon Process: Advapi Authentication Package: Negotiate Transited Services: - Package Name (NTLM only): - Key Length: 0 This event is generated when a logon session is created. It is generated on the computer that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service such as the Server service, or a local process such as Winlogon.exe or Services.exe. The logon type field indicates the kind of logon that occurred. The most common types are 2 (interactive) and 3 (network). The New Logon fields indicate the account for whom the new logon was created, i.e. the account that was logged on. The network fields indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impersonation level field indicates the extent to which a process in the logon session can impersonate. The authentication information fields provide detailed information about this specific logon request. - Logon GUID is a unique identifier that can be used to correlate this event with a KDC event. - Transited services indicate which intermediate services have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indicates the length of the generated session key. This will be 0 if no session key was requested.
					4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: LTRANPHD$ Account Domain: WORKGROUP Logon ID: 0x3e7 Logon Type: 5 Impersonation Level: %%1833 New Logon:

Security	Audit Success	12544	2015-04-24 18:10:35		Microsoft-Windows-Security-Auditing	Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Logon ID: 0x3e7 Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x230 Process Name: C:\Windows\System32\services.exe Network Information: Workstation Name: Source Network Address: - Source Port: - Detailed Authentication Information: Logon Process: Advapi Authentication Package: Negotiate Transited Services: - Package Name (NTLM only): - Key Length: 0 This event is generated when a logon session is created. It is generated on the computer that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service such as the Server service, or a local process such as Winlogon.exe or Services.exe. The logon type field indicates the kind of logon that occurred. The most common types are 2 (interactive) and 3 (network). The New Logon fields indicate the account for whom the new logon was created, i.e. the account that was logged on. The network fields indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impersonation level field indicates the extent to which a process in the logon session can impersonate. The authentication information fields provide detailed information about this specific logon request. - Logon GUID is a unique identifier that can be used to correlate this event with a KDC event. - Transited services indicate which intermediate services have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indicates the length of the generated session key. This will be 0 if no session key was requested.
Security	Audit Success	12544	2015-04-24 18:10:35		Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: LTRANPHD$ Account Domain: WORKGROUP Logon ID: 0x3e7 Logon Type: 5 Impersonation Level: %%1833 New Logon: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Logon ID: 0x3e7 Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x230 Process Name: C:\Windows\System32\services.exe Network Information: Workstation Name: Source Network Address: - Source Port: - Detailed Authentication Information: Logon Process: Advapi Authentication Package: Negotiate Transited Services: - Package Name (NTLM only): - Key Length: 0 This event is generated when a logon session is created. It is generated on the computer that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service such as the Server service, or a local process such as Winlogon.exe or Services.exe. The logon type field indicates the kind of logon that occurred. The most common types are 2 (interactive) and 3 (network). The New Logon fields indicate the account for whom the new logon was created, i.e. the account that was logged on. The network fields indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impersonation level field indicates the extent to which a process in the logon session can impersonate. The authentication information fields provide detailed information about this specific logon request. - Logon GUID is a unique identifier that can be used to correlate this event with a KDC event. - Transited services indicate which intermediate services have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indicates the length of the generated session key. This will be 0 if no session key was requested.
Security	Audit Success	12544	2015-04-24 18:10:35		Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-0-0 Account Name: - Account Domain: - Logon ID: 0x0 Logon Type: 3 Impersonation Level: %%1833 New Logon: Security ID: S-1-5-7 Account Name: ANONYMOUS LOGON Account Domain: NT AUTHORITY Logon ID: 0x15e86 Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x0 Process Name: - Network Information: Workstation Name: Source Network Address: - Source Port: - Detailed Authentication Information: Logon Process: NtLmSsp Authentication Package: NTLM Transited Services: - Package Name (NTLM only): NTLM V1 Key Length: 0 This event is generated when a logon session is created. It is generated on the computer that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service such as the Server service, or a local process such as Winlogon.exe or Services.exe. The logon type field indicates the kind of logon that occurred. The most common types are 2 (interactive) and 3 (network). The New Logon fields indicate the account for whom the new logon was created, i.e. the account that was logged on. The network fields indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impersonation level field indicates the extent to which a process in the logon session can impersonate. The authentication information fields provide detailed information about this specific logon request. - Logon GUID is a unique identifier that can be used to correlate this event with a KDC event. - Transited services indicate which intermediate services have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indicates the length of the generated session key. This will be 0 if no session key was requested.
Security	Audit Success	12548	2015-04-24 18:10:35		Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Logon ID: 0x3e7 Privileges: SeAssignPrimaryTokenPrivilege SeTcbPrivilege SeSecurityPrivilege SeTakeOwnershipPrivilege SeLoadDriverPrivilege SeBackupPrivilege SeRestorePrivilege SeDebugPrivilege SeAuditPrivilege SeSystemEnvironmentPrivilege SeImpersonatePrivilege
Security	Audit Success	12548	2015-04-24 18:10:35		Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Logon ID: 0x3e7 Privileges: SeAssignPrimaryTokenPrivilege SeTcbPrivilege SeSecurityPrivilege SeTakeOwnershipPrivilege SeLoadDriverPrivilege SeBackupPrivilege SeRestorePrivilege SeDebugPrivilege SeAuditPrivilege SeSystemEnvironmentPrivilege SeImpersonatePrivilege
Security	Audit Success	12548	2015-04-24 18:10:35		Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Logon ID: 0x3e7 Privileges: SeAssignPrimaryTokenPrivilege SeTcbPrivilege SeSecurityPrivilege SeTakeOwnershipPrivilege SeLoadDriverPrivilege SeBackupPrivilege SeRestorePrivilege SeDebugPrivilege SeAuditPrivilege SeSystemEnvironmentPrivilege SeImpersonatePrivilege

Security	Audit Success	12544	2015-04-24 18:10:49	Microsoft-Windows-Security-Auditing	4648: A logon was attempted using explicit credentials. Subject: Security ID: S-1-5-18 Account Name: LTRANPHD$ Account Domain: WORKGROUP Logon ID: 0x3e7 Logon GUID: {00000000-0000-0000-0000-000000000000} Account Whose Credentials Were Used: Account Name: Liem Account Domain: LTRANPHD Logon GUID: {00000000-0000-0000-0000-000000000000} Target Server: Target Server Name: localhost Additional Information: localhost Process Information: Process ID: 0x200 Process Name: C:\Windows\System32\winlogon.exe Network Information: Network Address: 127.0.0.1 Port: 0 This event is generated when a process attempts to log on an account by explicitly specifying that account's credentials. This most commonly occurs in batch-type configurations such as scheduled tasks, or when using the RUNAS command.
Security	Audit Success	12544	2015-04-24 18:10:49	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: LTRANPHD$ Account Domain: WORKGROUP Logon ID: 0x3e7 Logon Type: 2 Impersonation Level: %%1833 New Logon: Security ID: S-1-5-21-1888849264-3803429180-4108621888-1001 Account Name: Liem Account Domain: LTRANPHD Logon ID: 0x22ba4 Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x200 Process Name: C:\Windows\System32\winlogon.exe Network Information: Workstation Name: LTRANPHD Source Network Address: 127.0.0.1 Source Port: 0 Detailed Authentication Information: Logon Process: User32 Authentication Package: Negotiate Transited Services: - Package Name (NTLM only): - Key Length: 0 This event is generated when a logon session is created. It is generated on the computer that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service such as the Server service, or a local process such as Winlogon.exe or Services.exe. The logon type field indicates the kind of logon that occurred. The most common types are 2 (interactive) and 3 (network). The New Logon fields indicate the account for whom the new logon was created, i.e. the account that was logged on. The network fields indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impersonation level field indicates the extent to which a process in the logon session can impersonate. The authentication information fields provide detailed information about this specific logon request. - Logon GUID is a unique identifier that can be used to correlate this event with a KDC event. - Transited services indicate which intermediate services have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indicates the length of the generated session key. This will be 0 if no session key was requested.
Security	Audit Success	12544	2015-04-24 18:10:49	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: LTRANPHD$ Account Domain: WORKGROUP Logon ID: 0x3e7 Logon Type: 2 Impersonation Level: %%1833 New Logon: Security ID: S-1-5-21-1888849264-3803429180-4108621888-1001 Account Name: Liem Account Domain: LTRANPHD Logon ID: 0x22c07 Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x200 Process Name: C:\Windows\System32\winlogon.exe Network Information: Workstation Name: LTRANPHD Source Network Address: 127.0.0.1 Source Port: 0 Detailed Authentication Information: Logon Process: User32 Authentication Package: Negotiate Transited Services: - Package Name (NTLM only): - Key Length: 0 This event is generated when a logon session is created. It is generated on the computer that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service such as the Server service, or a local process such as Winlogon.exe or Services.exe. The logon type field indicates the kind of logon that occurred. The most common types are 2 (interactive) and 3 (network). The New Logon fields indicate the account for whom the new logon was created, i.e. the account that was logged on. The network fields indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impersonation level field indicates the extent to which a process in the logon session can impersonate. The authentication information fields provide detailed information about this specific logon request. - Logon GUID is a unique identifier that can be used to correlate this event with a KDC event. - Transited services indicate which intermediate services have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indicates the length of the generated session key. This will be 0 if no session key was requested.
Security	Audit Success	12544	2015-04-24 18:10:49	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: LTRANPHD$ Account Domain: WORKGROUP Logon ID: 0x3e7 Logon Type: 5 Impersonation Level: %%1833 New Logon: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Logon ID: 0x3e7 Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x230 Process Name: C:\Windows\System32\services.exe Network Information: Workstation Name: Source Network Address: - Source Port: - Detailed Authentication Information: Logon Process: Advapi Authentication Package: Negotiate Transited Services: - Package Name (NTLM only): - Key Length: 0 This event is generated when a logon session is created. It is generated on the computer that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service such as the Server service, or a local process such as Winlogon.exe or Services.exe. The logon type field indicates the kind of logon that occurred. The most common types are 2 (interactive) and 3 (network). The New Logon fields indicate the account for whom the new logon was created, i.e. the account that was logged on. The network fields indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impersonation level field indicates the extent to which a process in the logon session can impersonate. The authentication information fields provide detailed information about this specific logon request. - Logon GUID is a unique identifier that can be used to correlate this event with a KDC event. - Transited services indicate which intermediate services have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indicates the length of the generated session key. This will be 0 if no session key was requested.
					4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-21-1888849264-3803429180-

Security	Audit Success	12548	2015-04-24 18:10:49	Microsoft-Windows-Security-Auditing	4108621888-1001 Account Name: Liem Account Domain: LTRANPHD Logon ID: 0x22ba4 Privileges: SeSecurityPrivilege SeTakeOwnershipPrivilege SeLoadDriverPrivilege SeBackupPrivilege SeRestorePrivilege SeDebugPrivilege SeSystemEnvironmentPrivilege SeImpersonatePrivilege
Security	Audit Success	12548	2015-04-24 18:10:49	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Logon ID: 0x3e7 Privileges: SeAssignPrimaryTokenPrivilege SeTcbPrivilege SeSecurityPrivilege SeTakeOwnershipPrivilege SeLoadDriverPrivilege SeBackupPrivilege SeRestorePrivilege SeDebugPrivilege SeAuditPrivilege SeSystemEnvironmentPrivilege SeImpersonatePrivilege
Security	Audit Success	13824	2015-04-24 18:10:50	Microsoft-Windows-Security-Auditing	4797: An attempt was made to query the existence of a blank password for an account. Subject: Security ID: S-1-5-19 Account Name: LOCAL SERVICE Account Domain: NT AUTHORITY Logon ID: 0x3e5 Additional Information: Caller Workstation: LTRANPHD Target Account Name: Administrator Target Account Domain: LTRANPHD
Security	Audit Success	13824	2015-04-24 18:10:50	Microsoft-Windows-Security-Auditing	4797: An attempt was made to query the existence of a blank password for an account. Subject: Security ID: S-1-5-19 Account Name: LOCAL SERVICE Account Domain: NT AUTHORITY Logon ID: 0x3e5 Additional Information: Caller Workstation: LTRANPHD Target Account Name: Guest Target Account Domain: LTRANPHD
Security	Audit Success	13824	2015-04-24 18:10:50	Microsoft-Windows-Security-Auditing	4797: An attempt was made to query the existence of a blank password for an account. Subject: Security ID: S-1-5-19 Account Name: LOCAL SERVICE Account Domain: NT AUTHORITY Logon ID: 0x3e5 Additional Information: Caller Workstation: LTRANPHD Target Account Name: Liem Target Account Domain: LTRANPHD
Security	Audit Success	13824	2015-04-24 18:10:50	Microsoft-Windows-Security-Auditing	4797: An attempt was made to query the existence of a blank password for an account. Subject: Security ID: S-1-5-19 Account Name: LOCAL SERVICE Account Domain: NT AUTHORITY Logon ID: 0x3e5 Additional Information: Caller Workstation: LTRANPHD Target Account Name: Liem Target Account Domain: LTRANPHD
Security	Audit Success	13824	2015-04-24 18:10:50	Microsoft-Windows-Security-Auditing	4797: An attempt was made to query the existence of a blank password for an account. Subject: Security ID: S-1-5-19 Account Name: LOCAL SERVICE Account Domain: NT AUTHORITY Logon ID: 0x3e5 Additional Information: Caller Workstation: LTRANPHD Target Account Name: Administrator Target Account Domain: LTRANPHD
Security	Audit Success	13824	2015-04-24 18:10:50	Microsoft-Windows-Security-Auditing	4797: An attempt was made to query the existence of a blank password for an account. Subject: Security ID: S-1-5-19 Account Name: LOCAL SERVICE Account Domain: NT AUTHORITY Logon ID: 0x3e5 Additional Information: Caller Workstation: LTRANPHD Target Account Name: Guest Target Account Domain: LTRANPHD
Security	Audit Success	13824	2015-04-24 18:10:50	Microsoft-Windows-Security-Auditing	4797: An attempt was made to query the existence of a blank password for an account. Subject: Security ID: S-1-5-19 Account Name: LOCAL SERVICE Account Domain: NT AUTHORITY Logon ID: 0x3e5 Additional Information: Caller Workstation: LTRANPHD Target Account Name: Liem Target Account Domain: LTRANPHD
Security	Audit Success	13824	2015-04-24 18:10:50	Microsoft-Windows-Security-Auditing	4797: An attempt was made to query the existence of a blank password for an account. Subject: Security ID: S-1-5-19 Account Name: LOCAL SERVICE Account Domain: NT AUTHORITY Logon ID: 0x3e5 Additional Information: Caller Workstation: LTRANPHD Target Account Name: Administrator Target Account Domain: LTRANPHD
Security	Audit Success	13824	2015-04-24 18:10:50	Microsoft-Windows-Security-Auditing	4797: An attempt was made to query the existence of a blank password for an account. Subject: Security ID: S-1-5-19 Account Name: LOCAL SERVICE Account Domain: NT AUTHORITY Logon ID: 0x3e5 Additional Information: Caller Workstation: LTRANPHD Target Account Name: Liem Target Account Domain: LTRANPHD
Security	Audit Success	13824	2015-04-24 18:10:50	Microsoft-Windows-Security-Auditing	4797: An attempt was made to query the existence of a blank password for an account. Subject: Security ID: S-1-5-19 Account Name: LOCAL SERVICE Account Domain: NT AUTHORITY Logon ID: 0x3e5 Additional Information: Caller Workstation: LTRANPHD Target Account Name: Administrator Target Account Domain: LTRANPHD
Security	Audit Success	13824	2015-04-24 18:10:50	Microsoft-Windows-Security-Auditing	4797: An attempt was made to query the existence of a blank password for an account. Subject: Security ID: S-1-5-19 Account Name: LOCAL SERVICE Account Domain: NT AUTHORITY Logon ID: 0x3e5 Additional Information: Caller Workstation: LTRANPHD Target Account Name: Guest Target Account Domain: LTRANPHD
Security	Audit Success	13824	2015-04-24 18:10:50	Microsoft-Windows-Security-Auditing	4797: An attempt was made to query the existence of a blank password for an account. Subject: Security ID: S-1-5-19 Account Name: LOCAL SERVICE Account Domain: NT AUTHORITY Logon ID: 0x3e5 Additional Information: Caller Workstation: LTRANPHD Target Account Name: Liem Target Account Domain: LTRANPHD
Security	Audit Success	13824	2015-04-24 18:10:50	Microsoft-Windows-Security-Auditing	4797: An attempt was made to query the existence of a blank password for an account. Subject: Security ID: S-1-5-19 Account Name: LOCAL SERVICE Account Domain: NT AUTHORITY Logon ID: 0x3e5 Additional Information: Caller Workstation: LTRANPHD Target Account Name: Liem Target Account Domain: LTRANPHD
Security	Audit Success	13824	2015-04-24 18:10:50	Microsoft-Windows-Security-Auditing	4797: An attempt was made to query the existence of a blank password for an account. Subject: Security ID: S-1-5-19 Account Name: LOCAL SERVICE Account Domain: NT AUTHORITY Logon ID: 0x3e5 Additional Information: Caller Workstation: LTRANPHD Target Account Name: Administrator Target Account Domain: LTRANPHD
Security	Audit Success	13824	2015-04-24 18:10:50	Microsoft-Windows-Security-Auditing	4797: An attempt was made to query the existence of a blank password for an account. Subject: Security ID: S-1-5-19 Account Name: LOCAL SERVICE Account Domain: NT AUTHORITY Logon ID: 0x3e5 Additional Information: Caller Workstation: LTRANPHD Target Account Name: Guest Target Account Domain: LTRANPHD
Security	Audit Success	13824	2015-04-24 18:10:50	Microsoft-Windows-Security-Auditing	4797: An attempt was made to query the existence of a blank password for an account. Subject: Security ID: S-1-5-19 Account Name: LOCAL SERVICE Account Domain: NT AUTHORITY Logon ID: 0x3e5 Additional Information: Caller Workstation: LTRANPHD Target Account Name: Liem Target Account Domain: LTRANPHD
Security	Audit Success	13824	2015-04-24 18:10:50	Microsoft-Windows-Security-Auditing	4797: An attempt was made to query the existence of a blank password for an account. Subject: Security ID: S-1-5-19 Account Name: LOCAL SERVICE Account Domain: NT AUTHORITY Logon ID: 0x3e5 Additional Information: Caller Workstation: LTRANPHD Target Account Name: Liem Target Account Domain: LTRANPHD

Security	Audit Success	13824	2015-04-24 18:10:51	Microsoft-Windows-Security-Auditing	4797: An attempt was made to query the existence of a blank password for an account. Subject: Security ID: S-1-5-21-1888849264-3803429180-4108621888-1001 Account Name: Liem Account Domain: LTRANPHD Logon ID: 0x22c07 Additional Information: Caller Workstation: LTRANPHD Target Account Name: Administrator Target Account Domain: LTRANPHD
Security	Audit Success	13824	2015-04-24 18:10:51	Microsoft-Windows-Security-Auditing	4797: An attempt was made to query the existence of a blank password for an account. Subject: Security ID: S-1-5-21-1888849264-3803429180-4108621888-1001 Account Name: Liem Account Domain: LTRANPHD Logon ID: 0x22c07 Additional Information: Caller Workstation: LTRANPHD Target Account Name: Guest Target Account Domain: LTRANPHD
Security	Audit Success	13824	2015-04-24 18:10:51	Microsoft-Windows-Security-Auditing	4797: An attempt was made to query the existence of a blank password for an account. Subject: Security ID: S-1-5-21-1888849264-3803429180-4108621888-1001 Account Name: Liem Account Domain: LTRANPHD Logon ID: 0x22c07 Additional Information: Caller Workstation: LTRANPHD Target Account Name: Administrator Target Account Domain: LTRANPHD
Security	Audit Success	13824	2015-04-24 18:10:51	Microsoft-Windows-Security-Auditing	4797: An attempt was made to query the existence of a blank password for an account. Subject: Security ID: S-1-5-21-1888849264-3803429180-4108621888-1001 Account Name: Liem Account Domain: LTRANPHD Logon ID: 0x22c07 Additional Information: Caller Workstation: LTRANPHD Target Account Name: Guest Target Account Domain: LTRANPHD
Security	Audit Success	12544	2015-04-24 18:20:52	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: LTRANPHD$ Account Domain: WORKGROUP Logon ID: 0x3e7 Logon Type: 5 Impersonation Level: %%1833 New Logon: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Logon ID: 0x3e7 Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x230 Process Name: C:\Windows\System32\services.exe Network Information: Workstation Name: Source Network Address: - Source Port: - Detailed Authentication Information: Logon Process: Advapi Authentication Package: Negotiate Transited Services: - Package Name (NTLM only): - Key Length: 0 This event is generated when a logon session is created. It is generated on the computer that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service such as the Server service, or a local process such as Winlogon.exe or Services.exe. The logon type field indicates the kind of logon that occurred. The most common types are 2 (interactive) and 3 (network). The New Logon fields indicate the account for whom the new logon was created, i.e. the account that was logged on. The network fields indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impersonation level field indicates the extent to which a process in the logon session can impersonate. The authentication information fields provide detailed information about this specific logon request. - Logon GUID is a unique identifier that can be used to correlate this event with a KDC event. - Transited services indicate which intermediate services have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indicates the length of the generated session key. This will be 0 if no session key was requested.
Security	Audit Success	12548	2015-04-24 18:20:52	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Logon ID: 0x3e7 Privileges: SeAssignPrimaryTokenPrivilege SeTcbPrivilege SeSecurityPrivilege SeTakeOwnershipPrivilege SeLoadDriverPrivilege SeBackupPrivilege SeRestorePrivilege SeDebugPrivilege SeAuditPrivilege SeSystemEnvironmentPrivilege SeImpersonatePrivilege
Security	Audit Success	13568	2015-04-24 18:20:53	Microsoft-Windows-Security-Auditing	4907: Auditing settings on object were changed. Subject: Security ID: S-1-5-21-1888849264-3803429180-4108621888-1001 Account Name: Liem Account Domain: LTRANPHD Logon ID: 0x22ba4 Object: Object Server: Security Object Type: File Object Name: C:\Users\Liem\AppData\Local\Temp\winre\ExtractedFromWim Handle ID: 0x294 Process Information: Process ID: 0xca4 Process Name: C:\Windows\System32\taskhost.exe Auditing Settings: Original Security Descriptor: New Security Descriptor: S:ARAI(AU;SAFA;DCLCRPCRSDWDWO;;;WD)
Security	Audit Success	12544	2015-04-24 18:20:56	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: LTRANPHD$ Account Domain: WORKGROUP Logon ID: 0x3e7 Logon Type: 5 Impersonation Level: %%1833 New Logon: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Logon ID: 0x3e7 Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x230 Process Name: C:\Windows\System32\services.exe Network Information: Workstation Name: Source Network Address: - Source Port: - Detailed Authentication Information: Logon Process: Advapi Authentication Package: Negotiate Transited Services: - Package Name (NTLM only): - Key Length: 0 This event is generated when a logon session is created. It is generated on the computer that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service such as the Server service, or a local process such as Winlogon.exe or Services.exe. The logon type field indicates the kind of logon that occurred. The most common types are 2 (interactive) and 3 (network). The New Logon fields indicate the account for whom the new logon was created, i.e. the account that was logged on. The network fields indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impersonation level field indicates the extent to which a process in the logon session can impersonate. The authentication information fields provide detailed information about this specific logon request. - Logon GUID is a unique identifier that can be used to correlate this event with a KDC event. - Transited services indicate which intermediate services have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indicates the length of the generated session key. This will be 0 if no session key was requested.
Security	Audit Success	12548	2015-04-24	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Logon ID: 0x3e7 Privileges: SeAssignPrimaryTokenPrivilege SeTcbPrivilege SeSecurityPrivilege SeTakeOwnershipPrivilege SeLoadDriverPrivilege SeBackupPrivilege SeRestorePrivilege

			18:20:56		SeDebugPrivilege SeAuditPrivilege SeSystemEnvironmentPrivilege SeImpersonatePrivilege
Security	Audit Success	12544	2015-04-24 18:22:02	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: LTRANPHD$ Account Domain: WORKGROUP Logon ID: 0x3e7 Logon Type: 5 Impersonation Level: %%1833 New Logon: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Logon ID: 0x3e7 Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x230 Process Name: C:\Windows\System32\services.exe Network Information: Workstation Name: Source Network Address: - Source Port: - Detailed Authentication Information: Logon Process: Advapi Authentication Package: Negotiate Transited Services: - Package Name (NTLM only): - Key Length: 0 This event is generated when a logon session is created. It is generated on the computer that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service such as the Server service, or a local process such as Winlogon.exe or Services.exe. The logon type field indicates the kind of logon that occurred. The most common types are 2 (interactive) and 3 (network). The New Logon fields indicate the account for whom the new logon was created, i.e. the account that was logged on. The network fields indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impersonation level field indicates the extent to which a process in the logon session can impersonate. The authentication information fields provide detailed information about this specific logon request. - Logon GUID is a unique identifier that can be used to correlate this event with a KDC event. - Transited services indicate which intermediate services have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indicates the length of the generated session key. This will be 0 if no session key was requested.
Security	Audit Success	12548	2015-04-24 18:22:02	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Logon ID: 0x3e7 Privileges: SeAssignPrimaryTokenPrivilege SeTcbPrivilege SeSecurityPrivilege SeTakeOwnershipPrivilege SeLoadDriverPrivilege SeBackupPrivilege SeRestorePrivilege SeDebugPrivilege SeAuditPrivilege SeSystemEnvironmentPrivilege SeImpersonatePrivilege
Security	Audit Success	12544	2015-04-24 18:22:03	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: LTRANPHD$ Account Domain: WORKGROUP Logon ID: 0x3e7 Logon Type: 5 Impersonation Level: %%1833 New Logon: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Logon ID: 0x3e7 Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x230 Process Name: C:\Windows\System32\services.exe Network Information: Workstation Name: Source Network Address: - Source Port: - Detailed Authentication Information: Logon Process: Advapi Authentication Package: Negotiate Transited Services: - Package Name (NTLM only): - Key Length: 0 This event is generated when a logon session is created. It is generated on the computer that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service such as the Server service, or a local process such as Winlogon.exe or Services.exe. The logon type field indicates the kind of logon that occurred. The most common types are 2 (interactive) and 3 (network). The New Logon fields indicate the account for whom the new logon was created, i.e. the account that was logged on. The network fields indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impersonation level field indicates the extent to which a process in the logon session can impersonate. The authentication information fields provide detailed information about this specific logon request. - Logon GUID is a unique identifier that can be used to correlate this event with a KDC event. - Transited services indicate which intermediate services have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indicates the length of the generated session key. This will be 0 if no session key was requested.
Security	Audit Success	12548	2015-04-24 18:22:03	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Logon ID: 0x3e7 Privileges: SeAssignPrimaryTokenPrivilege SeTcbPrivilege SeSecurityPrivilege SeTakeOwnershipPrivilege SeLoadDriverPrivilege SeBackupPrivilege SeRestorePrivilege SeDebugPrivilege SeAuditPrivilege SeSystemEnvironmentPrivilege SeImpersonatePrivilege
Security	Audit Success	12544	2015-04-24 18:22:05	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: LTRANPHD$ Account Domain: WORKGROUP Logon ID: 0x3e7 Logon Type: 5 Impersonation Level: %%1833 New Logon: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Logon ID: 0x3e7 Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x230 Process Name: C:\Windows\System32\services.exe Network Information: Workstation Name: Source Network Address: - Source Port: - Detailed Authentication Information: Logon Process: Advapi Authentication Package: Negotiate Transited Services: - Package Name (NTLM only): - Key Length: 0 This event is generated when a logon session is created. It is generated on the computer that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service such as the Server service, or a local process such as Winlogon.exe or Services.exe. The logon type field indicates the kind of logon that occurred. The most common types are 2 (interactive) and 3 (network). The New Logon fields indicate the account for whom the new logon was created, i.e. the account that was logged on. The network fields indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impersonation level field indicates the extent to which a process in the logon session can impersonate. The authentication information fields provide detailed information about this specific logon request. - Logon GUID is a unique identifier that can be used to correlate this event with a KDC event. - Transited services indicate which intermediate services have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indicates the length of the generated session key. This will be 0 if no session key was requested.

Security	Audit Success	12548	2015-04-24 18:22:05	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Logon ID: 0x3e7 Privileges: SeAssignPrimaryTokenPrivilege SeTcbPrivilege SeSecurityPrivilege SeTakeOwnershipPrivilege SeLoadDriverPrivilege SeBackupPrivilege SeRestorePrivilege SeDebugPrivilege SeAuditPrivilege SeSystemEnvironmentPrivilege SeImpersonatePrivilege
Security	Audit Success	12544	2015-04-24 18:22:06	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: LTRANPHD$ Account Domain: WORKGROUP Logon ID: 0x3e7 Logon Type: 5 Impersonation Level: %%1833 New Logon: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Logon ID: 0x3e7 Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x230 Process Name: C:\Windows\System32\services.exe Network Information: Workstation Name: Source Network Address: - Source Port: - Detailed Authentication Information: Logon Process: Advapi Authentication Package: Negotiate Transited Services: - Package Name (NTLM only): - Key Length: 0 This event is generated when a logon session is created. It is generated on the computer that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service such as the Server service, or a local process such as Winlogon.exe or Services.exe. The logon type field indicates the kind of logon that occurred. The most common types are 2 (interactive) and 3 (network). The New Logon fields indicate the account for whom the new logon was created, i.e. the account that was logged on. The network fields indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impersonation level field indicates the extent to which a process in the logon session can impersonate. The authentication information fields provide detailed information about this specific logon request. - Logon GUID is a unique identifier that can be used to correlate this event with a KDC event. - Transited services indicate which intermediate services have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indicates the length of the generated session key. This will be 0 if no session key was requested.
Security	Audit Success	12548	2015-04-24 18:22:06	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Logon ID: 0x3e7 Privileges: SeAssignPrimaryTokenPrivilege SeTcbPrivilege SeSecurityPrivilege SeTakeOwnershipPrivilege SeLoadDriverPrivilege SeBackupPrivilege SeRestorePrivilege SeDebugPrivilege SeAuditPrivilege SeSystemEnvironmentPrivilege SeImpersonatePrivilege
Security	Audit Success	12544	2015-04-24 18:26:11	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: LTRANPHD$ Account Domain: WORKGROUP Logon ID: 0x3e7 Logon Type: 5 Impersonation Level: %%1833 New Logon: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Logon ID: 0x3e7 Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x230 Process Name: C:\Windows\System32\services.exe Network Information: Workstation Name: Source Network Address: - Source Port: - Detailed Authentication Information: Logon Process: Advapi Authentication Package: Negotiate Transited Services: - Package Name (NTLM only): - Key Length: 0 This event is generated when a logon session is created. It is generated on the computer that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service such as the Server service, or a local process such as Winlogon.exe or Services.exe. The logon type field indicates the kind of logon that occurred. The most common types are 2 (interactive) and 3 (network). The New Logon fields indicate the account for whom the new logon was created, i.e. the account that was logged on. The network fields indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impersonation level field indicates the extent to which a process in the logon session can impersonate. The authentication information fields provide detailed information about this specific logon request. - Logon GUID is a unique identifier that can be used to correlate this event with a KDC event. - Transited services indicate which intermediate services have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indicates the length of the generated session key. This will be 0 if no session key was requested.
Security	Audit Success	12548	2015-04-24 18:26:11	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Logon ID: 0x3e7 Privileges: SeAssignPrimaryTokenPrivilege SeTcbPrivilege SeSecurityPrivilege SeTakeOwnershipPrivilege SeLoadDriverPrivilege SeBackupPrivilege SeRestorePrivilege SeDebugPrivilege SeAuditPrivilege SeSystemEnvironmentPrivilege SeImpersonatePrivilege
Security	Audit Success	12288	2015-04-24 19:01:19	Microsoft-Windows-Security-Auditing	4608: Windows is starting up. This event is logged when LSASS.EXE starts and the auditing subsystem is initialized.
Security	Audit Success	12544	2015-04-24 19:01:19	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-0-0 Account Name: - Account Domain: - Logon ID: 0x0 Logon Type: 0 Impersonation Level: - New Logon: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Logon ID: 0x3e7 Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x4 Process Name: Network Information: Workstation Name: - Source Network Address: - Source Port: - Detailed Authentication Information: Logon Process: - Authentication Package: - Transited Services: - Package Name (NTLM only): - Key Length: 0 This event is generated when a logon session is created. It is generated on the computer that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service such as the Server service, or a local process such as Winlogon.exe or Services.exe. The logon type field indicates the kind of logon that occurred. The most common types are 2 (interactive) and 3 (network). The New Logon fields indicate the account for whom the new logon was created, i.e. the account that was logged on. The network fields indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impersonation level field indicates the extent to which a

					process in the logon session can impersonate. The authentication information fields provide detailed information about this specific logon request. - Logon GUID is a unique identifier that can be used to correlate this event with a KDC event. - Transited services indicate which intermediate services have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indicates the length of the generated session key. This will be 0 if no session key was requested.
Security	Audit Success	12544	2015-04-24 19:01:19	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: LTRANPHD$ Account Domain: WORKGROUP Logon ID: 0x3e7 Logon Type: 5 Impersonation Level: %%1833 New Logon: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Logon ID: 0x3e7 Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x238 Process Name: C:\Windows\System32\services.exe Network Information: Workstation Name: Source Network Address: - Source Port: - Detailed Authentication Information: Logon Process: Advapi Authentication Package: Negotiate Transited Services: - Package Name (NTLM only): - Key Length: 0 This event is generated when a logon session is created. It is generated on the computer that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service such as the Server service, or a local process such as Winlogon.exe or Services.exe. The logon type field indicates the kind of logon that occurred. The most common types are 2 (interactive) and 3 (network). The New Logon fields indicate the account for whom the new logon was created, i.e. the account that was logged on. The network fields indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impersonation level field indicates the extent to which a process in the logon session can impersonate. The authentication information fields provide detailed information about this specific logon request. - Logon GUID is a unique identifier that can be used to correlate this event with a KDC event. - Transited services indicate which intermediate services have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indicates the length of the generated session key. This will be 0 if no session key was requested.
Security	Audit Success	12544	2015-04-24 19:01:19	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: LTRANPHD$ Account Domain: WORKGROUP Logon ID: 0x3e7 Logon Type: 5 Impersonation Level: %%1833 New Logon: Security ID: S-1-5-20 Account Name: NETWORK SERVICE Account Domain: NT AUTHORITY Logon ID: 0x3e4 Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x238 Process Name: C:\Windows\System32\services.exe Network Information: Workstation Name: Source Network Address: - Source Port: - Detailed Authentication Information: Logon Process: Advapi Authentication Package: Negotiate Transited Services: - Package Name (NTLM only): - Key Length: 0 This event is generated when a logon session is created. It is generated on the computer that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service such as the Server service, or a local process such as Winlogon.exe or Services.exe. The logon type field indicates the kind of logon that occurred. The most common types are 2 (interactive) and 3 (network). The New Logon fields indicate the account for whom the new logon was created, i.e. the account that was logged on. The network fields indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impersonation level field indicates the extent to which a process in the logon session can impersonate. The authentication information fields provide detailed information about this specific logon request. - Logon GUID is a unique identifier that can be used to correlate this event with a KDC event. - Transited services indicate which intermediate services have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indicates the length of the generated session key. This will be 0 if no session key was requested.
Security	Audit Success	12544	2015-04-24 19:01:19	Microsoft-Windows-Security-Auditing	4648: A logon was attempted using explicit credentials. Subject: Security ID: S-1-5-18 Account Name: LTRANPHD$ Account Domain: WORKGROUP Logon ID: 0x3e7 Logon GUID: {00000000-0000-0000-0000-000000000000} Account Whose Credentials Were Used: Account Name: DWM-1 Account Domain: Window Manager Logon GUID: {00000000-0000-0000-0000-000000000000} Target Server: Target Server Name: localhost Additional Information: localhost Process Information: Process ID: 0x210 Process Name: C:\Windows\System32\winlogon.exe Network Information: Network Address: - Port: - This event is generated when a process attempts to log on an account by explicitly specifying that account's credentials. This most commonly occurs in batch-type configurations such as scheduled tasks, or when using the RUNAS command.
Security	Audit Success	12544	2015-04-24 19:01:19	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: LTRANPHD$ Account Domain: WORKGROUP Logon ID: 0x3e7 Logon Type: 2 Impersonation Level: %%1833 New Logon: Security ID: S-1-5-90-1 Account Name: DWM-1 Account Domain: Window Manager Logon ID: 0xd3b6 Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x210 Process Name: C:\Windows\System32\winlogon.exe Network Information: Workstation Name: Source Network Address: - Source Port: - Detailed Authentication Information: Logon Process: Advapi Authentication Package: Negotiate Transited Services: - Package Name (NTLM only): - Key Length: 0 This event is generated when a logon session is created. It is generated on the computer that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service such as the Server service, or a local process such as Winlogon.exe or Services.exe. The logon type field indicates the kind of logon that occurred. The most common types are 2 (interactive) and 3 (network). The New Logon fields indicate the account for whom the new logon was created, i.e. the account that was logged on. The network fields indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impersonation level field indicates the extent to which a process in the logon session can impersonate. The authentication information fields provide detailed information about this specific logon request. - Logon GUID is a unique identifier that can be used to correlate this event with a KDC event. - Transited

					services indicate which intermediate services have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indicates the length of the generated session key. This will be 0 if no session key was requested.
Security	Audit Success	12544	2015-04-24 19:01:19	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: LTRANPHD$ Account Domain: WORKGROUP Logon ID: 0x3e7 Logon Type: 2 Impersonation Level: %%1833 New Logon: Security ID: S-1-5-90-1 Account Name: DWM-1 Account Domain: Window Manager Logon ID: 0xd3cc Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x210 Process Name: C:\Windows\System32\winlogon.exe Network Information: Workstation Name: Source Network Address: - Source Port: - Detailed Authentication Information: Logon Process: Advapi Authentication Package: Negotiate Transited Services: - Package Name (NTLM only): - Key Length: 0 This event is generated when a logon session is created. It is generated on the computer that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service such as the Server service, or a local process such as Winlogon.exe or Services.exe. The logon type field indicates the kind of logon that occurred. The most common types are 2 (interactive) and 3 (network). The New Logon fields indicate the account for whom the new logon was created, i.e. the account that was logged on. The network fields indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impersonation level field indicates the extent to which a process in the logon session can impersonate. The authentication information fields provide detailed information about this specific logon request. - Logon GUID is a unique identifier that can be used to correlate this event with a KDC event. - Transited services indicate which intermediate services have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indicates the length of the generated session key. This will be 0 if no session key was requested.
Security	Audit Success	12544	2015-04-24 19:01:19	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: LTRANPHD$ Account Domain: WORKGROUP Logon ID: 0x3e7 Logon Type: 5 Impersonation Level: %%1833 New Logon: Security ID: S-1-5-19 Account Name: LOCAL SERVICE Account Domain: NT AUTHORITY Logon ID: 0x3e5 Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x238 Process Name: C:\Windows\System32\services.exe Network Information: Workstation Name: Source Network Address: - Source Port: - Detailed Authentication Information: Logon Process: Advapi Authentication Package: Negotiate Transited Services: - Package Name (NTLM only): - Key Length: 0 This event is generated when a logon session is created. It is generated on the computer that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service such as the Server service, or a local process such as Winlogon.exe or Services.exe. The logon type field indicates the kind of logon that occurred. The most common types are 2 (interactive) and 3 (network). The New Logon fields indicate the account for whom the new logon was created, i.e. the account that was logged on. The network fields indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impersonation level field indicates the extent to which a process in the logon session can impersonate. The authentication information fields provide detailed information about this specific logon request. - Logon GUID is a unique identifier that can be used to correlate this event with a KDC event. - Transited services indicate which intermediate services have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indicates the length of the generated session key. This will be 0 if no session key was requested.
Security	Audit Success	12544	2015-04-24 19:01:19	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: LTRANPHD$ Account Domain: WORKGROUP Logon ID: 0x3e7 Logon Type: 5 Impersonation Level: %%1833 New Logon: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Logon ID: 0x3e7 Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x238 Process Name: C:\Windows\System32\services.exe Network Information: Workstation Name: Source Network Address: - Source Port: - Detailed Authentication Information: Logon Process: Advapi Authentication Package: Negotiate Transited Services: - Package Name (NTLM only): - Key Length: 0 This event is generated when a logon session is created. It is generated on the computer that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service such as the Server service, or a local process such as Winlogon.exe or Services.exe. The logon type field indicates the kind of logon that occurred. The most common types are 2 (interactive) and 3 (network). The New Logon fields indicate the account for whom the new logon was created, i.e. the account that was logged on. The network fields indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impersonation level field indicates the extent to which a process in the logon session can impersonate. The authentication information fields provide detailed information about this specific logon request. - Logon GUID is a unique identifier that can be used to correlate this event with a KDC event. - Transited services indicate which intermediate services have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indicates the length of the generated session key. This will be 0 if no session key was requested.
					4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: LTRANPHD$ Account Domain: WORKGROUP Logon ID: 0x3e7 Logon Type: 5 Impersonation Level: %%1833 New Logon: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Logon ID: 0x3e7 Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x238 Process Name: C:\Windows\System32\services.exe Network Information: Workstation Name: Source Network Address: - Source Port: - Detailed Authentication Information: Logon Process: Advapi Authentication Package: Negotiate Transited Services: - Package Name (NTLM only): - Key Length: 0 This event is generated when a logon session is

Security	Audit Success	12544	2015-04-24 19:01:19	Microsoft-Windows-Security-Auditing	created. It is generated on the computer that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service such as the Server service, or a local process such as Winlogon.exe or Services.exe. The logon type field indicates the kind of logon that occurred. The most common types are 2 (interactive) and 3 (network). The New Logon fields indicate the account for whom the new logon was created, i.e. the account that was logged on. The network fields indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impersonation level field indicates the extent to which a process in the logon session can impersonate. The authentication information fields provide detailed information about this specific logon request. - Logon GUID is a unique identifier that can be used to correlate this event with a KDC event. - Transited services indicate which intermediate services have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indicates the length of the generated session key. This will be 0 if no session key was requested.
Security	Audit Success	12548	2015-04-24 19:01:19	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Logon ID: 0x3e7 Privileges: SeAssignPrimaryTokenPrivilege SeTcbPrivilege SeSecurityPrivilege SeTakeOwnershipPrivilege SeLoadDriverPrivilege SeBackupPrivilege SeRestorePrivilege SeDebugPrivilege SeAuditPrivilege SeSystemEnvironmentPrivilege SeImpersonatePrivilege
Security	Audit Success	12548	2015-04-24 19:01:19	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-20 Account Name: NETWORK SERVICE Account Domain: NT AUTHORITY Logon ID: 0x3e4 Privileges: SeAssignPrimaryTokenPrivilege SeAuditPrivilege SeImpersonatePrivilege
Security	Audit Success	12548	2015-04-24 19:01:19	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-90-1 Account Name: DWM-1 Account Domain: Window Manager Logon ID: 0xd3b6 Privileges: SeAssignPrimaryTokenPrivilege SeAuditPrivilege SeImpersonatePrivilege
Security	Audit Success	12548	2015-04-24 19:01:19	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-90-1 Account Name: DWM-1 Account Domain: Window Manager Logon ID: 0xd3cc Privileges: SeAssignPrimaryTokenPrivilege SeAuditPrivilege
Security	Audit Success	12548	2015-04-24 19:01:19	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-19 Account Name: LOCAL SERVICE Account Domain: NT AUTHORITY Logon ID: 0x3e5 Privileges: SeAssignPrimaryTokenPrivilege SeAuditPrivilege SeImpersonatePrivilege
Security	Audit Success	12548	2015-04-24 19:01:19	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Logon ID: 0x3e7 Privileges: SeAssignPrimaryTokenPrivilege SeTcbPrivilege SeSecurityPrivilege SeTakeOwnershipPrivilege SeLoadDriverPrivilege SeBackupPrivilege SeRestorePrivilege SeDebugPrivilege SeAuditPrivilege SeSystemEnvironmentPrivilege SeImpersonatePrivilege
Security	Audit Success	12548	2015-04-24 19:01:19	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Logon ID: 0x3e7 Privileges: SeAssignPrimaryTokenPrivilege SeTcbPrivilege SeSecurityPrivilege SeTakeOwnershipPrivilege SeLoadDriverPrivilege SeBackupPrivilege SeRestorePrivilege SeDebugPrivilege SeAuditPrivilege SeSystemEnvironmentPrivilege SeImpersonatePrivilege
Security	Audit Success	13568	2015-04-24 19:01:19	Microsoft-Windows-Security-Auditing	4902: The Per-user audit policy table was created. Number of Elements: 0 Policy ID: 0x8442
Security	Audit Success	12544	2015-04-24 19:01:20	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: LTRANPHD$ Account Domain: WORKGROUP Logon ID: 0x3e7 Logon Type: 5 Impersonation Level: %%1833 New Logon: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Logon ID: 0x3e7 Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x238 Process Name: C:\Windows\System32\services.exe Network Information: Workstation Name: Source Network Address: - Source Port: - Detailed Authentication Information: Logon Process: Advapi Authentication Package: Negotiate Transited Services: - Package Name (NTLM only): - Key Length: 0 This event is generated when a logon session is created. It is generated on the computer that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service such as the Server service, or a local process such as Winlogon.exe or Services.exe. The logon type field indicates the kind of logon that occurred. The most common types are 2 (interactive) and 3 (network). The New Logon fields indicate the account for whom the new logon was created, i.e. the account that was logged on. The network fields indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impersonation level field indicates the extent to which a process in the logon session can impersonate. The authentication information fields provide detailed information about this specific logon request. - Logon GUID is a unique identifier that can be used to correlate this event with a KDC event. - Transited services indicate which intermediate services have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indicates the length of the generated session key. This will be 0 if no session key was requested.
Security	Audit Success	12548	2015-04-24 19:01:20	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Logon ID: 0x3e7 Privileges: SeAssignPrimaryTokenPrivilege SeTcbPrivilege SeSecurityPrivilege SeTakeOwnershipPrivilege SeLoadDriverPrivilege SeBackupPrivilege SeRestorePrivilege SeDebugPrivilege SeAuditPrivilege SeSystemEnvironmentPrivilege SeImpersonatePrivilege
Security	Audit Success	12292	2015-04-24 19:01:22	Microsoft-Windows-Security-Auditing	5033: The Windows Firewall Driver started successfully.

Security	Audit Success	12544	2015-04-24 19:01:22	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: LTRANPHD$ Account Domain: WORKGROUP Logon ID: 0x3e7 Logon Type: 5 Impersonation Level: %%1833 New Logon: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Logon ID: 0x3e7 Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x238 Process Name: C:\Windows\System32\services.exe Network Information: Workstation Name: Source Network Address: - Source Port: - Detailed Authentication Information: Logon Process: Advapi Authentication Package: Negotiate Transited Services: - Package Name (NTLM only): - Key Length: 0 This event is generated when a logon session is created. It is generated on the computer that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service such as the Server service, or a local process such as Winlogon.exe or Services.exe. The logon type field indicates the kind of logon that occurred. The most common types are 2 (interactive) and 3 (network). The New Logon fields indicate the account for whom the new logon was created, i.e. the account that was logged on. The network fields indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impersonation level field indicates the extent to which a process in the logon session can impersonate. The authentication information fields provide detailed information about this specific logon request. - Logon GUID is a unique identifier that can be used to correlate this event with a KDC event. - Transited services indicate which intermediate services have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indicates the length of the generated session key. This will be 0 if no session key was requested.
Security	Audit Success	12544	2015-04-24 19:01:22	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: LTRANPHD$ Account Domain: WORKGROUP Logon ID: 0x3e7 Logon Type: 5 Impersonation Level: %%1833 New Logon: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Logon ID: 0x3e7 Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x238 Process Name: C:\Windows\System32\services.exe Network Information: Workstation Name: Source Network Address: - Source Port: - Detailed Authentication Information: Logon Process: Advapi Authentication Package: Negotiate Transited Services: - Package Name (NTLM only): - Key Length: 0 This event is generated when a logon session is created. It is generated on the computer that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service such as the Server service, or a local process such as Winlogon.exe or Services.exe. The logon type field indicates the kind of logon that occurred. The most common types are 2 (interactive) and 3 (network). The New Logon fields indicate the account for whom the new logon was created, i.e. the account that was logged on. The network fields indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impersonation level field indicates the extent to which a process in the logon session can impersonate. The authentication information fields provide detailed information about this specific logon request. - Logon GUID is a unique identifier that can be used to correlate this event with a KDC event. - Transited services indicate which intermediate services have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indicates the length of the generated session key. This will be 0 if no session key was requested.
Security	Audit Success	12544	2015-04-24 19:01:22	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: LTRANPHD$ Account Domain: WORKGROUP Logon ID: 0x3e7 Logon Type: 5 Impersonation Level: %%1833 New Logon: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Logon ID: 0x3e7 Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x238 Process Name: C:\Windows\System32\services.exe Network Information: Workstation Name: Source Network Address: - Source Port: - Detailed Authentication Information: Logon Process: Advapi Authentication Package: Negotiate Transited Services: - Package Name (NTLM only): - Key Length: 0 This event is generated when a logon session is created. It is generated on the computer that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service such as the Server service, or a local process such as Winlogon.exe or Services.exe. The logon type field indicates the kind of logon that occurred. The most common types are 2 (interactive) and 3 (network). The New Logon fields indicate the account for whom the new logon was created, i.e. the account that was logged on. The network fields indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impersonation level field indicates the extent to which a process in the logon session can impersonate. The authentication information fields provide detailed information about this specific logon request. - Logon GUID is a unique identifier that can be used to correlate this event with a KDC event. - Transited services indicate which intermediate services have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indicates the length of the generated session key. This will be 0 if no session key was requested.
Security	Audit Success	12548	2015-04-24 19:01:22	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Logon ID: 0x3e7 Privileges: SeAssignPrimaryTokenPrivilege SeTcbPrivilege SeSecurityPrivilege SeTakeOwnershipPrivilege SeLoadDriverPrivilege SeBackupPrivilege SeRestorePrivilege SeDebugPrivilege SeAuditPrivilege SeSystemEnvironmentPrivilege SeImpersonatePrivilege
Security	Audit Success	12548	2015-04-24 19:01:22	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Logon ID: 0x3e7 Privileges: SeAssignPrimaryTokenPrivilege SeTcbPrivilege SeSecurityPrivilege SeTakeOwnershipPrivilege SeLoadDriverPrivilege SeBackupPrivilege SeRestorePrivilege SeDebugPrivilege SeAuditPrivilege SeSystemEnvironmentPrivilege SeImpersonatePrivilege
			2015-04-		4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account

Security	Audit Success	12548	24 19:01:22	Microsoft-Windows-Security-Auditing	Domain: NT AUTHORITY Logon ID: 0x3e7 Privileges: SeAssignPrimaryTokenPrivilege SeTcbPrivilege SeSecurityPrivilege SeTakeOwnershipPrivilege SeLoadDriverPrivilege SeBackupPrivilege SeRestorePrivilege SeDebugPrivilege SeAuditPrivilege SeSystemEnvironmentPrivilege SeImpersonatePrivilege
Security	Audit Success	12292	2015-04-24 19:01:23	Microsoft-Windows-Security-Auditing	5024: The Windows Firewall service started successfully.
Security	Audit Success	12544	2015-04-24 19:01:23	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-0-0 Account Name: - Account Domain: - Logon ID: 0x0 Logon Type: 3 Impersonation Level: %%1833 New Logon: Security ID: S-1-5-7 Account Name: ANONYMOUS LOGON Account Domain: NT AUTHORITY Logon ID: 0x1989c Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x0 Process Name: - Network Information: Workstation Name: Source Network Address: - Source Port: - Detailed Authentication Information: Logon Process: NtLmSsp Authentication Package: NTLM Transited Services: - Package Name (NTLM only): NTLM V1 Key Length: 0 This event is generated when a logon session is created. It is generated on the computer that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service such as the Server service, or a local process such as Winlogon.exe or Services.exe. The logon type field indicates the kind of logon that occurred. The most common types are 2 (interactive) and 3 (network). The New Logon fields indicate the account for whom the new logon was created, i.e. the account that was logged on. The network fields indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impersonation level field indicates the extent to which a process in the logon session can impersonate. The authentication information fields provide detailed information about this specific logon request. - Logon GUID is a unique identifier that can be used to correlate this event with a KDC event. - Transited services indicate which intermediate services have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indicates the length of the generated session key. This will be 0 if no session key was requested.
Security	Audit Success	12544	2015-04-24 19:03:24	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: LTRANPHD$ Account Domain: WORKGROUP Logon ID: 0x3e7 Logon Type: 5 Impersonation Level: %%1833 New Logon: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Logon ID: 0x3e7 Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x238 Process Name: C:\Windows\System32\services.exe Network Information: Workstation Name: Source Network Address: - Source Port: - Detailed Authentication Information: Logon Process: Advapi Authentication Package: Negotiate Transited Services: - Package Name (NTLM only): - Key Length: 0 This event is generated when a logon session is created. It is generated on the computer that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service such as the Server service, or a local process such as Winlogon.exe or Services.exe. The logon type field indicates the kind of logon that occurred. The most common types are 2 (interactive) and 3 (network). The New Logon fields indicate the account for whom the new logon was created, i.e. the account that was logged on. The network fields indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impersonation level field indicates the extent to which a process in the logon session can impersonate. The authentication information fields provide detailed information about this specific logon request. - Logon GUID is a unique identifier that can be used to correlate this event with a KDC event. - Transited services indicate which intermediate services have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indicates the length of the generated session key. This will be 0 if no session key was requested.
Security	Audit Success	12548	2015-04-24 19:03:24	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Logon ID: 0x3e7 Privileges: SeAssignPrimaryTokenPrivilege SeTcbPrivilege SeSecurityPrivilege SeTakeOwnershipPrivilege SeLoadDriverPrivilege SeBackupPrivilege SeRestorePrivilege SeDebugPrivilege SeAuditPrivilege SeSystemEnvironmentPrivilege SeImpersonatePrivilege
Security	Audit Success	12544	2015-04-24 19:06:48	Microsoft-Windows-Security-Auditing	4648: A logon was attempted using explicit credentials. Subject: Security ID: S-1-5-18 Account Name: LTRANPHD$ Account Domain: WORKGROUP Logon ID: 0x3e7 Logon GUID: {00000000-0000-0000-0000-000000000000} Account Whose Credentials Were Used: Account Name: Liem Account Domain: LTRANPHD Logon GUID: {00000000-0000-0000-0000-000000000000} Target Server: Target Server Name: localhost Additional Information: localhost Process Information: Process ID: 0x210 Process Name: C:\Windows\System32\winlogon.exe Network Information: Network Address: 127.0.0.1 Port: 0 This event is generated when a process attempts to log on an account by explicitly specifying that account's credentials. This most commonly occurs in batch-type configurations such as scheduled tasks, or when using the RUNAS command.
Security	Audit Success	12544	2015-04-24	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: LTRANPHD$ Account Domain: WORKGROUP Logon ID: 0x3e7 Logon Type: 2 Impersonation Level: %%1833 New Logon: Security ID: S-1-5-21-1888849264-3803429180-4108621888-1001 Account Name: Liem Account Domain: LTRANPHD Logon ID: 0x3f385 Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x210 Process Name: C:\Windows\System32\winlogon.exe Network Information: Workstation Name: LTRANPHD Source Network Address: 127.0.0.1 Source Port: 0 Detailed Authentication Information: Logon Process: User32 Authentication Package: Negotiate Transited Services: - Package Name (NTLM only): - Key Length: 0 This event is generated when a logon session is created. It is generated on the computer that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service such as the Server service, or a local process such as Winlogon.exe or Services.exe.

			19:06:48		The logon type field indicates the kind of logon that occurred. The most common types are 2 (interactive) and 3 (network). The New Logon fields indicate the account for whom the new logon was created, i.e. the account that was logged on. The network fields indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impersonation level field indicates the extent to which a process in the logon session can impersonate. The authentication information fields provide detailed information about this specific logon request. - Logon GUID is a unique identifier that can be used to correlate this event with a KDC event. - Transited services indicate which intermediate services have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indicates the length of the generated session key. This will be 0 if no session key was requested.
Security	Audit Success	12544	2015-04-24 19:06:48	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: LTRANPHD$ Account Domain: WORKGROUP Logon ID: 0x3e7 Logon Type: 2 Impersonation Level: %%1833 New Logon: Security ID: S-1-5-21-1888849264-3803429180-4108621888-1001 Account Name: Liem Account Domain: LTRANPHD Logon ID: 0x3f3ad Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x210 Process Name: C:\Windows\System32\winlogon.exe Network Information: Workstation Name: LTRANPHD Source Network Address: 127.0.0.1 Source Port: 0 Detailed Authentication Information: Logon Process: User32 Authentication Package: Negotiate Transited Services: - Package Name (NTLM only): - Key Length: 0 This event is generated when a logon session is created. It is generated on the computer that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service such as the Server service, or a local process such as Winlogon.exe or Services.exe. The logon type field indicates the kind of logon that occurred. The most common types are 2 (interactive) and 3 (network). The New Logon fields indicate the account for whom the new logon was created, i.e. the account that was logged on. The network fields indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impersonation level field indicates the extent to which a process in the logon session can impersonate. The authentication information fields provide detailed information about this specific logon request. - Logon GUID is a unique identifier that can be used to correlate this event with a KDC event. - Transited services indicate which intermediate services have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indicates the length of the generated session key. This will be 0 if no session key was requested.
Security	Audit Success	12548	2015-04-24 19:06:48	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-21-1888849264-3803429180-4108621888-1001 Account Name: Liem Account Domain: LTRANPHD Logon ID: 0x3f385 Privileges: SeSecurityPrivilege SeTakeOwnershipPrivilege SeLoadDriverPrivilege SeBackupPrivilege SeRestorePrivilege SeDebugPrivilege SeSystemEnvironmentPrivilege SeImpersonatePrivilege
Security	Audit Success	13824	2015-04-24 19:06:49	Microsoft-Windows-Security-Auditing	4797: An attempt was made to query the existence of a blank password for an account. Subject: Security ID: S-1-5-19 Account Name: LOCAL SERVICE Account Domain: NT AUTHORITY Logon ID: 0x3e5 Additional Information: Caller Workstation: LTRANPHD Target Account Name: Administrator Target Account Domain: LTRANPHD
Security	Audit Success	13824	2015-04-24 19:06:49	Microsoft-Windows-Security-Auditing	4797: An attempt was made to query the existence of a blank password for an account. Subject: Security ID: S-1-5-19 Account Name: LOCAL SERVICE Account Domain: NT AUTHORITY Logon ID: 0x3e5 Additional Information: Caller Workstation: LTRANPHD Target Account Name: Guest Target Account Domain: LTRANPHD
Security	Audit Success	13824	2015-04-24 19:06:49	Microsoft-Windows-Security-Auditing	4797: An attempt was made to query the existence of a blank password for an account. Subject: Security ID: S-1-5-19 Account Name: LOCAL SERVICE Account Domain: NT AUTHORITY Logon ID: 0x3e5 Additional Information: Caller Workstation: LTRANPHD Target Account Name: Liem Target Account Domain: LTRANPHD
Security	Audit Success	13824	2015-04-24 19:06:49	Microsoft-Windows-Security-Auditing	4797: An attempt was made to query the existence of a blank password for an account. Subject: Security ID: S-1-5-19 Account Name: LOCAL SERVICE Account Domain: NT AUTHORITY Logon ID: 0x3e5 Additional Information: Caller Workstation: LTRANPHD Target Account Name: Liem Target Account Domain: LTRANPHD
Security	Audit Success	13824	2015-04-24 19:06:49	Microsoft-Windows-Security-Auditing	4797: An attempt was made to query the existence of a blank password for an account. Subject: Security ID: S-1-5-19 Account Name: LOCAL SERVICE Account Domain: NT AUTHORITY Logon ID: 0x3e5 Additional Information: Caller Workstation: LTRANPHD Target Account Name: Administrator Target Account Domain: LTRANPHD
Security	Audit Success	13824	2015-04-24 19:06:49	Microsoft-Windows-Security-Auditing	4797: An attempt was made to query the existence of a blank password for an account. Subject: Security ID: S-1-5-19 Account Name: LOCAL SERVICE Account Domain: NT AUTHORITY Logon ID: 0x3e5 Additional Information: Caller Workstation: LTRANPHD Target Account Name: Guest Target Account Domain: LTRANPHD
Security	Audit Success	13824	2015-04-24 19:06:49	Microsoft-Windows-Security-Auditing	4797: An attempt was made to query the existence of a blank password for an account. Subject: Security ID: S-1-5-19 Account Name: LOCAL SERVICE Account Domain: NT AUTHORITY Logon ID: 0x3e5 Additional Information: Caller Workstation: LTRANPHD Target Account Name: Liem Target Account Domain: LTRANPHD
Security	Audit Success	13824	2015-04-24 19:06:49	Microsoft-Windows-Security-Auditing	4797: An attempt was made to query the existence of a blank password for an account. Subject: Security ID: S-1-5-19 Account Name: LOCAL SERVICE Account Domain: NT AUTHORITY Logon ID: 0x3e5 Additional Information: Caller Workstation: LTRANPHD Target Account Name: Administrator Target Account Domain: LTRANPHD
Security	Audit Success	13824	2015-04-24 19:06:49	Microsoft-Windows-Security-Auditing	4797: An attempt was made to query the existence of a blank password for an account. Subject: Security ID: S-1-5-19 Account Name: LOCAL SERVICE Account Domain: NT AUTHORITY Logon ID: 0x3e5 Additional Information: Caller Workstation: LTRANPHD Target Account Name: Liem Target Account Domain: LTRANPHD
Security	Audit Success	13824	2015-04-24	Microsoft-Windows-Security-Auditing	4797: An attempt was made to query the existence of a blank password for an account. Subject: Security ID: S-1-5-19 Account Name: LOCAL SERVICE Account Domain: NT AUTHORITY Logon ID: 0x3e5 Additional Information: Caller Workstation: LTRANPHD Target Account Name: Administrator Target Account Domain:

			19:06:49		LTRANPHD
Security	Audit Success	13824	2015-04-24 19:06:49	Microsoft-Windows-Security-Auditing	4797: An attempt was made to query the existence of a blank password for an account. Subject: Security ID: S-1-5-19 Account Name: LOCAL SERVICE Account Domain: NT AUTHORITY Logon ID: 0x3e5 Additional Information: Caller Workstation: LTRANPHD Target Account Name: Guest Target Account Domain: LTRANPHD
Security	Audit Success	13824	2015-04-24 19:06:49	Microsoft-Windows-Security-Auditing	4797: An attempt was made to query the existence of a blank password for an account. Subject: Security ID: S-1-5-19 Account Name: LOCAL SERVICE Account Domain: NT AUTHORITY Logon ID: 0x3e5 Additional Information: Caller Workstation: LTRANPHD Target Account Name: Liem Target Account Domain: LTRANPHD
Security	Audit Success	13824	2015-04-24 19:06:49	Microsoft-Windows-Security-Auditing	4797: An attempt was made to query the existence of a blank password for an account. Subject: Security ID: S-1-5-19 Account Name: LOCAL SERVICE Account Domain: NT AUTHORITY Logon ID: 0x3e5 Additional Information: Caller Workstation: LTRANPHD Target Account Name: Liem Target Account Domain: LTRANPHD
Security	Audit Success	13824	2015-04-24 19:06:49	Microsoft-Windows-Security-Auditing	4797: An attempt was made to query the existence of a blank password for an account. Subject: Security ID: S-1-5-19 Account Name: LOCAL SERVICE Account Domain: NT AUTHORITY Logon ID: 0x3e5 Additional Information: Caller Workstation: LTRANPHD Target Account Name: Administrator Target Account Domain: LTRANPHD
Security	Audit Success	13824	2015-04-24 19:06:49	Microsoft-Windows-Security-Auditing	4797: An attempt was made to query the existence of a blank password for an account. Subject: Security ID: S-1-5-19 Account Name: LOCAL SERVICE Account Domain: NT AUTHORITY Logon ID: 0x3e5 Additional Information: Caller Workstation: LTRANPHD Target Account Name: Guest Target Account Domain: LTRANPHD
Security	Audit Success	13824	2015-04-24 19:06:49	Microsoft-Windows-Security-Auditing	4797: An attempt was made to query the existence of a blank password for an account. Subject: Security ID: S-1-5-19 Account Name: LOCAL SERVICE Account Domain: NT AUTHORITY Logon ID: 0x3e5 Additional Information: Caller Workstation: LTRANPHD Target Account Name: Liem Target Account Domain: LTRANPHD
Security	Audit Success	13824	2015-04-24 19:06:49	Microsoft-Windows-Security-Auditing	4797: An attempt was made to query the existence of a blank password for an account. Subject: Security ID: S-1-5-19 Account Name: LOCAL SERVICE Account Domain: NT AUTHORITY Logon ID: 0x3e5 Additional Information: Caller Workstation: LTRANPHD Target Account Name: Liem Target Account Domain: LTRANPHD
Security	Audit Success	13824	2015-04-24 19:06:50	Microsoft-Windows-Security-Auditing	4797: An attempt was made to query the existence of a blank password for an account. Subject: Security ID: S-1-5-21-1888849264-3803429180-4108621888-1001 Account Name: Liem Account Domain: LTRANPHD Logon ID: 0x3f3ad Additional Information: Caller Workstation: LTRANPHD Target Account Name: Administrator Target Account Domain: LTRANPHD
Security	Audit Success	13824	2015-04-24 19:06:50	Microsoft-Windows-Security-Auditing	4797: An attempt was made to query the existence of a blank password for an account. Subject: Security ID: S-1-5-21-1888849264-3803429180-4108621888-1001 Account Name: Liem Account Domain: LTRANPHD Logon ID: 0x3f3ad Additional Information: Caller Workstation: LTRANPHD Target Account Name: Guest Target Account Domain: LTRANPHD
Security	Audit Success	13824	2015-04-24 19:06:50	Microsoft-Windows-Security-Auditing	4797: An attempt was made to query the existence of a blank password for an account. Subject: Security ID: S-1-5-21-1888849264-3803429180-4108621888-1001 Account Name: Liem Account Domain: LTRANPHD Logon ID: 0x3f3ad Additional Information: Caller Workstation: LTRANPHD Target Account Name: Administrator Target Account Domain: LTRANPHD
Security	Audit Success	13824	2015-04-24 19:06:50	Microsoft-Windows-Security-Auditing	4797: An attempt was made to query the existence of a blank password for an account. Subject: Security ID: S-1-5-21-1888849264-3803429180-4108621888-1001 Account Name: Liem Account Domain: LTRANPHD Logon ID: 0x3f3ad Additional Information: Caller Workstation: LTRANPHD Target Account Name: Guest Target Account Domain: LTRANPHD
Security	Audit Success	12544	2015-04-24 19:08:39	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: LTRANPHD$ Account Domain: WORKGROUP Logon ID: 0x3e7 Logon Type: 5 Impersonation Level: %%1833 New Logon: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Logon ID: 0x3e7 Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x238 Process Name: C:\Windows\System32\services.exe Network Information: Workstation Name: Source Network Address: - Source Port: - Detailed Authentication Information: Logon Process: Advapi Authentication Package: Negotiate Transited Services: - Package Name (NTLM only): - Key Length: 0 This event is generated when a logon session is created. It is generated on the computer that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service such as the Server service, or a local process such as Winlogon.exe or Services.exe. The logon type field indicates the kind of logon that occurred. The most common types are 2 (interactive) and 3 (network). The New Logon fields indicate the account for whom the new logon was created, i.e. the account that was logged on. The network fields indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impersonation level field indicates the extent to which a process in the logon session can impersonate. The authentication information fields provide detailed information about this specific logon request. - Logon GUID is a unique identifier that can be used to correlate this event with a KDC event. - Transited services indicate which intermediate services have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indicates the length of the generated session key. This will be 0 if no session key was requested.
Security	Audit Success	12548	2015-04-24 19:08:39	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Logon ID: 0x3e7 Privileges: SeAssignPrimaryTokenPrivilege SeTcbPrivilege SeSecurityPrivilege SeTakeOwnershipPrivilege SeLoadDriverPrivilege SeBackupPrivilege SeRestorePrivilege SeDebugPrivilege SeAuditPrivilege SeSystemEnvironmentPrivilege SeImpersonatePrivilege
					4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: LTRANPHD$ Account Domain: WORKGROUP Logon ID: 0x3e7 Logon Type: 5 Impersonation Level: %%1833 New Logon:

Security	Audit Success	12544	2015-04-24 19:08:40	Microsoft-Windows-Security-Auditing	Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Logon ID: 0x3e7 Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x238 Process Name: C:\Windows\System32\services.exe Network Information: Workstation Name: Source Network Address: - Source Port: - Detailed Authentication Information: Logon Process: Advapi Authentication Package: Negotiate Transited Services: - Package Name (NTLM only): - Key Length: 0 This event is generated when a logon session is created. It is generated on the computer that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service such as the Server service, or a local process such as Winlogon.exe or Services.exe. The logon type field indicates the kind of logon that occurred. The most common types are 2 (interactive) and 3 (network). The New Logon fields indicate the account for whom the new logon was created, i.e. the account that was logged on. The network fields indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impersonation level field indicates the extent to which a process in the logon session can impersonate. The authentication information fields provide detailed information about this specific logon request. - Logon GUID is a unique identifier that can be used to correlate this event with a KDC event. - Transited services indicate which intermediate services have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indicates the length of the generated session key. This will be 0 if no session key was requested.
Security	Audit Success	12548	2015-04-24 19:08:40	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Logon ID: 0x3e7 Privileges: SeAssignPrimaryTokenPrivilege SeTcbPrivilege SeSecurityPrivilege SeTakeOwnershipPrivilege SeLoadDriverPrivilege SeBackupPrivilege SeRestorePrivilege SeDebugPrivilege SeAuditPrivilege SeSystemEnvironmentPrivilege SeImpersonatePrivilege
Security	Audit Success	12288	2015-04-24 19:37:49	Microsoft-Windows-Security-Auditing	4608: Windows is starting up. This event is logged when LSASS.EXE starts and the auditing subsystem is initialized.
Security	Audit Success	12544	2015-04-24 19:37:49	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-0-0 Account Name: - Account Domain: - Logon ID: 0x0 Logon Type: 0 Impersonation Level: - New Logon: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Logon ID: 0x3e7 Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x4 Process Name: Network Information: Workstation Name: - Source Network Address: - Source Port: - Detailed Authentication Information: Logon Process: - Authentication Package: - Transited Services: - Package Name (NTLM only): - Key Length: 0 This event is generated when a logon session is created. It is generated on the computer that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service such as the Server service, or a local process such as Winlogon.exe or Services.exe. The logon type field indicates the kind of logon that occurred. The most common types are 2 (interactive) and 3 (network). The New Logon fields indicate the account for whom the new logon was created, i.e. the account that was logged on. The network fields indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impersonation level field indicates the extent to which a process in the logon session can impersonate. The authentication information fields provide detailed information about this specific logon request. - Logon GUID is a unique identifier that can be used to correlate this event with a KDC event. - Transited services indicate which intermediate services have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indicates the length of the generated session key. This will be 0 if no session key was requested.
Security	Audit Success	12544	2015-04-24 19:37:49	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: LTRANPHD$ Account Domain: WORKGROUP Logon ID: 0x3e7 Logon Type: 5 Impersonation Level: %%1833 New Logon: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Logon ID: 0x3e7 Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x230 Process Name: C:\Windows\System32\services.exe Network Information: Workstation Name: Source Network Address: - Source Port: - Detailed Authentication Information: Logon Process: Advapi Authentication Package: Negotiate Transited Services: - Package Name (NTLM only): - Key Length: 0 This event is generated when a logon session is created. It is generated on the computer that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service such as the Server service, or a local process such as Winlogon.exe or Services.exe. The logon type field indicates the kind of logon that occurred. The most common types are 2 (interactive) and 3 (network). The New Logon fields indicate the account for whom the new logon was created, i.e. the account that was logged on. The network fields indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impersonation level field indicates the extent to which a process in the logon session can impersonate. The authentication information fields provide detailed information about this specific logon request. - Logon GUID is a unique identifier that can be used to correlate this event with a KDC event. - Transited services indicate which intermediate services have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indicates the length of the generated session key. This will be 0 if no session key was requested.
Security	Audit Success	12544	2015-04-24 19:37:49	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: LTRANPHD$ Account Domain: WORKGROUP Logon ID: 0x3e7 Logon Type: 5 Impersonation Level: %%1833 New Logon: Security ID: S-1-5-20 Account Name: NETWORK SERVICE Account Domain: NT AUTHORITY Logon ID: 0x3e4 Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x230 Process Name: C:\Windows\System32\services.exe Network Information: Workstation Name: Source Network Address: -

Security	Audit Success	12544	2015-04-24 19:37:49	Microsoft-Windows-Security-Auditing	Source Port: - Detailed Authentication Information: Logon Process: Advapi Authentication Package: Negotiate Transited Services: - Package Name (NTLM only): - Key Length: 0 This event is generated when a logon session is created. It is generated on the computer that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service such as the Server service, or a local process such as Winlogon.exe or Services.exe. The logon type field indicates the kind of logon that occurred. The most common types are 2 (interactive) and 3 (network). The New Logon fields indicate the account for whom the new logon was created, i.e. the account that was logged on. The network fields indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impersonation level field indicates the extent to which a process in the logon session can impersonate. The authentication information fields provide detailed information about this specific logon request. - Logon GUID is a unique identifier that can be used to correlate this event with a KDC event. - Transited services indicate which intermediate services have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indicates the length of the generated session key. This will be 0 if no session key was requested.
Security	Audit Success	12544	2015-04-24 19:37:49	Microsoft-Windows-Security-Auditing	4648: A logon was attempted using explicit credentials. Subject: Security ID: S-1-5-18 Account Name: LTRANPHD$ Account Domain: WORKGROUP Logon ID: 0x3e7 Logon GUID: {00000000-0000-0000-0000-000000000000} Account Whose Credentials Were Used: Account Name: DWM-1 Account Domain: Window Manager Logon GUID: {00000000-0000-0000-0000-000000000000} Target Server: Target Server Name: localhost Additional Information: localhost Process Information: Process ID: 0x200 Process Name: C:\Windows\System32\winlogon.exe Network Information: Network Address: - Port: - This event is generated when a process attempts to log on an account by explicitly specifying that account's credentials. This most commonly occurs in batch-type configurations such as scheduled tasks, or when using the RUNAS command.
Security	Audit Success	12544	2015-04-24 19:37:49	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: LTRANPHD$ Account Domain: WORKGROUP Logon ID: 0x3e7 Logon Type: 2 Impersonation Level: %%1833 New Logon: Security ID: S-1-5-90-1 Account Name: DWM-1 Account Domain: Window Manager Logon ID: 0xc5c6 Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x200 Process Name: C:\Windows\System32\winlogon.exe Network Information: Workstation Name: Source Network Address: - Source Port: - Detailed Authentication Information: Logon Process: Advapi Authentication Package: Negotiate Transited Services: - Package Name (NTLM only): - Key Length: 0 This event is generated when a logon session is created. It is generated on the computer that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service such as the Server service, or a local process such as Winlogon.exe or Services.exe. The logon type field indicates the kind of logon that occurred. The most common types are 2 (interactive) and 3 (network). The New Logon fields indicate the account for whom the new logon was created, i.e. the account that was logged on. The network fields indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impersonation level field indicates the extent to which a process in the logon session can impersonate. The authentication information fields provide detailed information about this specific logon request. - Logon GUID is a unique identifier that can be used to correlate this event with a KDC event. - Transited services indicate which intermediate services have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indicates the length of the generated session key. This will be 0 if no session key was requested.
Security	Audit Success	12544	2015-04-24 19:37:49	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: LTRANPHD$ Account Domain: WORKGROUP Logon ID: 0x3e7 Logon Type: 2 Impersonation Level: %%1833 New Logon: Security ID: S-1-5-90-1 Account Name: DWM-1 Account Domain: Window Manager Logon ID: 0xc5e1 Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x200 Process Name: C:\Windows\System32\winlogon.exe Network Information: Workstation Name: Source Network Address: - Source Port: - Detailed Authentication Information: Logon Process: Advapi Authentication Package: Negotiate Transited Services: - Package Name (NTLM only): - Key Length: 0 This event is generated when a logon session is created. It is generated on the computer that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service such as the Server service, or a local process such as Winlogon.exe or Services.exe. The logon type field indicates the kind of logon that occurred. The most common types are 2 (interactive) and 3 (network). The New Logon fields indicate the account for whom the new logon was created, i.e. the account that was logged on. The network fields indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impersonation level field indicates the extent to which a process in the logon session can impersonate. The authentication information fields provide detailed information about this specific logon request. - Logon GUID is a unique identifier that can be used to correlate this event with a KDC event. - Transited services indicate which intermediate services have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indicates the length of the generated session key. This will be 0 if no session key was requested.
					4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: LTRANPHD$ Account Domain: WORKGROUP Logon ID: 0x3e7 Logon Type: 5 Impersonation Level: %%1833 New Logon: Security ID: S-1-5-19 Account Name: LOCAL SERVICE Account Domain: NT AUTHORITY Logon ID: 0x3e5 Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x230 Process Name: C:\Windows\System32\services.exe Network Information: Workstation Name: Source Network Address: - Source Port: - Detailed Authentication Information: Logon Process: Advapi Authentication Package: Negotiate Transited Services: - Package Name (NTLM only): - Key Length: 0 This event is generated when a logon session is

Security	Audit Success	12544	2015-04-24 19:37:49	Microsoft-Windows-Security-Auditing	created. It is generated on the computer that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service such as the Server service, or a local process such as Winlogon.exe or Services.exe. The logon type field indicates the kind of logon that occurred. The most common types are 2 (interactive) and 3 (network). The New Logon fields indicate the account for whom the new logon was created, i.e. the account that was logged on. The network fields indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impersonation level field indicates the extent to which a process in the logon session can impersonate. The authentication information fields provide detailed information about this specific logon request. - Logon GUID is a unique identifier that can be used to correlate this event with a KDC event. - Transited services indicate which intermediate services have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indicates the length of the generated session key. This will be 0 if no session key was requested.
Security	Audit Success	12544	2015-04-24 19:37:49	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: LTRANPHD$ Account Domain: WORKGROUP Logon ID: 0x3e7 Logon Type: 5 Impersonation Level: %%1833 New Logon: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Logon ID: 0x3e7 Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x230 Process Name: C:\Windows\System32\services.exe Network Information: Workstation Name: Source Network Address: - Source Port: - Detailed Authentication Information: Logon Process: Advapi Authentication Package: Negotiate Transited Services: - Package Name (NTLM only): - Key Length: 0 This event is generated when a logon session is created. It is generated on the computer that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service such as the Server service, or a local process such as Winlogon.exe or Services.exe. The logon type field indicates the kind of logon that occurred. The most common types are 2 (interactive) and 3 (network). The New Logon fields indicate the account for whom the new logon was created, i.e. the account that was logged on. The network fields indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impersonation level field indicates the extent to which a process in the logon session can impersonate. The authentication information fields provide detailed information about this specific logon request. - Logon GUID is a unique identifier that can be used to correlate this event with a KDC event. - Transited services indicate which intermediate services have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indicates the length of the generated session key. This will be 0 if no session key was requested.
Security	Audit Success	12544	2015-04-24 19:37:49	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: LTRANPHD$ Account Domain: WORKGROUP Logon ID: 0x3e7 Logon Type: 5 Impersonation Level: %%1833 New Logon: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Logon ID: 0x3e7 Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x230 Process Name: C:\Windows\System32\services.exe Network Information: Workstation Name: Source Network Address: - Source Port: - Detailed Authentication Information: Logon Process: Advapi Authentication Package: Negotiate Transited Services: - Package Name (NTLM only): - Key Length: 0 This event is generated when a logon session is created. It is generated on the computer that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service such as the Server service, or a local process such as Winlogon.exe or Services.exe. The logon type field indicates the kind of logon that occurred. The most common types are 2 (interactive) and 3 (network). The New Logon fields indicate the account for whom the new logon was created, i.e. the account that was logged on. The network fields indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impersonation level field indicates the extent to which a process in the logon session can impersonate. The authentication information fields provide detailed information about this specific logon request. - Logon GUID is a unique identifier that can be used to correlate this event with a KDC event. - Transited services indicate which intermediate services have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indicates the length of the generated session key. This will be 0 if no session key was requested.
Security	Audit Success	12548	2015-04-24 19:37:49	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Logon ID: 0x3e7 Privileges: SeAssignPrimaryTokenPrivilege SeTcbPrivilege SeSecurityPrivilege SeTakeOwnershipPrivilege SeLoadDriverPrivilege SeBackupPrivilege SeRestorePrivilege SeDebugPrivilege SeAuditPrivilege SeSystemEnvironmentPrivilege SeImpersonatePrivilege
Security	Audit Success	12548	2015-04-24 19:37:49	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-20 Account Name: NETWORK SERVICE Account Domain: NT AUTHORITY Logon ID: 0x3e4 Privileges: SeAssignPrimaryTokenPrivilege SeAuditPrivilege SeImpersonatePrivilege
Security	Audit Success	12548	2015-04-24 19:37:49	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-90-1 Account Name: DWM-1 Account Domain: Window Manager Logon ID: 0xc5c6 Privileges: SeAssignPrimaryTokenPrivilege SeAuditPrivilege SeImpersonatePrivilege
Security	Audit Success	12548	2015-04-24 19:37:49	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-90-1 Account Name: DWM-1 Account Domain: Window Manager Logon ID: 0xc5e1 Privileges: SeAssignPrimaryTokenPrivilege SeAuditPrivilege
Security	Audit Success	12548	2015-04-24 19:37:49	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-19 Account Name: LOCAL SERVICE Account Domain: NT AUTHORITY Logon ID: 0x3e5 Privileges: SeAssignPrimaryTokenPrivilege SeAuditPrivilege SeImpersonatePrivilege

Security	Audit Success	12548	2015-04-24 19:37:49	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Logon ID: 0x3e7 Privileges: SeAssignPrimaryTokenPrivilege SeTcbPrivilege SeSecurityPrivilege SeTakeOwnershipPrivilege SeLoadDriverPrivilege SeBackupPrivilege SeRestorePrivilege SeDebugPrivilege SeAuditPrivilege SeSystemEnvironmentPrivilege SeImpersonatePrivilege
Security	Audit Success	12548	2015-04-24 19:37:49	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Logon ID: 0x3e7 Privileges: SeAssignPrimaryTokenPrivilege SeTcbPrivilege SeSecurityPrivilege SeTakeOwnershipPrivilege SeLoadDriverPrivilege SeBackupPrivilege SeRestorePrivilege SeDebugPrivilege SeAuditPrivilege SeSystemEnvironmentPrivilege SeImpersonatePrivilege
Security	Audit Success	13568	2015-04-24 19:37:49	Microsoft-Windows-Security-Auditing	4902: The Per-user audit policy table was created. Number of Elements: 0 Policy ID: 0x7653
Security	Audit Success	12292	2015-04-24 19:37:51	Microsoft-Windows-Security-Auditing	5033: The Windows Firewall Driver started successfully.
Security	Audit Success	12292	2015-04-24 19:37:51	Microsoft-Windows-Security-Auditing	5024: The Windows Firewall service started successfully.
Security	Audit Success	12544	2015-04-24 19:37:51	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: LTRANPHD$ Account Domain: WORKGROUP Logon ID: 0x3e7 Logon Type: 5 Impersonation Level: %%1833 New Logon: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Logon ID: 0x3e7 Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x230 Process Name: C:\Windows\System32\services.exe Network Information: Workstation Name: Source Network Address: - Source Port: - Detailed Authentication Information: Logon Process: Advapi Authentication Package: Negotiate Transited Services: - Package Name (NTLM only): - Key Length: 0 This event is generated when a logon session is created. It is generated on the computer that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service such as the Server service, or a local process such as Winlogon.exe or Services.exe. The logon type field indicates the kind of logon that occurred. The most common types are 2 (interactive) and 3 (network). The New Logon fields indicate the account for whom the new logon was created, i.e. the account that was logged on. The network fields indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impersonation level field indicates the extent to which a process in the logon session can impersonate. The authentication information fields provide detailed information about this specific logon request. - Logon GUID is a unique identifier that can be used to correlate this event with a KDC event. - Transited services indicate which intermediate services have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indicates the length of the generated session key. This will be 0 if no session key was requested.
Security	Audit Success	12544	2015-04-24 19:37:51	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: LTRANPHD$ Account Domain: WORKGROUP Logon ID: 0x3e7 Logon Type: 5 Impersonation Level: %%1833 New Logon: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Logon ID: 0x3e7 Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x230 Process Name: C:\Windows\System32\services.exe Network Information: Workstation Name: Source Network Address: - Source Port: - Detailed Authentication Information: Logon Process: Advapi Authentication Package: Negotiate Transited Services: - Package Name (NTLM only): - Key Length: 0 This event is generated when a logon session is created. It is generated on the computer that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service such as the Server service, or a local process such as Winlogon.exe or Services.exe. The logon type field indicates the kind of logon that occurred. The most common types are 2 (interactive) and 3 (network). The New Logon fields indicate the account for whom the new logon was created, i.e. the account that was logged on. The network fields indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impersonation level field indicates the extent to which a process in the logon session can impersonate. The authentication information fields provide detailed information about this specific logon request. - Logon GUID is a unique identifier that can be used to correlate this event with a KDC event. - Transited services indicate which intermediate services have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indicates the length of the generated session key. This will be 0 if no session key was requested.
Security	Audit Success	12544	2015-04-24 19:37:51	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: LTRANPHD$ Account Domain: WORKGROUP Logon ID: 0x3e7 Logon Type: 5 Impersonation Level: %%1833 New Logon: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Logon ID: 0x3e7 Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x230 Process Name: C:\Windows\System32\services.exe Network Information: Workstation Name: Source Network Address: - Source Port: - Detailed Authentication Information: Logon Process: Advapi Authentication Package: Negotiate Transited Services: - Package Name (NTLM only): - Key Length: 0 This event is generated when a logon session is created. It is generated on the computer that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service such as the Server service, or a local process such as Winlogon.exe or Services.exe. The logon type field indicates the kind of logon that occurred. The most common types are 2 (interactive) and 3 (network). The New Logon fields indicate the account for

						whom the new logon was created, i.e. the account that was logged on. The network fields indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impersonation level field indicates the extent to which a process in the logon session can impersonate. The authentication information fields provide detailed information about this specific logon request. - Logon GUID is a unique identifier that can be used to correlate this event with a KDC event. - Transited services indicate which intermediate services have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indicates the length of the generated session key. This will be 0 if no session key was requested.
Security	Audit Success	12548	2015-04-24 19:37:51		Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Logon ID: 0x3e7 Privileges: SeAssignPrimaryTokenPrivilege SeTcbPrivilege SeSecurityPrivilege SeTakeOwnershipPrivilege SeLoadDriverPrivilege SeBackupPrivilege SeRestorePrivilege SeDebugPrivilege SeAuditPrivilege SeSystemEnvironmentPrivilege SeImpersonatePrivilege
Security	Audit Success	12548	2015-04-24 19:37:51		Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Logon ID: 0x3e7 Privileges: SeAssignPrimaryTokenPrivilege SeTcbPrivilege SeSecurityPrivilege SeTakeOwnershipPrivilege SeLoadDriverPrivilege SeBackupPrivilege SeRestorePrivilege SeDebugPrivilege SeAuditPrivilege SeSystemEnvironmentPrivilege SeImpersonatePrivilege
Security	Audit Success	12548	2015-04-24 19:37:51		Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Logon ID: 0x3e7 Privileges: SeAssignPrimaryTokenPrivilege SeTcbPrivilege SeSecurityPrivilege SeTakeOwnershipPrivilege SeLoadDriverPrivilege SeBackupPrivilege SeRestorePrivilege SeDebugPrivilege SeAuditPrivilege SeSystemEnvironmentPrivilege SeImpersonatePrivilege
Security	Audit Success	12544	2015-04-24 19:37:52		Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-0-0 Account Name: - Account Domain: - Logon ID: 0x0 Logon Type: 3 Impersonation Level: %%1833 New Logon: Security ID: S-1-5-7 Account Name: ANONYMOUS LOGON Account Domain: NT AUTHORITY Logon ID: 0x18b33 Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x0 Process Name: - Network Information: Workstation Name: Source Network Address: - Source Port: - Detailed Authentication Information: Logon Process: NtLmSsp Authentication Package: NTLM Transited Services: - Package Name (NTLM only): NTLM V1 Key Length: 0 This event is generated when a logon session is created. It is generated on the computer that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service such as the Server service, or a local process such as Winlogon.exe or Services.exe. The logon type field indicates the kind of logon that occurred. The most common types are 2 (interactive) and 3 (network). The New Logon fields indicate the account for whom the new logon was created, i.e. the account that was logged on. The network fields indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impersonation level field indicates the extent to which a process in the logon session can impersonate. The authentication information fields provide detailed information about this specific logon request. - Logon GUID is a unique identifier that can be used to correlate this event with a KDC event. - Transited services indicate which intermediate services have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indicates the length of the generated session key. This will be 0 if no session key was requested.
Security	Audit Success	12544	2015-04-24 19:37:59		Microsoft-Windows-Security-Auditing	4648: A logon was attempted using explicit credentials. Subject: Security ID: S-1-5-18 Account Name: LTRANPHD$ Account Domain: WORKGROUP Logon ID: 0x3e7 Logon GUID: {00000000-0000-0000-0000-000000000000} Account Whose Credentials Were Used: Account Name: Liem Account Domain: LTRANPHD Logon GUID: {00000000-0000-0000-0000-000000000000} Target Server: Target Server Name: localhost Additional Information: localhost Process Information: Process ID: 0x200 Process Name: C:\Windows\System32\winlogon.exe Network Information: Network Address: 127.0.0.1 Port: 0 This event is generated when a process attempts to log on an account by explicitly specifying that account's credentials. This most commonly occurs in batch-type configurations such as scheduled tasks, or when using the RUNAS command.
Security	Audit Success	12544	2015-04-24 19:37:59		Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: LTRANPHD$ Account Domain: WORKGROUP Logon ID: 0x3e7 Logon Type: 2 Impersonation Level: %%1833 New Logon: Security ID: S-1-5-21-1888849264-3803429180-4108621888-1001 Account Name: Liem Account Domain: LTRANPHD Logon ID: 0x1e712 Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x200 Process Name: C:\Windows\System32\winlogon.exe Network Information: Workstation Name: LTRANPHD Source Network Address: 127.0.0.1 Source Port: 0 Detailed Authentication Information: Logon Process: User32 Authentication Package: Negotiate Transited Services: - Package Name (NTLM only): - Key Length: 0 This event is generated when a logon session is created. It is generated on the computer that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service such as the Server service, or a local process such as Winlogon.exe or Services.exe. The logon type field indicates the kind of logon that occurred. The most common types are 2 (interactive) and 3 (network). The New Logon fields indicate the account for whom the new logon was created, i.e. the account that was logged on. The network fields indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impersonation level field indicates the extent to which a process in the logon session can impersonate. The authentication information fields provide detailed information about this specific logon request. - Logon GUID is a unique identifier that can be used to correlate this event with a KDC event. - Transited services indicate which intermediate services have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indicates the length of the generated session key. This will be 0 if no session key was requested.

Security	Audit Success	12544	2015-04-24 19:37:59	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: LTRANPHD$ Account Domain: WORKGROUP Logon ID: 0x3e7 Logon Type: 2 Impersonation Level: %%1833 New Logon: Security ID: S-1-5-21-1888849264-3803429180-4108621888-1001 Account Name: Liem Account Domain: LTRANPHD Logon ID: 0x1e743 Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x200 Process Name: C:\Windows\System32\winlogon.exe Network Information: Workstation Name: LTRANPHD Source Network Address: 127.0.0.1 Source Port: 0 Detailed Authentication Information: Logon Process: User32 Authentication Package: Negotiate Transited Services: - Package Name (NTLM only): - Key Length: 0 This event is generated when a logon session is created. It is generated on the computer that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service such as the Server service, or a local process such as Winlogon.exe or Services.exe. The logon type field indicates the kind of logon that occurred. The most common types are 2 (interactive) and 3 (network). The New Logon fields indicate the account for whom the new logon was created, i.e. the account that was logged on. The network fields indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impersonation level field indicates the extent to which a process in the logon session can impersonate. The authentication information fields provide detailed information about this specific logon request. - Logon GUID is a unique identifier that can be used to correlate this event with a KDC event. - Transited services indicate which intermediate services have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indicates the length of the generated session key. This will be 0 if no session key was requested.
Security	Audit Success	12548	2015-04-24 19:37:59	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-21-1888849264-3803429180-4108621888-1001 Account Name: Liem Account Domain: LTRANPHD Logon ID: 0x1e712 Privileges: SeSecurityPrivilege SeTakeOwnershipPrivilege SeLoadDriverPrivilege SeBackupPrivilege SeRestorePrivilege SeDebugPrivilege SeSystemEnvironmentPrivilege SeImpersonatePrivilege
Security	Audit Success	12544	2015-04-24 19:38:00	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: LTRANPHD$ Account Domain: WORKGROUP Logon ID: 0x3e7 Logon Type: 5 Impersonation Level: %%1833 New Logon: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Logon ID: 0x3e7 Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x230 Process Name: C:\Windows\System32\services.exe Network Information: Workstation Name: Source Network Address: - Source Port: - Detailed Authentication Information: Logon Process: Advapi Authentication Package: Negotiate Transited Services: - Package Name (NTLM only): - Key Length: 0 This event is generated when a logon session is created. It is generated on the computer that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service such as the Server service, or a local process such as Winlogon.exe or Services.exe. The logon type field indicates the kind of logon that occurred. The most common types are 2 (interactive) and 3 (network). The New Logon fields indicate the account for whom the new logon was created, i.e. the account that was logged on. The network fields indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impersonation level field indicates the extent to which a process in the logon session can impersonate. The authentication information fields provide detailed information about this specific logon request. - Logon GUID is a unique identifier that can be used to correlate this event with a KDC event. - Transited services indicate which intermediate services have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indicates the length of the generated session key. This will be 0 if no session key was requested.
Security	Audit Success	12548	2015-04-24 19:38:00	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Logon ID: 0x3e7 Privileges: SeAssignPrimaryTokenPrivilege SeTcbPrivilege SeSecurityPrivilege SeTakeOwnershipPrivilege SeLoadDriverPrivilege SeBackupPrivilege SeRestorePrivilege SeDebugPrivilege SeAuditPrivilege SeSystemEnvironmentPrivilege SeImpersonatePrivilege
Security	Audit Success	13824	2015-04-24 19:38:01	Microsoft-Windows-Security-Auditing	4797: An attempt was made to query the existence of a blank password for an account. Subject: Security ID: S-1-5-19 Account Name: LOCAL SERVICE Account Domain: NT AUTHORITY Logon ID: 0x3e5 Additional Information: Caller Workstation: LTRANPHD Target Account Name: Administrator Target Account Domain: LTRANPHD
Security	Audit Success	13824	2015-04-24 19:38:01	Microsoft-Windows-Security-Auditing	4797: An attempt was made to query the existence of a blank password for an account. Subject: Security ID: S-1-5-19 Account Name: LOCAL SERVICE Account Domain: NT AUTHORITY Logon ID: 0x3e5 Additional Information: Caller Workstation: LTRANPHD Target Account Name: Guest Target Account Domain: LTRANPHD
Security	Audit Success	13824	2015-04-24 19:38:01	Microsoft-Windows-Security-Auditing	4797: An attempt was made to query the existence of a blank password for an account. Subject: Security ID: S-1-5-19 Account Name: LOCAL SERVICE Account Domain: NT AUTHORITY Logon ID: 0x3e5 Additional Information: Caller Workstation: LTRANPHD Target Account Name: Liem Target Account Domain: LTRANPHD
Security	Audit Success	13824	2015-04-24 19:38:01	Microsoft-Windows-Security-Auditing	4797: An attempt was made to query the existence of a blank password for an account. Subject: Security ID: S-1-5-19 Account Name: LOCAL SERVICE Account Domain: NT AUTHORITY Logon ID: 0x3e5 Additional Information: Caller Workstation: LTRANPHD Target Account Name: Liem Target Account Domain: LTRANPHD
Security	Audit Success	13824	2015-04-24 19:38:01	Microsoft-Windows-Security-Auditing	4797: An attempt was made to query the existence of a blank password for an account. Subject: Security ID: S-1-5-19 Account Name: LOCAL SERVICE Account Domain: NT AUTHORITY Logon ID: 0x3e5 Additional Information: Caller Workstation: LTRANPHD Target Account Name: Administrator Target Account Domain: LTRANPHD
Security	Audit Success	13824	2015-04-24	Microsoft-Windows-Security-Auditing	4797: An attempt was made to query the existence of a blank password for an account. Subject: Security ID: S-1-5-19 Account Name: LOCAL SERVICE Account Domain: NT AUTHORITY Logon ID: 0x3e5 Additional

			19:38:01		Information: Caller Workstation: LTRANPHD Target Account Name: Guest Target Account Domain: LTRANPHD
Security	Audit Success	13824	2015-04-24 19:38:01	Microsoft-Windows-Security-Auditing	4797: An attempt was made to query the existence of a blank password for an account. Subject: Security ID: S-1-5-19 Account Name: LOCAL SERVICE Account Domain: NT AUTHORITY Logon ID: 0x3e5 Additional Information: Caller Workstation: LTRANPHD Target Account Name: Liem Target Account Domain: LTRANPHD
Security	Audit Success	13824	2015-04-24 19:38:01	Microsoft-Windows-Security-Auditing	4797: An attempt was made to query the existence of a blank password for an account. Subject: Security ID: S-1-5-19 Account Name: LOCAL SERVICE Account Domain: NT AUTHORITY Logon ID: 0x3e5 Additional Information: Caller Workstation: LTRANPHD Target Account Name: Administrator Target Account Domain: LTRANPHD
Security	Audit Success	13824	2015-04-24 19:38:01	Microsoft-Windows-Security-Auditing	4797: An attempt was made to query the existence of a blank password for an account. Subject: Security ID: S-1-5-19 Account Name: LOCAL SERVICE Account Domain: NT AUTHORITY Logon ID: 0x3e5 Additional Information: Caller Workstation: LTRANPHD Target Account Name: Liem Target Account Domain: LTRANPHD
Security	Audit Success	13824	2015-04-24 19:38:01	Microsoft-Windows-Security-Auditing	4797: An attempt was made to query the existence of a blank password for an account. Subject: Security ID: S-1-5-19 Account Name: LOCAL SERVICE Account Domain: NT AUTHORITY Logon ID: 0x3e5 Additional Information: Caller Workstation: LTRANPHD Target Account Name: Administrator Target Account Domain: LTRANPHD
Security	Audit Success	13824	2015-04-24 19:38:01	Microsoft-Windows-Security-Auditing	4797: An attempt was made to query the existence of a blank password for an account. Subject: Security ID: S-1-5-19 Account Name: LOCAL SERVICE Account Domain: NT AUTHORITY Logon ID: 0x3e5 Additional Information: Caller Workstation: LTRANPHD Target Account Name: Guest Target Account Domain: LTRANPHD
Security	Audit Success	13824	2015-04-24 19:38:01	Microsoft-Windows-Security-Auditing	4797: An attempt was made to query the existence of a blank password for an account. Subject: Security ID: S-1-5-19 Account Name: LOCAL SERVICE Account Domain: NT AUTHORITY Logon ID: 0x3e5 Additional Information: Caller Workstation: LTRANPHD Target Account Name: Liem Target Account Domain: LTRANPHD
Security	Audit Success	13824	2015-04-24 19:38:01	Microsoft-Windows-Security-Auditing	4797: An attempt was made to query the existence of a blank password for an account. Subject: Security ID: S-1-5-19 Account Name: LOCAL SERVICE Account Domain: NT AUTHORITY Logon ID: 0x3e5 Additional Information: Caller Workstation: LTRANPHD Target Account Name: Liem Target Account Domain: LTRANPHD
Security	Audit Success	13824	2015-04-24 19:38:01	Microsoft-Windows-Security-Auditing	4797: An attempt was made to query the existence of a blank password for an account. Subject: Security ID: S-1-5-19 Account Name: LOCAL SERVICE Account Domain: NT AUTHORITY Logon ID: 0x3e5 Additional Information: Caller Workstation: LTRANPHD Target Account Name: Administrator Target Account Domain: LTRANPHD
Security	Audit Success	13824	2015-04-24 19:38:01	Microsoft-Windows-Security-Auditing	4797: An attempt was made to query the existence of a blank password for an account. Subject: Security ID: S-1-5-19 Account Name: LOCAL SERVICE Account Domain: NT AUTHORITY Logon ID: 0x3e5 Additional Information: Caller Workstation: LTRANPHD Target Account Name: Guest Target Account Domain: LTRANPHD
Security	Audit Success	13824	2015-04-24 19:38:01	Microsoft-Windows-Security-Auditing	4797: An attempt was made to query the existence of a blank password for an account. Subject: Security ID: S-1-5-19 Account Name: LOCAL SERVICE Account Domain: NT AUTHORITY Logon ID: 0x3e5 Additional Information: Caller Workstation: LTRANPHD Target Account Name: Liem Target Account Domain: LTRANPHD
Security	Audit Success	13824	2015-04-24 19:38:01	Microsoft-Windows-Security-Auditing	4797: An attempt was made to query the existence of a blank password for an account. Subject: Security ID: S-1-5-19 Account Name: LOCAL SERVICE Account Domain: NT AUTHORITY Logon ID: 0x3e5 Additional Information: Caller Workstation: LTRANPHD Target Account Name: Liem Target Account Domain: LTRANPHD
Security	Audit Success	13824	2015-04-24 19:38:02	Microsoft-Windows-Security-Auditing	4797: An attempt was made to query the existence of a blank password for an account. Subject: Security ID: S-1-5-21-1888849264-3803429180-4108621888-1001 Account Name: Liem Account Domain: LTRANPHD Logon ID: 0x1e743 Additional Information: Caller Workstation: LTRANPHD Target Account Name: Administrator Target Account Domain: LTRANPHD
Security	Audit Success	13824	2015-04-24 19:38:02	Microsoft-Windows-Security-Auditing	4797: An attempt was made to query the existence of a blank password for an account. Subject: Security ID: S-1-5-21-1888849264-3803429180-4108621888-1001 Account Name: Liem Account Domain: LTRANPHD Logon ID: 0x1e743 Additional Information: Caller Workstation: LTRANPHD Target Account Name: Guest Target Account Domain: LTRANPHD
Security	Audit Success	13824	2015-04-24 19:38:02	Microsoft-Windows-Security-Auditing	4797: An attempt was made to query the existence of a blank password for an account. Subject: Security ID: S-1-5-21-1888849264-3803429180-4108621888-1001 Account Name: Liem Account Domain: LTRANPHD Logon ID: 0x1e743 Additional Information: Caller Workstation: LTRANPHD Target Account Name: Administrator Target Account Domain: LTRANPHD
Security	Audit Success	13824	2015-04-24 19:38:02	Microsoft-Windows-Security-Auditing	4797: An attempt was made to query the existence of a blank password for an account. Subject: Security ID: S-1-5-21-1888849264-3803429180-4108621888-1001 Account Name: Liem Account Domain: LTRANPHD Logon ID: 0x1e743 Additional Information: Caller Workstation: LTRANPHD Target Account Name: Guest Target Account Domain: LTRANPHD
Security	Audit Success	103	2015-04-24 19:41:29	Microsoft-Windows-Eventlog	1100: The event logging service has shut down.
Security	Audit Success	12545	2015-04-24 19:41:29	Microsoft-Windows-Security-Auditing	4647: User initiated logoff: Subject: Security ID: S-1-5-21-1888849264-3803429180-4108621888-1001 Account Name: Liem Account Domain: LTRANPHD Logon ID: 0x1e743 This event is generated when a logoff is initiated. No further user-initiated activity can occur. This event can be interpreted as a logoff event.
Security	Audit Success	12288	2015-04-24 19:41:53	Microsoft-Windows-Security-Auditing	4608: Windows is starting up. This event is logged when LSASS.EXE starts and the auditing subsystem is initialized.
					4624: An account was successfully logged on. Subject: Security ID: S-1-0-0 Account Name: - Account Domain:

Security	Audit Success	12544	2015-04-24 19:41:53	Microsoft-Windows-Security-Auditing	- Logon ID: 0x0 Logon Type: 0 Impersonation Level: - New Logon: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Logon ID: 0x3e7 Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x4 Process Name: Network Information: Workstation Name: - Source Network Address: - Source Port: - Detailed Authentication Information: Logon Process: - Authentication Package: - Transited Services: - Package Name (NTLM only): - Key Length: 0 This event is generated when a logon session is created. It is generated on the computer that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service such as the Server service, or a local process such as Winlogon.exe or Services.exe. The logon type field indicates the kind of logon that occurred. The most common types are 2 (interactive) and 3 (network). The New Logon fields indicate the account for whom the new logon was created, i.e. the account that was logged on. The network fields indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impersonation level field indicates the extent to which a process in the logon session can impersonate. The authentication information fields provide detailed information about this specific logon request. - Logon GUID is a unique identifier that can be used to correlate this event with a KDC event. - Transited services indicate which intermediate services have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indicates the length of the generated session key. This will be 0 if no session key was requested.
Security	Audit Success	12544	2015-04-24 19:41:53	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: LTRANPHD$ Account Domain: WORKGROUP Logon ID: 0x3e7 Logon Type: 5 Impersonation Level: %%1833 New Logon: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Logon ID: 0x3e7 Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x230 Process Name: C:\Windows\System32\services.exe Network Information: Workstation Name: Source Network Address: - Source Port: - Detailed Authentication Information: Logon Process: Advapi Authentication Package: Negotiate Transited Services: - Package Name (NTLM only): - Key Length: 0 This event is generated when a logon session is created. It is generated on the computer that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service such as the Server service, or a local process such as Winlogon.exe or Services.exe. The logon type field indicates the kind of logon that occurred. The most common types are 2 (interactive) and 3 (network). The New Logon fields indicate the account for whom the new logon was created, i.e. the account that was logged on. The network fields indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impersonation level field indicates the extent to which a process in the logon session can impersonate. The authentication information fields provide detailed information about this specific logon request. - Logon GUID is a unique identifier that can be used to correlate this event with a KDC event. - Transited services indicate which intermediate services have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indicates the length of the generated session key. This will be 0 if no session key was requested.
Security	Audit Success	12544	2015-04-24 19:41:53	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: LTRANPHD$ Account Domain: WORKGROUP Logon ID: 0x3e7 Logon Type: 5 Impersonation Level: %%1833 New Logon: Security ID: S-1-5-20 Account Name: NETWORK SERVICE Account Domain: NT AUTHORITY Logon ID: 0x3e4 Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x230 Process Name: C:\Windows\System32\services.exe Network Information: Workstation Name: Source Network Address: - Source Port: - Detailed Authentication Information: Logon Process: Advapi Authentication Package: Negotiate Transited Services: - Package Name (NTLM only): - Key Length: 0 This event is generated when a logon session is created. It is generated on the computer that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service such as the Server service, or a local process such as Winlogon.exe or Services.exe. The logon type field indicates the kind of logon that occurred. The most common types are 2 (interactive) and 3 (network). The New Logon fields indicate the account for whom the new logon was created, i.e. the account that was logged on. The network fields indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impersonation level field indicates the extent to which a process in the logon session can impersonate. The authentication information fields provide detailed information about this specific logon request. - Logon GUID is a unique identifier that can be used to correlate this event with a KDC event. - Transited services indicate which intermediate services have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indicates the length of the generated session key. This will be 0 if no session key was requested.
Security	Audit Success	12544	2015-04-24 19:41:53	Microsoft-Windows-Security-Auditing	4648: A logon was attempted using explicit credentials. Subject: Security ID: S-1-5-18 Account Name: LTRANPHD$ Account Domain: WORKGROUP Logon ID: 0x3e7 Logon GUID: {00000000-0000-0000-0000-000000000000} Account Whose Credentials Were Used: Account Name: DWM-1 Account Domain: Window Manager Logon GUID: {00000000-0000-0000-0000-000000000000} Target Server: Target Server Name: localhost Additional Information: localhost Process Information: Process ID: 0x200 Process Name: C:\Windows\System32\winlogon.exe Network Information: Network Address: - Port: - This event is generated when a process attempts to log on an account by explicitly specifying that account's credentials. This most commonly occurs in batch-type configurations such as scheduled tasks, or when using the RUNAS command.
					4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: LTRANPHD$ Account Domain: WORKGROUP Logon ID: 0x3e7 Logon Type: 2 Impersonation Level: %%1833 New Logon: Security ID: S-1-5-90-1 Account Name: DWM-1 Account Domain: Window Manager Logon ID: 0xc367 Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x200 Process Name:

Security	Audit Success	12544	2015-04-24 19:41:53	Microsoft-Windows-Security-Auditing	C:\Windows\System32\winlogon.exe Network Information: Workstation Name: Source Network Address: - Source Port: - Detailed Authentication Information: Logon Process: Advapi Authentication Package: Negotiate Transited Services: - Package Name (NTLM only): - Key Length: 0 This event is generated when a logon session is created. It is generated on the computer that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service such as the Server service, or a local process such as Winlogon.exe or Services.exe. The logon type field indicates the kind of logon that occurred. The most common types are 2 (interactive) and 3 (network). The New Logon fields indicate the account for whom the new logon was created, i.e. the account that was logged on. The network fields indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impersonation level field indicates the extent to which a process in the logon session can impersonate. The authentication information fields provide detailed information about this specific logon request. - Logon GUID is a unique identifier that can be used to correlate this event with a KDC event. - Transited services indicate which intermediate services have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indicates the length of the generated session key. This will be 0 if no session key was requested.
Security	Audit Success	12544	2015-04-24 19:41:53	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: LTRANPHD$ Account Domain: WORKGROUP Logon ID: 0x3e7 Logon Type: 2 Impersonation Level: %%1833 New Logon: Security ID: S-1-5-90-1 Account Name: DWM-1 Account Domain: Window Manager Logon ID: 0xc37f Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x200 Process Name: C:\Windows\System32\winlogon.exe Network Information: Workstation Name: Source Network Address: - Source Port: - Detailed Authentication Information: Logon Process: Advapi Authentication Package: Negotiate Transited Services: - Package Name (NTLM only): - Key Length: 0 This event is generated when a logon session is created. It is generated on the computer that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service such as the Server service, or a local process such as Winlogon.exe or Services.exe. The logon type field indicates the kind of logon that occurred. The most common types are 2 (interactive) and 3 (network). The New Logon fields indicate the account for whom the new logon was created, i.e. the account that was logged on. The network fields indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impersonation level field indicates the extent to which a process in the logon session can impersonate. The authentication information fields provide detailed information about this specific logon request. - Logon GUID is a unique identifier that can be used to correlate this event with a KDC event. - Transited services indicate which intermediate services have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indicates the length of the generated session key. This will be 0 if no session key was requested.
Security	Audit Success	12544	2015-04-24 19:41:53	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: LTRANPHD$ Account Domain: WORKGROUP Logon ID: 0x3e7 Logon Type: 5 Impersonation Level: %%1833 New Logon: Security ID: S-1-5-19 Account Name: LOCAL SERVICE Account Domain: NT AUTHORITY Logon ID: 0x3e5 Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x230 Process Name: C:\Windows\System32\services.exe Network Information: Workstation Name: Source Network Address: - Source Port: - Detailed Authentication Information: Logon Process: Advapi Authentication Package: Negotiate Transited Services: - Package Name (NTLM only): - Key Length: 0 This event is generated when a logon session is created. It is generated on the computer that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service such as the Server service, or a local process such as Winlogon.exe or Services.exe. The logon type field indicates the kind of logon that occurred. The most common types are 2 (interactive) and 3 (network). The New Logon fields indicate the account for whom the new logon was created, i.e. the account that was logged on. The network fields indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impersonation level field indicates the extent to which a process in the logon session can impersonate. The authentication information fields provide detailed information about this specific logon request. - Logon GUID is a unique identifier that can be used to correlate this event with a KDC event. - Transited services indicate which intermediate services have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indicates the length of the generated session key. This will be 0 if no session key was requested.
Security	Audit Success	12544	2015-04-24 19:41:53	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: LTRANPHD$ Account Domain: WORKGROUP Logon ID: 0x3e7 Logon Type: 5 Impersonation Level: %%1833 New Logon: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Logon ID: 0x3e7 Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x230 Process Name: C:\Windows\System32\services.exe Network Information: Workstation Name: Source Network Address: - Source Port: - Detailed Authentication Information: Logon Process: Advapi Authentication Package: Negotiate Transited Services: - Package Name (NTLM only): - Key Length: 0 This event is generated when a logon session is created. It is generated on the computer that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service such as the Server service, or a local process such as Winlogon.exe or Services.exe. The logon type field indicates the kind of logon that occurred. The most common types are 2 (interactive) and 3 (network). The New Logon fields indicate the account for whom the new logon was created, i.e. the account that was logged on. The network fields indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impersonation level field indicates the extent to which a process in the logon session can

					impersonate. The authentication information fields provide detailed information about this specific logon request. - Logon GUID is a unique identifier that can be used to correlate this event with a KDC event. - Transited services indicate which intermediate services have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indicates the length of the generated session key. This will be 0 if no session key was requested.
Security	Audit Success	12548	2015-04-24 19:41:53	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Logon ID: 0x3e7 Privileges: SeAssignPrimaryTokenPrivilege SeTcbPrivilege SeSecurityPrivilege SeTakeOwnershipPrivilege SeLoadDriverPrivilege SeBackupPrivilege SeRestorePrivilege SeDebugPrivilege SeAuditPrivilege SeSystemEnvironmentPrivilege SeImpersonatePrivilege
Security	Audit Success	12548	2015-04-24 19:41:53	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-20 Account Name: NETWORK SERVICE Account Domain: NT AUTHORITY Logon ID: 0x3e4 Privileges: SeAssignPrimaryTokenPrivilege SeAuditPrivilege SeImpersonatePrivilege
Security	Audit Success	12548	2015-04-24 19:41:53	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-90-1 Account Name: DWM-1 Account Domain: Window Manager Logon ID: 0xc367 Privileges: SeAssignPrimaryTokenPrivilege SeAuditPrivilege SeImpersonatePrivilege
Security	Audit Success	12548	2015-04-24 19:41:53	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-90-1 Account Name: DWM-1 Account Domain: Window Manager Logon ID: 0xc37f Privileges: SeAssignPrimaryTokenPrivilege SeAuditPrivilege
Security	Audit Success	12548	2015-04-24 19:41:53	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-19 Account Name: LOCAL SERVICE Account Domain: NT AUTHORITY Logon ID: 0x3e5 Privileges: SeAssignPrimaryTokenPrivilege SeAuditPrivilege SeImpersonatePrivilege
Security	Audit Success	12548	2015-04-24 19:41:53	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Logon ID: 0x3e7 Privileges: SeAssignPrimaryTokenPrivilege SeTcbPrivilege SeSecurityPrivilege SeTakeOwnershipPrivilege SeLoadDriverPrivilege SeBackupPrivilege SeRestorePrivilege SeDebugPrivilege SeAuditPrivilege SeSystemEnvironmentPrivilege SeImpersonatePrivilege
Security	Audit Success	13568	2015-04-24 19:41:53	Microsoft-Windows-Security-Auditing	4902: The Per-user audit policy table was created. Number of Elements: 0 Policy ID: 0x747f
Security	Audit Success	12292	2015-04-24 19:41:54	Microsoft-Windows-Security-Auditing	5033: The Windows Firewall Driver started successfully.
Security	Audit Success	12292	2015-04-24 19:41:54	Microsoft-Windows-Security-Auditing	5024: The Windows Firewall service started successfully.
Security	Audit Success	12544	2015-04-24 19:41:54	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: LTRANPHD$ Account Domain: WORKGROUP Logon ID: 0x3e7 Logon Type: 5 Impersonation Level: %%1833 New Logon: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Logon ID: 0x3e7 Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x230 Process Name: C:\Windows\System32\services.exe Network Information: Workstation Name: Source Network Address: - Source Port: - Detailed Authentication Information: Logon Process: Advapi Authentication Package: Negotiate Transited Services: - Package Name (NTLM only): - Key Length: 0 This event is generated when a logon session is created. It is generated on the computer that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service such as the Server service, or a local process such as Winlogon.exe or Services.exe. The logon type field indicates the kind of logon that occurred. The most common types are 2 (interactive) and 3 (network). The New Logon fields indicate the account for whom the new logon was created, i.e. the account that was logged on. The network fields indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impersonation level field indicates the extent to which a process in the logon session can impersonate. The authentication information fields provide detailed information about this specific logon request. - Logon GUID is a unique identifier that can be used to correlate this event with a KDC event. - Transited services indicate which intermediate services have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indicates the length of the generated session key. This will be 0 if no session key was requested.
Security	Audit Success	12544	2015-04-24 19:41:54	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: LTRANPHD$ Account Domain: WORKGROUP Logon ID: 0x3e7 Logon Type: 5 Impersonation Level: %%1833 New Logon: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Logon ID: 0x3e7 Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x230 Process Name: C:\Windows\System32\services.exe Network Information: Workstation Name: Source Network Address: - Source Port: - Detailed Authentication Information: Logon Process: Advapi Authentication Package: Negotiate Transited Services: - Package Name (NTLM only): - Key Length: 0 This event is generated when a logon session is created. It is generated on the computer that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service such as the Server service, or a local process such as Winlogon.exe or Services.exe. The logon type field indicates the kind of logon that occurred. The most common types are 2 (interactive) and 3 (network). The New Logon fields indicate the account for whom the new logon was created, i.e. the account that was logged on. The network fields indicate where a

					remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impersonation level field indicates the extent to which a process in the logon session can impersonate. The authentication information fields provide detailed information about this specific logon request. - Logon GUID is a unique identifier that can be used to correlate this event with a KDC event. - Transited services indicate which intermediate services have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indicates the length of the generated session key. This will be 0 if no session key was requested.
Security	Audit Success	12544	2015-04-24 19:41:54	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: LTRANPHD$ Account Domain: WORKGROUP Logon ID: 0x3e7 Logon Type: 5 Impersonation Level: %%1833 New Logon: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Logon ID: 0x3e7 Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x230 Process Name: C:\Windows\System32\services.exe Network Information: Workstation Name: Source Network Address: - Source Port: - Detailed Authentication Information: Logon Process: Advapi Authentication Package: Negotiate Transited Services: - Package Name (NTLM only): - Key Length: 0 This event is generated when a logon session is created. It is generated on the computer that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service such as the Server service, or a local process such as Winlogon.exe or Services.exe. The logon type field indicates the kind of logon that occurred. The most common types are 2 (interactive) and 3 (network). The New Logon fields indicate the account for whom the new logon was created, i.e. the account that was logged on. The network fields indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impersonation level field indicates the extent to which a process in the logon session can impersonate. The authentication information fields provide detailed information about this specific logon request. - Logon GUID is a unique identifier that can be used to correlate this event with a KDC event. - Transited services indicate which intermediate services have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indicates the length of the generated session key. This will be 0 if no session key was requested.
Security	Audit Success	12544	2015-04-24 19:41:54	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: LTRANPHD$ Account Domain: WORKGROUP Logon ID: 0x3e7 Logon Type: 5 Impersonation Level: %%1833 New Logon: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Logon ID: 0x3e7 Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x230 Process Name: C:\Windows\System32\services.exe Network Information: Workstation Name: Source Network Address: - Source Port: - Detailed Authentication Information: Logon Process: Advapi Authentication Package: Negotiate Transited Services: - Package Name (NTLM only): - Key Length: 0 This event is generated when a logon session is created. It is generated on the computer that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service such as the Server service, or a local process such as Winlogon.exe or Services.exe. The logon type field indicates the kind of logon that occurred. The most common types are 2 (interactive) and 3 (network). The New Logon fields indicate the account for whom the new logon was created, i.e. the account that was logged on. The network fields indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impersonation level field indicates the extent to which a process in the logon session can impersonate. The authentication information fields provide detailed information about this specific logon request. - Logon GUID is a unique identifier that can be used to correlate this event with a KDC event. - Transited services indicate which intermediate services have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indicates the length of the generated session key. This will be 0 if no session key was requested.
Security	Audit Success	12544	2015-04-24 19:41:54	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-0-0 Account Name: - Account Domain: - Logon ID: 0x0 Logon Type: 3 Impersonation Level: %%1833 New Logon: Security ID: S-1-5-7 Account Name: ANONYMOUS LOGON Account Domain: NT AUTHORITY Logon ID: 0x18893 Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x0 Process Name: - Network Information: Workstation Name: Source Network Address: - Source Port: - Detailed Authentication Information: Logon Process: NtLmSsp Authentication Package: NTLM Transited Services: - Package Name (NTLM only): NTLM V1 Key Length: 0 This event is generated when a logon session is created. It is generated on the computer that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service such as the Server service, or a local process such as Winlogon.exe or Services.exe. The logon type field indicates the kind of logon that occurred. The most common types are 2 (interactive) and 3 (network). The New Logon fields indicate the account for whom the new logon was created, i.e. the account that was logged on. The network fields indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impersonation level field indicates the extent to which a process in the logon session can impersonate. The authentication information fields provide detailed information about this specific logon request. - Logon GUID is a unique identifier that can be used to correlate this event with a KDC event. - Transited services indicate which intermediate services have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indicates the length of the generated session key. This will be 0 if no session key was requested.
Security	Audit Success	12548	2015-04-24 19:41:54	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Logon ID: 0x3e7 Privileges: SeAssignPrimaryTokenPrivilege SeTcbPrivilege SeSecurityPrivilege SeTakeOwnershipPrivilege SeLoadDriverPrivilege SeBackupPrivilege SeRestorePrivilege SeDebugPrivilege SeAuditPrivilege SeSystemEnvironmentPrivilege SeImpersonatePrivilege

Security	Audit Success	12548	2015-04-24 19:41:54	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Logon ID: 0x3e7 Privileges: SeAssignPrimaryTokenPrivilege SeTcbPrivilege SeSecurityPrivilege SeTakeOwnershipPrivilege SeLoadDriverPrivilege SeBackupPrivilege SeRestorePrivilege SeDebugPrivilege SeAuditPrivilege SeSystemEnvironmentPrivilege SeImpersonatePrivilege
Security	Audit Success	12548	2015-04-24 19:41:54	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Logon ID: 0x3e7 Privileges: SeAssignPrimaryTokenPrivilege SeTcbPrivilege SeSecurityPrivilege SeTakeOwnershipPrivilege SeLoadDriverPrivilege SeBackupPrivilege SeRestorePrivilege SeDebugPrivilege SeAuditPrivilege SeSystemEnvironmentPrivilege SeImpersonatePrivilege
Security	Audit Success	12548	2015-04-24 19:41:54	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Logon ID: 0x3e7 Privileges: SeAssignPrimaryTokenPrivilege SeTcbPrivilege SeSecurityPrivilege SeTakeOwnershipPrivilege SeLoadDriverPrivilege SeBackupPrivilege SeRestorePrivilege SeDebugPrivilege SeAuditPrivilege SeSystemEnvironmentPrivilege SeImpersonatePrivilege
Security	Audit Success	12544	2015-04-24 19:41:58	Microsoft-Windows-Security-Auditing	4648: A logon was attempted using explicit credentials. Subject: Security ID: S-1-5-18 Account Name: LTRANPHD$ Account Domain: WORKGROUP Logon ID: 0x3e7 Logon GUID: {00000000-0000-0000-0000-000000000000} Account Whose Credentials Were Used: Account Name: Liem Account Domain: LTRANPHD Logon GUID: {00000000-0000-0000-0000-000000000000} Target Server: Target Server Name: localhost Additional Information: localhost Process Information: Process ID: 0x200 Process Name: C:\Windows\System32\winlogon.exe Network Information: Network Address: 127.0.0.1 Port: 0 This event is generated when a process attempts to log on an account by explicitly specifying that account’s credentials. This most commonly occurs in batch-type configurations such as scheduled tasks, or when using the RUNAS command.
Security	Audit Success	12544	2015-04-24 19:41:58	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: LTRANPHD$ Account Domain: WORKGROUP Logon ID: 0x3e7 Logon Type: 2 Impersonation Level: %%1833 New Logon: Security ID: S-1-5-21-1888849264-3803429180-4108621888-1001 Account Name: Liem Account Domain: LTRANPHD Logon ID: 0x1d7c9 Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x200 Process Name: C:\Windows\System32\winlogon.exe Network Information: Workstation Name: LTRANPHD Source Network Address: 127.0.0.1 Source Port: 0 Detailed Authentication Information: Logon Process: User32 Authentication Package: Negotiate Transited Services: - Package Name (NTLM only): - Key Length: 0 This event is generated when a logon session is created. It is generated on the computer that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service such as the Server service, or a local process such as Winlogon.exe or Services.exe. The logon type field indicates the kind of logon that occurred. The most common types are 2 (interactive) and 3 (network). The New Logon fields indicate the account for whom the new logon was created, i.e. the account that was logged on. The network fields indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impersonation level field indicates the extent to which a process in the logon session can impersonate. The authentication information fields provide detailed information about this specific logon request. - Logon GUID is a unique identifier that can be used to correlate this event with a KDC event. - Transited services indicate which intermediate services have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indicates the length of the generated session key. This will be 0 if no session key was requested.
Security	Audit Success	12544	2015-04-24 19:41:58	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: LTRANPHD$ Account Domain: WORKGROUP Logon ID: 0x3e7 Logon Type: 2 Impersonation Level: %%1833 New Logon: Security ID: S-1-5-21-1888849264-3803429180-4108621888-1001 Account Name: Liem Account Domain: LTRANPHD Logon ID: 0x1d7f8 Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x200 Process Name: C:\Windows\System32\winlogon.exe Network Information: Workstation Name: LTRANPHD Source Network Address: 127.0.0.1 Source Port: 0 Detailed Authentication Information: Logon Process: User32 Authentication Package: Negotiate Transited Services: - Package Name (NTLM only): - Key Length: 0 This event is generated when a logon session is created. It is generated on the computer that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service such as the Server service, or a local process such as Winlogon.exe or Services.exe. The logon type field indicates the kind of logon that occurred. The most common types are 2 (interactive) and 3 (network). The New Logon fields indicate the account for whom the new logon was created, i.e. the account that was logged on. The network fields indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impersonation level field indicates the extent to which a process in the logon session can impersonate. The authentication information fields provide detailed information about this specific logon request. - Logon GUID is a unique identifier that can be used to correlate this event with a KDC event. - Transited services indicate which intermediate services have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indicates the length of the generated session key. This will be 0 if no session key was requested.
					4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: LTRANPHD$ Account Domain: WORKGROUP Logon ID: 0x3e7 Logon Type: 5 Impersonation Level: %%1833 New Logon: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Logon ID: 0x3e7 Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x230 Process Name: C:\Windows\System32\services.exe Network Information: Workstation Name: Source Network Address: - Source Port: - Detailed Authentication Information: Logon Process: Advapi Authentication Package: Negotiate Transited Services: - Package Name (NTLM only): - Key Length: 0 This event is generated when a logon session is

Security	Audit Success	12544	2015-04-24 19:41:58	Microsoft-Windows-Security-Auditing	created. It is generated on the computer that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service such as the Server service, or a local process such as Winlogon.exe or Services.exe. The logon type field indicates the kind of logon that occurred. The most common types are 2 (interactive) and 3 (network). The New Logon fields indicate the account for whom the new logon was created, i.e. the account that was logged on. The network fields indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impersonation level field indicates the extent to which a process in the logon session can impersonate. The authentication information fields provide detailed information about this specific logon request. - Logon GUID is a unique identifier that can be used to correlate this event with a KDC event. - Transited services indicate which intermediate services have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indicates the length of the generated session key. This will be 0 if no session key was requested.
Security	Audit Success	12548	2015-04-24 19:41:58	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-21-1888849264-3803429180-4108621888-1001 Account Name: Liem Account Domain: LTRANPHD Logon ID: 0x1d7c9 Privileges: SeSecurityPrivilege SeTakeOwnershipPrivilege SeLoadDriverPrivilege SeBackupPrivilege SeRestorePrivilege SeDebugPrivilege SeSystemEnvironmentPrivilege SeImpersonatePrivilege
Security	Audit Success	12548	2015-04-24 19:41:58	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Logon ID: 0x3e7 Privileges: SeAssignPrimaryTokenPrivilege SeTcbPrivilege SeSecurityPrivilege SeTakeOwnershipPrivilege SeLoadDriverPrivilege SeBackupPrivilege SeRestorePrivilege SeDebugPrivilege SeAuditPrivilege SeSystemEnvironmentPrivilege SeImpersonatePrivilege
Security	Audit Success	13824	2015-04-24 19:42:00	Microsoft-Windows-Security-Auditing	4797: An attempt was made to query the existence of a blank password for an account. Subject: Security ID: S-1-5-21-1888849264-3803429180-4108621888-1001 Account Name: Liem Account Domain: LTRANPHD Logon ID: 0x1d7f8 Additional Information: Caller Workstation: LTRANPHD Target Account Name: Administrator Target Account Domain: LTRANPHD
Security	Audit Success	13824	2015-04-24 19:42:00	Microsoft-Windows-Security-Auditing	4797: An attempt was made to query the existence of a blank password for an account. Subject: Security ID: S-1-5-21-1888849264-3803429180-4108621888-1001 Account Name: Liem Account Domain: LTRANPHD Logon ID: 0x1d7f8 Additional Information: Caller Workstation: LTRANPHD Target Account Name: Guest Target Account Domain: LTRANPHD
Security	Audit Success	13824	2015-04-24 19:42:00	Microsoft-Windows-Security-Auditing	4797: An attempt was made to query the existence of a blank password for an account. Subject: Security ID: S-1-5-21-1888849264-3803429180-4108621888-1001 Account Name: Liem Account Domain: LTRANPHD Logon ID: 0x1d7f8 Additional Information: Caller Workstation: LTRANPHD Target Account Name: Administrator Target Account Domain: LTRANPHD
Security	Audit Success	13824	2015-04-24 19:42:00	Microsoft-Windows-Security-Auditing	4797: An attempt was made to query the existence of a blank password for an account. Subject: Security ID: S-1-5-21-1888849264-3803429180-4108621888-1001 Account Name: Liem Account Domain: LTRANPHD Logon ID: 0x1d7f8 Additional Information: Caller Workstation: LTRANPHD Target Account Name: Guest Target Account Domain: LTRANPHD
Security	Audit Success	13824	2015-04-24 19:42:02	Microsoft-Windows-Security-Auditing	4797: An attempt was made to query the existence of a blank password for an account. Subject: Security ID: S-1-5-19 Account Name: LOCAL SERVICE Account Domain: NT AUTHORITY Logon ID: 0x3e5 Additional Information: Caller Workstation: LTRANPHD Target Account Name: Administrator Target Account Domain: LTRANPHD
Security	Audit Success	13824	2015-04-24 19:42:02	Microsoft-Windows-Security-Auditing	4797: An attempt was made to query the existence of a blank password for an account. Subject: Security ID: S-1-5-19 Account Name: LOCAL SERVICE Account Domain: NT AUTHORITY Logon ID: 0x3e5 Additional Information: Caller Workstation: LTRANPHD Target Account Name: Administrator Target Account Domain: LTRANPHD
Security	Audit Success	13824	2015-04-24 19:42:02	Microsoft-Windows-Security-Auditing	4797: An attempt was made to query the existence of a blank password for an account. Subject: Security ID: S-1-5-19 Account Name: LOCAL SERVICE Account Domain: NT AUTHORITY Logon ID: 0x3e5 Additional Information: Caller Workstation: LTRANPHD Target Account Name: Guest Target Account Domain: LTRANPHD
Security	Audit Success	13824	2015-04-24 19:42:02	Microsoft-Windows-Security-Auditing	4797: An attempt was made to query the existence of a blank password for an account. Subject: Security ID: S-1-5-19 Account Name: LOCAL SERVICE Account Domain: NT AUTHORITY Logon ID: 0x3e5 Additional Information: Caller Workstation: LTRANPHD Target Account Name: Guest Target Account Domain: LTRANPHD
Security	Audit Success	13824	2015-04-24 19:42:02	Microsoft-Windows-Security-Auditing	4797: An attempt was made to query the existence of a blank password for an account. Subject: Security ID: S-1-5-19 Account Name: LOCAL SERVICE Account Domain: NT AUTHORITY Logon ID: 0x3e5 Additional Information: Caller Workstation: LTRANPHD Target Account Name: Liem Target Account Domain: LTRANPHD
Security	Audit Success	13824	2015-04-24 19:42:02	Microsoft-Windows-Security-Auditing	4797: An attempt was made to query the existence of a blank password for an account. Subject: Security ID: S-1-5-19 Account Name: LOCAL SERVICE Account Domain: NT AUTHORITY Logon ID: 0x3e5 Additional Information: Caller Workstation: LTRANPHD Target Account Name: Liem Target Account Domain: LTRANPHD
Security	Audit Success	13824	2015-04-24 19:42:02	Microsoft-Windows-Security-Auditing	4797: An attempt was made to query the existence of a blank password for an account. Subject: Security ID: S-1-5-19 Account Name: LOCAL SERVICE Account Domain: NT AUTHORITY Logon ID: 0x3e5 Additional Information: Caller Workstation: LTRANPHD Target Account Name: Liem Target Account Domain: LTRANPHD
Security	Audit Success	13824	2015-04-24 19:42:02	Microsoft-Windows-Security-Auditing	4797: An attempt was made to query the existence of a blank password for an account. Subject: Security ID: S-1-5-19 Account Name: LOCAL SERVICE Account Domain: NT AUTHORITY Logon ID: 0x3e5 Additional Information: Caller Workstation: LTRANPHD Target Account Name: Liem Target Account Domain: LTRANPHD
					4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: LTRANPHD$ Account Domain: WORKGROUP Logon ID: 0x3e7 Logon Type: 5 Impersonation Level: %%1833 New Logon:

Security	Audit Success	12544	2015-04-24 19:48:16	Microsoft-Windows-Security-Auditing	Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Logon ID: 0x3e7 Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x230 Process Name: C:\Windows\System32\services.exe Network Information: Workstation Name: Source Network Address: - Source Port: - Detailed Authentication Information: Logon Process: Advapi Authentication Package: Negotiate Transited Services: - Package Name (NTLM only): - Key Length: 0 This event is generated when a logon session is created. It is generated on the computer that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service such as the Server service, or a local process such as Winlogon.exe or Services.exe. The logon type field indicates the kind of logon that occurred. The most common types are 2 (interactive) and 3 (network). The New Logon fields indicate the account for whom the new logon was created, i.e. the account that was logged on. The network fields indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impersonation level field indicates the extent to which a process in the logon session can impersonate. The authentication information fields provide detailed information about this specific logon request. - Logon GUID is a unique identifier that can be used to correlate this event with a KDC event. - Transited services indicate which intermediate services have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indicates the length of the generated session key. This will be 0 if no session key was requested.
Security	Audit Success	12548	2015-04-24 19:48:16	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Logon ID: 0x3e7 Privileges: SeAssignPrimaryTokenPrivilege SeTcbPrivilege SeSecurityPrivilege SeTakeOwnershipPrivilege SeLoadDriverPrivilege SeBackupPrivilege SeRestorePrivilege SeDebugPrivilege SeAuditPrivilege SeSystemEnvironmentPrivilege SeImpersonatePrivilege
Security	Audit Success	12544	2015-04-24 19:48:18	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: LTRANPHD$ Account Domain: WORKGROUP Logon ID: 0x3e7 Logon Type: 5 Impersonation Level: %%1833 New Logon: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Logon ID: 0x3e7 Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x230 Process Name: C:\Windows\System32\services.exe Network Information: Workstation Name: Source Network Address: - Source Port: - Detailed Authentication Information: Logon Process: Advapi Authentication Package: Negotiate Transited Services: - Package Name (NTLM only): - Key Length: 0 This event is generated when a logon session is created. It is generated on the computer that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service such as the Server service, or a local process such as Winlogon.exe or Services.exe. The logon type field indicates the kind of logon that occurred. The most common types are 2 (interactive) and 3 (network). The New Logon fields indicate the account for whom the new logon was created, i.e. the account that was logged on. The network fields indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impersonation level field indicates the extent to which a process in the logon session can impersonate. The authentication information fields provide detailed information about this specific logon request. - Logon GUID is a unique identifier that can be used to correlate this event with a KDC event. - Transited services indicate which intermediate services have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indicates the length of the generated session key. This will be 0 if no session key was requested.
Security	Audit Success	12548	2015-04-24 19:48:18	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Logon ID: 0x3e7 Privileges: SeAssignPrimaryTokenPrivilege SeTcbPrivilege SeSecurityPrivilege SeTakeOwnershipPrivilege SeLoadDriverPrivilege SeBackupPrivilege SeRestorePrivilege SeDebugPrivilege SeAuditPrivilege SeSystemEnvironmentPrivilege SeImpersonatePrivilege
Security	Audit Success	12544	2015-04-24 19:57:41	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: LTRANPHD$ Account Domain: WORKGROUP Logon ID: 0x3e7 Logon Type: 5 Impersonation Level: %%1833 New Logon: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Logon ID: 0x3e7 Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x230 Process Name: C:\Windows\System32\services.exe Network Information: Workstation Name: Source Network Address: - Source Port: - Detailed Authentication Information: Logon Process: Advapi Authentication Package: Negotiate Transited Services: - Package Name (NTLM only): - Key Length: 0 This event is generated when a logon session is created. It is generated on the computer that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service such as the Server service, or a local process such as Winlogon.exe or Services.exe. The logon type field indicates the kind of logon that occurred. The most common types are 2 (interactive) and 3 (network). The New Logon fields indicate the account for whom the new logon was created, i.e. the account that was logged on. The network fields indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impersonation level field indicates the extent to which a process in the logon session can impersonate. The authentication information fields provide detailed information about this specific logon request. - Logon GUID is a unique identifier that can be used to correlate this event with a KDC event. - Transited services indicate which intermediate services have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indicates the length of the generated session key. This will be 0 if no session key was requested.
Security	Audit Success	12548	2015-04-24 19:57:41	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Logon ID: 0x3e7 Privileges: SeAssignPrimaryTokenPrivilege SeTcbPrivilege SeSecurityPrivilege SeTakeOwnershipPrivilege SeLoadDriverPrivilege SeBackupPrivilege SeRestorePrivilege

					SeDebugPrivilege SeAuditPrivilege SeSystemEnvironmentPrivilege SeImpersonatePrivilege
Security	Audit Success	12288	2015-04-24 20:35:18	Microsoft-Windows-Security-Auditing	4608: Windows is starting up. This event is logged when LSASS.EXE starts and the auditing subsystem is initialized.
Security	Audit Success	12544	2015-04-24 20:35:18	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-0-0 Account Name: - Account Domain: - Logon ID: 0x0 Logon Type: 0 Impersonation Level: - New Logon: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Logon ID: 0x3e7 Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x4 Process Name: Network Information: Workstation Name: - Source Network Address: - Source Port: - Detailed Authentication Information: Logon Process: - Authentication Package: - Transited Services: - Package Name (NTLM only): - Key Length: 0 This event is generated when a logon session is created. It is generated on the computer that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service such as the Server service, or a local process such as Winlogon.exe or Services.exe. The logon type field indicates the kind of logon that occurred. The most common types are 2 (interactive) and 3 (network). The New Logon fields indicate the account for whom the new logon was created, i.e. the account that was logged on. The network fields indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impersonation level field indicates the extent to which a process in the logon session can impersonate. The authentication information fields provide detailed information about this specific logon request. - Logon GUID is a unique identifier that can be used to correlate this event with a KDC event. - Transited services indicate which intermediate services have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indicates the length of the generated session key. This will be 0 if no session key was requested.
Security	Audit Success	12544	2015-04-24 20:35:18	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: LTRANPHD$ Account Domain: WORKGROUP Logon ID: 0x3e7 Logon Type: 5 Impersonation Level: %%1833 New Logon: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Logon ID: 0x3e7 Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x224 Process Name: C:\Windows\System32\services.exe Network Information: Workstation Name: Source Network Address: - Source Port: - Detailed Authentication Information: Logon Process: Advapi Authentication Package: Negotiate Transited Services: - Package Name (NTLM only): - Key Length: 0 This event is generated when a logon session is created. It is generated on the computer that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service such as the Server service, or a local process such as Winlogon.exe or Services.exe. The logon type field indicates the kind of logon that occurred. The most common types are 2 (interactive) and 3 (network). The New Logon fields indicate the account for whom the new logon was created, i.e. the account that was logged on. The network fields indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impersonation level field indicates the extent to which a process in the logon session can impersonate. The authentication information fields provide detailed information about this specific logon request. - Logon GUID is a unique identifier that can be used to correlate this event with a KDC event. - Transited services indicate which intermediate services have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indicates the length of the generated session key. This will be 0 if no session key was requested.
Security	Audit Success	12544	2015-04-24 20:35:18	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: LTRANPHD$ Account Domain: WORKGROUP Logon ID: 0x3e7 Logon Type: 5 Impersonation Level: %%1833 New Logon: Security ID: S-1-5-20 Account Name: NETWORK SERVICE Account Domain: NT AUTHORITY Logon ID: 0x3e4 Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x224 Process Name: C:\Windows\System32\services.exe Network Information: Workstation Name: Source Network Address: - Source Port: - Detailed Authentication Information: Logon Process: Advapi Authentication Package: Negotiate Transited Services: - Package Name (NTLM only): - Key Length: 0 This event is generated when a logon session is created. It is generated on the computer that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service such as the Server service, or a local process such as Winlogon.exe or Services.exe. The logon type field indicates the kind of logon that occurred. The most common types are 2 (interactive) and 3 (network). The New Logon fields indicate the account for whom the new logon was created, i.e. the account that was logged on. The network fields indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impersonation level field indicates the extent to which a process in the logon session can impersonate. The authentication information fields provide detailed information about this specific logon request. - Logon GUID is a unique identifier that can be used to correlate this event with a KDC event. - Transited services indicate which intermediate services have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indicates the length of the generated session key. This will be 0 if no session key was requested.
Security	Audit Success	12548	2015-04-24 20:35:18	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Logon ID: 0x3e7 Privileges: SeAssignPrimaryTokenPrivilege SeTcbPrivilege SeSecurityPrivilege SeTakeOwnershipPrivilege SeLoadDriverPrivilege SeBackupPrivilege SeRestorePrivilege SeDebugPrivilege SeAuditPrivilege SeSystemEnvironmentPrivilege SeImpersonatePrivilege
Security	Audit Success	12548	2015-04-24	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-20 Account Name: NETWORK SERVICE Account Domain: NT AUTHORITY Logon ID: 0x3e4 Privileges: SeAssignPrimaryTokenPrivilege

			20:35:18		SeAuditPrivilege SeImpersonatePrivilege
Security	Audit Success	13568	2015-04-24 20:35:18	Microsoft-Windows-Security-Auditing	4902: The Per-user audit policy table was created. Number of Elements: 0 Policy ID: 0xa202
Security	Audit Success	12544	2015-04-24 20:35:19	Microsoft-Windows-Security-Auditing	4648: A logon was attempted using explicit credentials. Subject: Security ID: S-1-5-18 Account Name: LTRANPHD$ Account Domain: WORKGROUP Logon ID: 0x3e7 Logon GUID: {00000000-0000-0000-0000-000000000000} Account Whose Credentials Were Used: Account Name: DWM-1 Account Domain: Window Manager Logon GUID: {00000000-0000-0000-0000-000000000000} Target Server: Target Server Name: localhost Additional Information: localhost Process Information: Process ID: 0x1fc Process Name: C:\Windows\System32\winlogon.exe Network Information: Network Address: - Port: - This event is generated when a process attempts to log on an account by explicitly specifying that account's credentials. This most commonly occurs in batch-type configurations such as scheduled tasks, or when using the RUNAS command.
Security	Audit Success	12544	2015-04-24 20:35:19	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: LTRANPHD$ Account Domain: WORKGROUP Logon ID: 0x3e7 Logon Type: 2 Impersonation Level: %%1833 New Logon: Security ID: S-1-5-90-1 Account Name: DWM-1 Account Domain: Window Manager Logon ID: 0xf27a Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x1fc Process Name: C:\Windows\System32\winlogon.exe Network Information: Workstation Name: Source Network Address: - Source Port: - Detailed Authentication Information: Logon Process: Advapi Authentication Package: Negotiate Transited Services: - Package Name (NTLM only): - Key Length: 0 This event is generated when a logon session is created. It is generated on the computer that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service such as the Server service, or a local process such as Winlogon.exe or Services.exe. The logon type field indicates the kind of logon that occurred. The most common types are 2 (interactive) and 3 (network). The New Logon fields indicate the account for whom the new logon was created, i.e. the account that was logged on. The network fields indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impersonation level field indicates the extent to which a process in the logon session can impersonate. The authentication information fields provide detailed information about this specific logon request. - Logon GUID is a unique identifier that can be used to correlate this event with a KDC event. - Transited services indicate which intermediate services have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indicates the length of the generated session key. This will be 0 if no session key was requested.
Security	Audit Success	12544	2015-04-24 20:35:19	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: LTRANPHD$ Account Domain: WORKGROUP Logon ID: 0x3e7 Logon Type: 2 Impersonation Level: %%1833 New Logon: Security ID: S-1-5-90-1 Account Name: DWM-1 Account Domain: Window Manager Logon ID: 0xf297 Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x1fc Process Name: C:\Windows\System32\winlogon.exe Network Information: Workstation Name: Source Network Address: - Source Port: - Detailed Authentication Information: Logon Process: Advapi Authentication Package: Negotiate Transited Services: - Package Name (NTLM only): - Key Length: 0 This event is generated when a logon session is created. It is generated on the computer that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service such as the Server service, or a local process such as Winlogon.exe or Services.exe. The logon type field indicates the kind of logon that occurred. The most common types are 2 (interactive) and 3 (network). The New Logon fields indicate the account for whom the new logon was created, i.e. the account that was logged on. The network fields indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impersonation level field indicates the extent to which a process in the logon session can impersonate. The authentication information fields provide detailed information about this specific logon request. - Logon GUID is a unique identifier that can be used to correlate this event with a KDC event. - Transited services indicate which intermediate services have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indicates the length of the generated session key. This will be 0 if no session key was requested.
Security	Audit Success	12544	2015-04-24 20:35:19	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: LTRANPHD$ Account Domain: WORKGROUP Logon ID: 0x3e7 Logon Type: 5 Impersonation Level: %%1833 New Logon: Security ID: S-1-5-19 Account Name: LOCAL SERVICE Account Domain: NT AUTHORITY Logon ID: 0x3e5 Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x224 Process Name: C:\Windows\System32\services.exe Network Information: Workstation Name: Source Network Address: - Source Port: - Detailed Authentication Information: Logon Process: Advapi Authentication Package: Negotiate Transited Services: - Package Name (NTLM only): - Key Length: 0 This event is generated when a logon session is created. It is generated on the computer that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service such as the Server service, or a local process such as Winlogon.exe or Services.exe. The logon type field indicates the kind of logon that occurred. The most common types are 2 (interactive) and 3 (network). The New Logon fields indicate the account for whom the new logon was created, i.e. the account that was logged on. The network fields indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impersonation level field indicates the extent to which a process in the logon session can impersonate. The authentication information fields provide detailed information about this specific logon request. - Logon GUID is a unique identifier that can be used to correlate this event with a KDC event. - Transited

					services indicate which intermediate services have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indicates the length of the generated session key. This will be 0 if no session key was requested.
Security	Audit Success	12544	2015-04-24 20:35:19	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: LTRANPHD$ Account Domain: WORKGROUP Logon ID: 0x3e7 Logon Type: 5 Impersonation Level: %%1833 New Logon: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Logon ID: 0x3e7 Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x224 Process Name: C:\Windows\System32\services.exe Network Information: Workstation Name: Source Network Address: - Source Port: - Detailed Authentication Information: Logon Process: Advapi Authentication Package: Negotiate Transited Services: - Package Name (NTLM only): - Key Length: 0 This event is generated when a logon session is created. It is generated on the computer that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service such as the Server service, or a local process such as Winlogon.exe or Services.exe. The logon type field indicates the kind of logon that occurred. The most common types are 2 (interactive) and 3 (network). The New Logon fields indicate the account for whom the new logon was created, i.e. the account that was logged on. The network fields indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impersonation level field indicates the extent to which a process in the logon session can impersonate. The authentication information fields provide detailed information about this specific logon request. - Logon GUID is a unique identifier that can be used to correlate this event with a KDC event. - Transited services indicate which intermediate services have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indicates the length of the generated session key. This will be 0 if no session key was requested.
Security	Audit Success	12544	2015-04-24 20:35:19	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: LTRANPHD$ Account Domain: WORKGROUP Logon ID: 0x3e7 Logon Type: 5 Impersonation Level: %%1833 New Logon: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Logon ID: 0x3e7 Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x224 Process Name: C:\Windows\System32\services.exe Network Information: Workstation Name: Source Network Address: - Source Port: - Detailed Authentication Information: Logon Process: Advapi Authentication Package: Negotiate Transited Services: - Package Name (NTLM only): - Key Length: 0 This event is generated when a logon session is created. It is generated on the computer that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service such as the Server service, or a local process such as Winlogon.exe or Services.exe. The logon type field indicates the kind of logon that occurred. The most common types are 2 (interactive) and 3 (network). The New Logon fields indicate the account for whom the new logon was created, i.e. the account that was logged on. The network fields indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impersonation level field indicates the extent to which a process in the logon session can impersonate. The authentication information fields provide detailed information about this specific logon request. - Logon GUID is a unique identifier that can be used to correlate this event with a KDC event. - Transited services indicate which intermediate services have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indicates the length of the generated session key. This will be 0 if no session key was requested.
Security	Audit Success	12548	2015-04-24 20:35:19	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-90-1 Account Name: DWM-1 Account Domain: Window Manager Logon ID: 0xf27a Privileges: SeAssignPrimaryTokenPrivilege SeAuditPrivilege SeImpersonatePrivilege
Security	Audit Success	12548	2015-04-24 20:35:19	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-90-1 Account Name: DWM-1 Account Domain: Window Manager Logon ID: 0xf297 Privileges: SeAssignPrimaryTokenPrivilege SeAuditPrivilege
Security	Audit Success	12548	2015-04-24 20:35:19	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-19 Account Name: LOCAL SERVICE Account Domain: NT AUTHORITY Logon ID: 0x3e5 Privileges: SeAssignPrimaryTokenPrivilege SeAuditPrivilege SeImpersonatePrivilege
Security	Audit Success	12548	2015-04-24 20:35:19	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Logon ID: 0x3e7 Privileges: SeAssignPrimaryTokenPrivilege SeTcbPrivilege SeSecurityPrivilege SeTakeOwnershipPrivilege SeLoadDriverPrivilege SeBackupPrivilege SeRestorePrivilege SeDebugPrivilege SeAuditPrivilege SeSystemEnvironmentPrivilege SeImpersonatePrivilege
Security	Audit Success	12548	2015-04-24 20:35:19	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Logon ID: 0x3e7 Privileges: SeAssignPrimaryTokenPrivilege SeTcbPrivilege SeSecurityPrivilege SeTakeOwnershipPrivilege SeLoadDriverPrivilege SeBackupPrivilege SeRestorePrivilege SeDebugPrivilege SeAuditPrivilege SeSystemEnvironmentPrivilege SeImpersonatePrivilege
Security	Audit Success	12292	2015-04-24 20:35:20	Microsoft-Windows-Security-Auditing	5033: The Windows Firewall Driver started successfully.
					4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: LTRANPHD$ Account Domain: WORKGROUP Logon ID: 0x3e7 Logon Type: 5 Impersonation Level: %%1833 New Logon: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Logon ID: 0x3e7 Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x224 Process Name:

Security	Audit Success	12544	2015-04-24 20:35:20	Microsoft-Windows-Security-Auditing	C:\Windows\System32\services.exe Network Information: Workstation Name: Source Network Address: - Source Port: - Detailed Authentication Information: Logon Process: Advapi Authentication Package: Negotiate Transited Services: - Package Name (NTLM only): - Key Length: 0 This event is generated when a logon session is created. It is generated on the computer that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service such as the Server service, or a local process such as Winlogon.exe or Services.exe. The logon type field indicates the kind of logon that occurred. The most common types are 2 (interactive) and 3 (network). The New Logon fields indicate the account for whom the new logon was created, i.e. the account that was logged on. The network fields indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impersonation level field indicates the extent to which a process in the logon session can impersonate. The authentication information fields provide detailed information about this specific logon request. - Logon GUID is a unique identifier that can be used to correlate this event with a KDC event. - Transited services indicate which intermediate services have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indicates the length of the generated session key. This will be 0 if no session key was requested.
Security	Audit Success	12544	2015-04-24 20:35:20	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: LTRANPHD$ Account Domain: WORKGROUP Logon ID: 0x3e7 Logon Type: 5 Impersonation Level: %%1833 New Logon: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Logon ID: 0x3e7 Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x224 Process Name: C:\Windows\System32\services.exe Network Information: Workstation Name: Source Network Address: - Source Port: - Detailed Authentication Information: Logon Process: Advapi Authentication Package: Negotiate Transited Services: - Package Name (NTLM only): - Key Length: 0 This event is generated when a logon session is created. It is generated on the computer that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service such as the Server service, or a local process such as Winlogon.exe or Services.exe. The logon type field indicates the kind of logon that occurred. The most common types are 2 (interactive) and 3 (network). The New Logon fields indicate the account for whom the new logon was created, i.e. the account that was logged on. The network fields indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impersonation level field indicates the extent to which a process in the logon session can impersonate. The authentication information fields provide detailed information about this specific logon request. - Logon GUID is a unique identifier that can be used to correlate this event with a KDC event. - Transited services indicate which intermediate services have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indicates the length of the generated session key. This will be 0 if no session key was requested.
Security	Audit Success	12544	2015-04-24 20:35:20	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: LTRANPHD$ Account Domain: WORKGROUP Logon ID: 0x3e7 Logon Type: 5 Impersonation Level: %%1833 New Logon: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Logon ID: 0x3e7 Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x224 Process Name: C:\Windows\System32\services.exe Network Information: Workstation Name: Source Network Address: - Source Port: - Detailed Authentication Information: Logon Process: Advapi Authentication Package: Negotiate Transited Services: - Package Name (NTLM only): - Key Length: 0 This event is generated when a logon session is created. It is generated on the computer that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service such as the Server service, or a local process such as Winlogon.exe or Services.exe. The logon type field indicates the kind of logon that occurred. The most common types are 2 (interactive) and 3 (network). The New Logon fields indicate the account for whom the new logon was created, i.e. the account that was logged on. The network fields indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impersonation level field indicates the extent to which a process in the logon session can impersonate. The authentication information fields provide detailed information about this specific logon request. - Logon GUID is a unique identifier that can be used to correlate this event with a KDC event. - Transited services indicate which intermediate services have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indicates the length of the generated session key. This will be 0 if no session key was requested.
Security	Audit Success	12548	2015-04-24 20:35:20	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Logon ID: 0x3e7 Privileges: SeAssignPrimaryTokenPrivilege SeTcbPrivilege SeSecurityPrivilege SeTakeOwnershipPrivilege SeLoadDriverPrivilege SeBackupPrivilege SeRestorePrivilege SeDebugPrivilege SeAuditPrivilege SeSystemEnvironmentPrivilege SeImpersonatePrivilege
Security	Audit Success	12548	2015-04-24 20:35:20	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Logon ID: 0x3e7 Privileges: SeAssignPrimaryTokenPrivilege SeTcbPrivilege SeSecurityPrivilege SeTakeOwnershipPrivilege SeLoadDriverPrivilege SeBackupPrivilege SeRestorePrivilege SeDebugPrivilege SeAuditPrivilege SeSystemEnvironmentPrivilege SeImpersonatePrivilege
Security	Audit Success	12548	2015-04-24 20:35:20	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Logon ID: 0x3e7 Privileges: SeAssignPrimaryTokenPrivilege SeTcbPrivilege SeSecurityPrivilege SeTakeOwnershipPrivilege SeLoadDriverPrivilege SeBackupPrivilege SeRestorePrivilege SeDebugPrivilege SeAuditPrivilege SeSystemEnvironmentPrivilege SeImpersonatePrivilege
	Audit		2015-04-	Microsoft-Windows-Security-	

Security	Success	12292	24 20:35:21	Auditing	5024: The Windows Firewall service started successfully.
Security	Audit Success	12544	2015-04-24 20:35:21	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-0-0 Account Name: - Account Domain: - Logon ID: 0x0 Logon Type: 3 Impersonation Level: %%1833 New Logon: Security ID: S-1-5-7 Account Name: ANONYMOUS LOGON Account Domain: NT AUTHORITY Logon ID: 0x1ad99 Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x0 Process Name: - Network Information: Workstation Name: Source Network Address: - Source Port: - Detailed Authentication Information: Logon Process: NtLmSsp Authentication Package: NTLM Transited Services: - Package Name (NTLM only): NTLM V1 Key Length: 0 This event is generated when a logon session is created. It is generated on the computer that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service such as the Server service, or a local process such as Winlogon.exe or Services.exe. The logon type field indicates the kind of logon that occurred. The most common types are 2 (interactive) and 3 (network). The New Logon fields indicate the account for whom the new logon was created, i.e. the account that was logged on. The network fields indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impersonation level field indicates the extent to which a process in the logon session can impersonate. The authentication information fields provide detailed information about this specific logon request. - Logon GUID is a unique identifier that can be used to correlate this event with a KDC event. - Transited services indicate which intermediate services have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indicates the length of the generated session key. This will be 0 if no session key was requested.
Security	Audit Success	12544	2015-04-24 20:35:24	Microsoft-Windows-Security-Auditing	4648: A logon was attempted using explicit credentials. Subject: Security ID: S-1-5-18 Account Name: LTRANPHD$ Account Domain: WORKGROUP Logon ID: 0x3e7 Logon GUID: {00000000-0000-0000-0000-000000000000} Account Whose Credentials Were Used: Account Name: Liem Account Domain: LTRANPHD Logon GUID: {00000000-0000-0000-0000-000000000000} Target Server: Target Server Name: localhost Additional Information: localhost Process Information: Process ID: 0x1fc Process Name: C:\Windows\System32\winlogon.exe Network Information: Network Address: 127.0.0.1 Port: 0 This event is generated when a process attempts to log on an account by explicitly specifying that account's credentials. This most commonly occurs in batch-type configurations such as scheduled tasks, or when using the RUNAS command.
Security	Audit Success	12544	2015-04-24 20:35:24	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: LTRANPHD$ Account Domain: WORKGROUP Logon ID: 0x3e7 Logon Type: 2 Impersonation Level: %%1833 New Logon: Security ID: S-1-5-21-1888849264-3803429180-4108621888-1001 Account Name: Liem Account Domain: LTRANPHD Logon ID: 0x1d4a8 Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x1fc Process Name: C:\Windows\System32\winlogon.exe Network Information: Workstation Name: LTRANPHD Source Network Address: 127.0.0.1 Source Port: 0 Detailed Authentication Information: Logon Process: User32 Authentication Package: Negotiate Transited Services: - Package Name (NTLM only): - Key Length: 0 This event is generated when a logon session is created. It is generated on the computer that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service such as the Server service, or a local process such as Winlogon.exe or Services.exe. The logon type field indicates the kind of logon that occurred. The most common types are 2 (interactive) and 3 (network). The New Logon fields indicate the account for whom the new logon was created, i.e. the account that was logged on. The network fields indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impersonation level field indicates the extent to which a process in the logon session can impersonate. The authentication information fields provide detailed information about this specific logon request. - Logon GUID is a unique identifier that can be used to correlate this event with a KDC event. - Transited services indicate which intermediate services have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indicates the length of the generated session key. This will be 0 if no session key was requested.
Security	Audit Success	12544	2015-04-24 20:35:24	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: LTRANPHD$ Account Domain: WORKGROUP Logon ID: 0x3e7 Logon Type: 2 Impersonation Level: %%1833 New Logon: Security ID: S-1-5-21-1888849264-3803429180-4108621888-1001 Account Name: Liem Account Domain: LTRANPHD Logon ID: 0x1d4d7 Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x1fc Process Name: C:\Windows\System32\winlogon.exe Network Information: Workstation Name: LTRANPHD Source Network Address: 127.0.0.1 Source Port: 0 Detailed Authentication Information: Logon Process: User32 Authentication Package: Negotiate Transited Services: - Package Name (NTLM only): - Key Length: 0 This event is generated when a logon session is created. It is generated on the computer that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service such as the Server service, or a local process such as Winlogon.exe or Services.exe. The logon type field indicates the kind of logon that occurred. The most common types are 2 (interactive) and 3 (network). The New Logon fields indicate the account for whom the new logon was created, i.e. the account that was logged on. The network fields indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impersonation level field indicates the extent to which a process in the logon session can impersonate. The authentication information fields provide detailed information about this specific logon request. - Logon GUID is a unique identifier that can be used to correlate this event with a KDC event. - Transited services indicate which intermediate services have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indicates the length of the generated session key. This will be 0 if no session key was requested.

Security	Audit Success	12544	2015-04-24 20:35:24	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: LTRANPHD$ Account Domain: WORKGROUP Logon ID: 0x3e7 Logon Type: 5 Impersonation Level: %%1833 New Logon: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Logon ID: 0x3e7 Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x224 Process Name: C:\Windows\System32\services.exe Network Information: Workstation Name: Source Network Address: - Source Port: - Detailed Authentication Information: Logon Process: Advapi Authentication Package: Negotiate Transited Services: - Package Name (NTLM only): - Key Length: 0 This event is generated when a logon session is created. It is generated on the computer that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service such as the Server service, or a local process such as Winlogon.exe or Services.exe. The logon type field indicates the kind of logon that occurred. The most common types are 2 (interactive) and 3 (network). The New Logon fields indicate the account for whom the new logon was created, i.e. the account that was logged on. The network fields indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impersonation level field indicates the extent to which a process in the logon session can impersonate. The authentication information fields provide detailed information about this specific logon request. - Logon GUID is a unique identifier that can be used to correlate this event with a KDC event. - Transited services indicate which intermediate services have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indicates the length of the generated session key. This will be 0 if no session key was requested.
Security	Audit Success	12544	2015-04-24 20:35:24	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: LTRANPHD$ Account Domain: WORKGROUP Logon ID: 0x3e7 Logon Type: 5 Impersonation Level: %%1833 New Logon: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Logon ID: 0x3e7 Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x224 Process Name: C:\Windows\System32\services.exe Network Information: Workstation Name: Source Network Address: - Source Port: - Detailed Authentication Information: Logon Process: Advapi Authentication Package: Negotiate Transited Services: - Package Name (NTLM only): - Key Length: 0 This event is generated when a logon session is created. It is generated on the computer that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service such as the Server service, or a local process such as Winlogon.exe or Services.exe. The logon type field indicates the kind of logon that occurred. The most common types are 2 (interactive) and 3 (network). The New Logon fields indicate the account for whom the new logon was created, i.e. the account that was logged on. The network fields indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impersonation level field indicates the extent to which a process in the logon session can impersonate. The authentication information fields provide detailed information about this specific logon request. - Logon GUID is a unique identifier that can be used to correlate this event with a KDC event. - Transited services indicate which intermediate services have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indicates the length of the generated session key. This will be 0 if no session key was requested.
Security	Audit Success	12548	2015-04-24 20:35:24	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-21-1888849264-3803429180-4108621888-1001 Account Name: Liem Account Domain: LTRANPHD Logon ID: 0x1d4a8 Privileges: SeSecurityPrivilege SeTakeOwnershipPrivilege SeLoadDriverPrivilege SeBackupPrivilege SeRestorePrivilege SeDebugPrivilege SeSystemEnvironmentPrivilege SeImpersonatePrivilege
Security	Audit Success	12548	2015-04-24 20:35:24	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Logon ID: 0x3e7 Privileges: SeAssignPrimaryTokenPrivilege SeTcbPrivilege SeSecurityPrivilege SeTakeOwnershipPrivilege SeLoadDriverPrivilege SeBackupPrivilege SeRestorePrivilege SeDebugPrivilege SeAuditPrivilege SeSystemEnvironmentPrivilege SeImpersonatePrivilege
Security	Audit Success	12548	2015-04-24 20:35:24	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Logon ID: 0x3e7 Privileges: SeAssignPrimaryTokenPrivilege SeTcbPrivilege SeSecurityPrivilege SeTakeOwnershipPrivilege SeLoadDriverPrivilege SeBackupPrivilege SeRestorePrivilege SeDebugPrivilege SeAuditPrivilege SeSystemEnvironmentPrivilege SeImpersonatePrivilege
Security	Audit Success	13824	2015-04-24 20:35:26	Microsoft-Windows-Security-Auditing	4797: An attempt was made to query the existence of a blank password for an account. Subject: Security ID: S-1-5-21-1888849264-3803429180-4108621888-1001 Account Name: Liem Account Domain: LTRANPHD Logon ID: 0x1d4d7 Additional Information: Caller Workstation: LTRANPHD Target Account Name: Administrator Target Account Domain: LTRANPHD
Security	Audit Success	13824	2015-04-24 20:35:26	Microsoft-Windows-Security-Auditing	4797: An attempt was made to query the existence of a blank password for an account. Subject: Security ID: S-1-5-21-1888849264-3803429180-4108621888-1001 Account Name: Liem Account Domain: LTRANPHD Logon ID: 0x1d4d7 Additional Information: Caller Workstation: LTRANPHD Target Account Name: Guest Target Account Domain: LTRANPHD
Security	Audit Success	13824	2015-04-24 20:35:26	Microsoft-Windows-Security-Auditing	4797: An attempt was made to query the existence of a blank password for an account. Subject: Security ID: S-1-5-21-1888849264-3803429180-4108621888-1001 Account Name: Liem Account Domain: LTRANPHD Logon ID: 0x1d4d7 Additional Information: Caller Workstation: LTRANPHD Target Account Name: Administrator Target Account Domain: LTRANPHD
Security	Audit Success	13824	2015-04-24 20:35:26	Microsoft-Windows-Security-Auditing	4797: An attempt was made to query the existence of a blank password for an account. Subject: Security ID: S-1-5-21-1888849264-3803429180-4108621888-1001 Account Name: Liem Account Domain: LTRANPHD Logon ID: 0x1d4d7 Additional Information: Caller Workstation: LTRANPHD Target Account Name: Guest Target Account Domain: LTRANPHD

Security	Audit Success	13824	2015-04-24 20:35:28	Microsoft-Windows-Security-Auditing	4797: An attempt was made to query the existence of a blank password for an account. Subject: Security ID: S-1-5-19 Account Name: LOCAL SERVICE Account Domain: NT AUTHORITY Logon ID: 0x3e5 Additional Information: Caller Workstation: LTRANPHD Target Account Name: Administrator Target Account Domain: LTRANPHD
Security	Audit Success	13824	2015-04-24 20:35:28	Microsoft-Windows-Security-Auditing	4797: An attempt was made to query the existence of a blank password for an account. Subject: Security ID: S-1-5-19 Account Name: LOCAL SERVICE Account Domain: NT AUTHORITY Logon ID: 0x3e5 Additional Information: Caller Workstation: LTRANPHD Target Account Name: Administrator Target Account Domain: LTRANPHD
Security	Audit Success	13824	2015-04-24 20:35:28	Microsoft-Windows-Security-Auditing	4797: An attempt was made to query the existence of a blank password for an account. Subject: Security ID: S-1-5-19 Account Name: LOCAL SERVICE Account Domain: NT AUTHORITY Logon ID: 0x3e5 Additional Information: Caller Workstation: LTRANPHD Target Account Name: Guest Target Account Domain: LTRANPHD
Security	Audit Success	13824	2015-04-24 20:35:28	Microsoft-Windows-Security-Auditing	4797: An attempt was made to query the existence of a blank password for an account. Subject: Security ID: S-1-5-19 Account Name: LOCAL SERVICE Account Domain: NT AUTHORITY Logon ID: 0x3e5 Additional Information: Caller Workstation: LTRANPHD Target Account Name: Guest Target Account Domain: LTRANPHD
Security	Audit Success	13824	2015-04-24 20:35:28	Microsoft-Windows-Security-Auditing	4797: An attempt was made to query the existence of a blank password for an account. Subject: Security ID: S-1-5-19 Account Name: LOCAL SERVICE Account Domain: NT AUTHORITY Logon ID: 0x3e5 Additional Information: Caller Workstation: LTRANPHD Target Account Name: Liem Target Account Domain: LTRANPHD
Security	Audit Success	13824	2015-04-24 20:35:28	Microsoft-Windows-Security-Auditing	4797: An attempt was made to query the existence of a blank password for an account. Subject: Security ID: S-1-5-19 Account Name: LOCAL SERVICE Account Domain: NT AUTHORITY Logon ID: 0x3e5 Additional Information: Caller Workstation: LTRANPHD Target Account Name: Liem Target Account Domain: LTRANPHD
Security	Audit Success	13824	2015-04-24 20:35:28	Microsoft-Windows-Security-Auditing	4797: An attempt was made to query the existence of a blank password for an account. Subject: Security ID: S-1-5-19 Account Name: LOCAL SERVICE Account Domain: NT AUTHORITY Logon ID: 0x3e5 Additional Information: Caller Workstation: LTRANPHD Target Account Name: Liem Target Account Domain: LTRANPHD
Security	Audit Success	13824	2015-04-24 20:35:28	Microsoft-Windows-Security-Auditing	4797: An attempt was made to query the existence of a blank password for an account. Subject: Security ID: S-1-5-19 Account Name: LOCAL SERVICE Account Domain: NT AUTHORITY Logon ID: 0x3e5 Additional Information: Caller Workstation: LTRANPHD Target Account Name: Liem Target Account Domain: LTRANPHD
Security	Audit Success	103	2015-04-24 20:45:52	Microsoft-Windows-Eventlog	1100: The event logging service has shut down.
Security	Audit Success	12545	2015-04-24 20:45:52	Microsoft-Windows-Security-Auditing	4647: User initiated logoff: Subject: Security ID: S-1-5-21-1888849264-3803429180-4108621888-1001 Account Name: Liem Account Domain: LTRANPHD Logon ID: 0x1d4d7 This event is generated when a logoff is initiated. No further user-initiated activity can occur. This event can be interpreted as a logoff event.
Security	Audit Success	12288	2015-04-24 20:47:05	Microsoft-Windows-Security-Auditing	4608: Windows is starting up. This event is logged when LSASS.EXE starts and the auditing subsystem is initialized.
Security	Audit Success	12292	2015-04-24 20:47:05	Microsoft-Windows-Security-Auditing	5033: The Windows Firewall Driver started successfully.
Security	Audit Success	12544	2015-04-24 20:47:05	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-0-0 Account Name: - Account Domain: - Logon ID: 0x0 Logon Type: 0 Impersonation Level: - New Logon: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Logon ID: 0x3e7 Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x4 Process Name: Network Information: Workstation Name: - Source Network Address: - Source Port: - Detailed Authentication Information: Logon Process: - Authentication Package: - Transited Services: - Package Name (NTLM only): - Key Length: 0 This event is generated when a logon session is created. It is generated on the computer that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service such as the Server service, or a local process such as Winlogon.exe or Services.exe. The logon type field indicates the kind of logon that occurred. The most common types are 2 (interactive) and 3 (network). The New Logon fields indicate the account for whom the new logon was created, i.e. the account that was logged on. The network fields indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impersonation level field indicates the extent to which a process in the logon session can impersonate. The authentication information fields provide detailed information about this specific logon request. - Logon GUID is a unique identifier that can be used to correlate this event with a KDC event. - Transited services indicate which intermediate services have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indicates the length of the generated session key. This will be 0 if no session key was requested.
					4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: LTRANPHD$ Account Domain: WORKGROUP Logon ID: 0x3e7 Logon Type: 5 Impersonation Level: %%1833 New Logon: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Logon ID: 0x3e7 Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x1f0 Process Name: C:\Windows\System32\services.exe Network Information: Workstation Name: Source Network Address: - Source Port: - Detailed Authentication Information: Logon Process: Advapi Authentication Package: Negotiate Transited Services: - Package Name (NTLM only): - Key Length: 0 This event is generated when a logon session is created. It is generated on the computer that was accessed. The subject fields indicate the account on the local

Security	Audit Success	12544	2015-04-24 20:47:05	Microsoft-Windows-Security-Auditing	system which requested the logon. This is most commonly a service such as the Server service, or a local process such as Winlogon.exe or Services.exe. The logon type field indicates the kind of logon that occurred. The most common types are 2 (interactive) and 3 (network). The New Logon fields indicate the account for whom the new logon was created, i.e. the account that was logged on. The network fields indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impersonation level field indicates the extent to which a process in the logon session can impersonate. The authentication information fields provide detailed information about this specific logon request. - Logon GUID is a unique identifier that can be used to correlate this event with a KDC event. - Transited services indicate which intermediate services have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indicates the length of the generated session key. This will be 0 if no session key was requested.
Security	Audit Success	12544	2015-04-24 20:47:05	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: LTRANPHD$ Account Domain: WORKGROUP Logon ID: 0x3e7 Logon Type: 5 Impersonation Level: %%1833 New Logon: Security ID: S-1-5-20 Account Name: NETWORK SERVICE Account Domain: NT AUTHORITY Logon ID: 0x3e4 Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x1f0 Process Name: C:\Windows\System32\services.exe Network Information: Workstation Name: Source Network Address: - Source Port: - Detailed Authentication Information: Logon Process: Advapi Authentication Package: Negotiate Transited Services: - Package Name (NTLM only): - Key Length: 0 This event is generated when a logon session is created. It is generated on the computer that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service such as the Server service, or a local process such as Winlogon.exe or Services.exe. The logon type field indicates the kind of logon that occurred. The most common types are 2 (interactive) and 3 (network). The New Logon fields indicate the account for whom the new logon was created, i.e. the account that was logged on. The network fields indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impersonation level field indicates the extent to which a process in the logon session can impersonate. The authentication information fields provide detailed information about this specific logon request. - Logon GUID is a unique identifier that can be used to correlate this event with a KDC event. - Transited services indicate which intermediate services have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indicates the length of the generated session key. This will be 0 if no session key was requested.
Security	Audit Success	12544	2015-04-24 20:47:05	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: LTRANPHD$ Account Domain: WORKGROUP Logon ID: 0x3e7 Logon Type: 5 Impersonation Level: %%1833 New Logon: Security ID: S-1-5-19 Account Name: LOCAL SERVICE Account Domain: NT AUTHORITY Logon ID: 0x3e5 Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x1f0 Process Name: C:\Windows\System32\services.exe Network Information: Workstation Name: Source Network Address: - Source Port: - Detailed Authentication Information: Logon Process: Advapi Authentication Package: Negotiate Transited Services: - Package Name (NTLM only): - Key Length: 0 This event is generated when a logon session is created. It is generated on the computer that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service such as the Server service, or a local process such as Winlogon.exe or Services.exe. The logon type field indicates the kind of logon that occurred. The most common types are 2 (interactive) and 3 (network). The New Logon fields indicate the account for whom the new logon was created, i.e. the account that was logged on. The network fields indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impersonation level field indicates the extent to which a process in the logon session can impersonate. The authentication information fields provide detailed information about this specific logon request. - Logon GUID is a unique identifier that can be used to correlate this event with a KDC event. - Transited services indicate which intermediate services have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indicates the length of the generated session key. This will be 0 if no session key was requested.
Security	Audit Success	12544	2015-04-24 20:47:05	Microsoft-Windows-Security-Auditing	4648: A logon was attempted using explicit credentials. Subject: Security ID: S-1-5-18 Account Name: LTRANPHD$ Account Domain: WORKGROUP Logon ID: 0x3e7 Logon GUID: {00000000-0000-0000-0000-000000000000} Account Whose Credentials Were Used: Account Name: DWM-1 Account Domain: Window Manager Logon GUID: {00000000-0000-0000-0000-000000000000} Target Server: Target Server Name: localhost Additional Information: localhost Process Information: Process ID: 0x208 Process Name: C:\Windows\System32\winlogon.exe Network Information: Network Address: - Port: - This event is generated when a process attempts to log on an account by explicitly specifying that account's credentials. This most commonly occurs in batch-type configurations such as scheduled tasks, or when using the RUNAS command.
Security	Audit	12544	2015-04-24	Microsoft-Windows-Security-	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: LTRANPHD$ Account Domain: WORKGROUP Logon ID: 0x3e7 Logon Type: 2 Impersonation Level: %%1833 New Logon: Security ID: S-1-5-90-1 Account Name: DWM-1 Account Domain: Window Manager Logon ID: 0xfd5a Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x208 Process Name: C:\Windows\System32\winlogon.exe Network Information: Workstation Name: Source Network Address: - Source Port: - Detailed Authentication Information: Logon Process: Advapi Authentication Package: Negotiate Transited Services: - Package Name (NTLM only): - Key Length: 0 This event is generated when a logon session is created. It is generated on the computer that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service such as the Server service, or a local process such as Winlogon.exe or Services.exe. The logon type field indicates the kind of logon that occurred.

	Success		20:47:05	Auditing	The most common types are 2 (interactive) and 3 (network). The New Logon fields indicate the account for whom the new logon was created, i.e. the account that was logged on. The network fields indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impersonation level field indicates the extent to which a process in the logon session can impersonate. The authentication information fields provide detailed information about this specific logon request. - Logon GUID is a unique identifier that can be used to correlate this event with a KDC event. - Transited services indicate which intermediate services have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indicates the length of the generated session key. This will be 0 if no session key was requested.
Security	Audit Success	12544	2015-04-24 20:47:05	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: LTRANPHD$ Account Domain: WORKGROUP Logon ID: 0x3e7 Logon Type: 5 Impersonation Level: %%1833 New Logon: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Logon ID: 0x3e7 Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x1f0 Process Name: C:\Windows\System32\services.exe Network Information: Workstation Name: Source Network Address: - Source Port: - Detailed Authentication Information: Logon Process: Advapi Authentication Package: Negotiate Transited Services: - Package Name (NTLM only): - Key Length: 0 This event is generated when a logon session is created. It is generated on the computer that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service such as the Server service, or a local process such as Winlogon.exe or Services.exe. The logon type field indicates the kind of logon that occurred. The most common types are 2 (interactive) and 3 (network). The New Logon fields indicate the account for whom the new logon was created, i.e. the account that was logged on. The network fields indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impersonation level field indicates the extent to which a process in the logon session can impersonate. The authentication information fields provide detailed information about this specific logon request. - Logon GUID is a unique identifier that can be used to correlate this event with a KDC event. - Transited services indicate which intermediate services have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indicates the length of the generated session key. This will be 0 if no session key was requested.
Security	Audit Success	12544	2015-04-24 20:47:05	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: LTRANPHD$ Account Domain: WORKGROUP Logon ID: 0x3e7 Logon Type: 5 Impersonation Level: %%1833 New Logon: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Logon ID: 0x3e7 Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x1f0 Process Name: C:\Windows\System32\services.exe Network Information: Workstation Name: Source Network Address: - Source Port: - Detailed Authentication Information: Logon Process: Advapi Authentication Package: Negotiate Transited Services: - Package Name (NTLM only): - Key Length: 0 This event is generated when a logon session is created. It is generated on the computer that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service such as the Server service, or a local process such as Winlogon.exe or Services.exe. The logon type field indicates the kind of logon that occurred. The most common types are 2 (interactive) and 3 (network). The New Logon fields indicate the account for whom the new logon was created, i.e. the account that was logged on. The network fields indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impersonation level field indicates the extent to which a process in the logon session can impersonate. The authentication information fields provide detailed information about this specific logon request. - Logon GUID is a unique identifier that can be used to correlate this event with a KDC event. - Transited services indicate which intermediate services have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indicates the length of the generated session key. This will be 0 if no session key was requested.
Security	Audit Success	12548	2015-04-24 20:47:05	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Logon ID: 0x3e7 Privileges: SeAssignPrimaryTokenPrivilege SeTcbPrivilege SeSecurityPrivilege SeTakeOwnershipPrivilege SeLoadDriverPrivilege SeBackupPrivilege SeRestorePrivilege SeDebugPrivilege SeAuditPrivilege SeSystemEnvironmentPrivilege SeImpersonatePrivilege
Security	Audit Success	12548	2015-04-24 20:47:05	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-20 Account Name: NETWORK SERVICE Account Domain: NT AUTHORITY Logon ID: 0x3e4 Privileges: SeAssignPrimaryTokenPrivilege SeAuditPrivilege SeImpersonatePrivilege
Security	Audit Success	12548	2015-04-24 20:47:05	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-19 Account Name: LOCAL SERVICE Account Domain: NT AUTHORITY Logon ID: 0x3e5 Privileges: SeAssignPrimaryTokenPrivilege SeAuditPrivilege SeImpersonatePrivilege
Security	Audit Success	12548	2015-04-24 20:47:05	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-90-1 Account Name: DWM-1 Account Domain: Window Manager Logon ID: 0xfd5a Privileges: SeAssignPrimaryTokenPrivilege SeAuditPrivilege SeImpersonatePrivilege
Security	Audit Success	12548	2015-04-24 20:47:05	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Logon ID: 0x3e7 Privileges: SeAssignPrimaryTokenPrivilege SeTcbPrivilege SeSecurityPrivilege SeTakeOwnershipPrivilege SeLoadDriverPrivilege SeBackupPrivilege SeRestorePrivilege SeDebugPrivilege SeAuditPrivilege SeSystemEnvironmentPrivilege SeImpersonatePrivilege
			2015-04-		4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account

Security	Audit Success	12548	24 20:47:05	Microsoft-Windows-Security-Auditing	Domain: NT AUTHORITY Logon ID: 0x3e7 Privileges: SeAssignPrimaryTokenPrivilege SeTcbPrivilege SeSecurityPrivilege SeTakeOwnershipPrivilege SeLoadDriverPrivilege SeBackupPrivilege SeRestorePrivilege SeDebugPrivilege SeAuditPrivilege SeSystemEnvironmentPrivilege SeImpersonatePrivilege
Security	Audit Success	13568	2015-04-24 20:47:05	Microsoft-Windows-Security-Auditing	4902: The Per-user audit policy table was created. Number of Elements: 0 Policy ID: 0x9638
Security	Audit Success	12292	2015-04-24 20:47:06	Microsoft-Windows-Security-Auditing	5024: The Windows Firewall service started successfully.
Security	Audit Success	12544	2015-04-24 20:47:06	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: LTRANPHD$ Account Domain: WORKGROUP Logon ID: 0x3e7 Logon Type: 5 Impersonation Level: %%1833 New Logon: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Logon ID: 0x3e7 Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x1f0 Process Name: C:\Windows\System32\services.exe Network Information: Workstation Name: Source Network Address: - Source Port: - Detailed Authentication Information: Logon Process: Advapi Authentication Package: Negotiate Transited Services: - Package Name (NTLM only): - Key Length: 0 This event is generated when a logon session is created. It is generated on the computer that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service such as the Server service, or a local process such as Winlogon.exe or Services.exe. The logon type field indicates the kind of logon that occurred. The most common types are 2 (interactive) and 3 (network). The New Logon fields indicate the account for whom the new logon was created, i.e. the account that was logged on. The network fields indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impersonation level field indicates the extent to which a process in the logon session can impersonate. The authentication information fields provide detailed information about this specific logon request. - Logon GUID is a unique identifier that can be used to correlate this event with a KDC event. - Transited services indicate which intermediate services have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indicates the length of the generated session key. This will be 0 if no session key was requested.
Security	Audit Success	12548	2015-04-24 20:47:06	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Logon ID: 0x3e7 Privileges: SeAssignPrimaryTokenPrivilege SeTcbPrivilege SeSecurityPrivilege SeTakeOwnershipPrivilege SeLoadDriverPrivilege SeBackupPrivilege SeRestorePrivilege SeDebugPrivilege SeAuditPrivilege SeSystemEnvironmentPrivilege SeImpersonatePrivilege
Security	Audit Success	12544	2015-04-24 20:47:14	Microsoft-Windows-Security-Auditing	4648: A logon was attempted using explicit credentials. Subject: Security ID: S-1-5-18 Account Name: LTRANPHD$ Account Domain: WORKGROUP Logon ID: 0x3e7 Logon GUID: {00000000-0000-0000-0000-000000000000} Account Whose Credentials Were Used: Account Name: Liem Account Domain: LTRANPHD Logon GUID: {00000000-0000-0000-0000-000000000000} Target Server: Target Server Name: localhost Additional Information: localhost Process Information: Process ID: 0x208 Process Name: C:\Windows\System32\winlogon.exe Network Information: Network Address: 127.0.0.1 Port: 0 This event is generated when a process attempts to log on an account by explicitly specifying that account's credentials. This most commonly occurs in batch-type configurations such as scheduled tasks, or when using the RUNAS command.
Security	Audit Success	12544	2015-04-24 20:47:14	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: LTRANPHD$ Account Domain: WORKGROUP Logon ID: 0x3e7 Logon Type: 2 Impersonation Level: %%1833 New Logon: Security ID: S-1-5-21-1888849264-3803429180-4108621888-1001 Account Name: Liem Account Domain: LTRANPHD Logon ID: 0x16713 Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x208 Process Name: C:\Windows\System32\winlogon.exe Network Information: Workstation Name: LTRANPHD Source Network Address: 127.0.0.1 Source Port: 0 Detailed Authentication Information: Logon Process: User32 Authentication Package: Negotiate Transited Services: - Package Name (NTLM only): - Key Length: 0 This event is generated when a logon session is created. It is generated on the computer that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service such as the Server service, or a local process such as Winlogon.exe or Services.exe. The logon type field indicates the kind of logon that occurred. The most common types are 2 (interactive) and 3 (network). The New Logon fields indicate the account for whom the new logon was created, i.e. the account that was logged on. The network fields indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impersonation level field indicates the extent to which a process in the logon session can impersonate. The authentication information fields provide detailed information about this specific logon request. - Logon GUID is a unique identifier that can be used to correlate this event with a KDC event. - Transited services indicate which intermediate services have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indicates the length of the generated session key. This will be 0 if no session key was requested.
Security	Audit Success	12548	2015-04-24 20:47:14	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-21-1888849264-3803429180-4108621888-1001 Account Name: Liem Account Domain: LTRANPHD Logon ID: 0x16713 Privileges: SeSecurityPrivilege SeTakeOwnershipPrivilege SeLoadDriverPrivilege SeBackupPrivilege SeRestorePrivilege SeDebugPrivilege SeSystemEnvironmentPrivilege SeImpersonatePrivilege
Security	Audit	103	2015-04-24	Microsoft-Windows-Eventlog	1100: The event logging service has shut down.

	Success		20:48:58		
Security	Audit Success	12545	2015-04-24 20:48:58	Microsoft-Windows-Security-Auditing	4647: User initiated logoff: Subject: Security ID: S-1-5-21-1888849264-3803429180-4108621888-1001 Account Name: Liem Account Domain: LTRANPHD Logon ID: 0x16713 This event is generated when a logoff is initiated. No further user-initiated activity can occur. This event can be interpreted as a logoff event.
Security	Audit Success	12288	2015-04-24 20:49:11	Microsoft-Windows-Security-Auditing	4608: Windows is starting up. This event is logged when LSASS.EXE starts and the auditing subsystem is initialized.
Security	Audit Success	12292	2015-04-24 20:49:11	Microsoft-Windows-Security-Auditing	5033: The Windows Firewall Driver started successfully.
Security	Audit Success	12544	2015-04-24 20:49:11	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-0-0 Account Name: - Account Domain: - Logon ID: 0x0 Logon Type: 0 Impersonation Level: - New Logon: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Logon ID: 0x3e7 Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x4 Process Name: Network Information: Workstation Name: - Source Network Address: - Source Port: - Detailed Authentication Information: Logon Process: - Authentication Package: - Transited Services: - Package Name (NTLM only): - Key Length: 0 This event is generated when a logon session is created. It is generated on the computer that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service such as the Server service, or a local process such as Winlogon.exe or Services.exe. The logon type field indicates the kind of logon that occurred. The most common types are 2 (interactive) and 3 (network). The New Logon fields indicate the account for whom the new logon was created, i.e. the account that was logged on. The network fields indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impersonation level field indicates the extent to which a process in the logon session can impersonate. The authentication information fields provide detailed information about this specific logon request. - Logon GUID is a unique identifier that can be used to correlate this event with a KDC event. - Transited services indicate which intermediate services have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indicates the length of the generated session key. This will be 0 if no session key was requested.
Security	Audit Success	12544	2015-04-24 20:49:11	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: LTRANPHD$ Account Domain: WORKGROUP Logon ID: 0x3e7 Logon Type: 5 Impersonation Level: %%1833 New Logon: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Logon ID: 0x3e7 Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x234 Process Name: C:\Windows\System32\services.exe Network Information: Workstation Name: Source Network Address: - Source Port: - Detailed Authentication Information: Logon Process: Advapi Authentication Package: Negotiate Transited Services: - Package Name (NTLM only): - Key Length: 0 This event is generated when a logon session is created. It is generated on the computer that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service such as the Server service, or a local process such as Winlogon.exe or Services.exe. The logon type field indicates the kind of logon that occurred. The most common types are 2 (interactive) and 3 (network). The New Logon fields indicate the account for whom the new logon was created, i.e. the account that was logged on. The network fields indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impersonation level field indicates the extent to which a process in the logon session can impersonate. The authentication information fields provide detailed information about this specific logon request. - Logon GUID is a unique identifier that can be used to correlate this event with a KDC event. - Transited services indicate which intermediate services have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indicates the length of the generated session key. This will be 0 if no session key was requested.
Security	Audit Success	12544	2015-04-24 20:49:11	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: LTRANPHD$ Account Domain: WORKGROUP Logon ID: 0x3e7 Logon Type: 5 Impersonation Level: %%1833 New Logon: Security ID: S-1-5-20 Account Name: NETWORK SERVICE Account Domain: NT AUTHORITY Logon ID: 0x3e4 Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x234 Process Name: C:\Windows\System32\services.exe Network Information: Workstation Name: Source Network Address: - Source Port: - Detailed Authentication Information: Logon Process: Advapi Authentication Package: Negotiate Transited Services: - Package Name (NTLM only): - Key Length: 0 This event is generated when a logon session is created. It is generated on the computer that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service such as the Server service, or a local process such as Winlogon.exe or Services.exe. The logon type field indicates the kind of logon that occurred. The most common types are 2 (interactive) and 3 (network). The New Logon fields indicate the account for whom the new logon was created, i.e. the account that was logged on. The network fields indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impersonation level field indicates the extent to which a process in the logon session can impersonate. The authentication information fields provide detailed information about this specific logon request. - Logon GUID is a unique identifier that can be used to correlate this event with a KDC event. - Transited services indicate which intermediate services have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indicates the length of the generated session key. This will be 0 if no session key was requested.

Security	Audit Success	12544	2015-04-24 20:49:11	Microsoft-Windows-Security-Auditing	4648: A logon was attempted using explicit credentials. Subject: Security ID: S-1-5-18 Account Name: LTRANPHD$ Account Domain: WORKGROUP Logon ID: 0x3e7 Logon GUID: {00000000-0000-0000-0000-000000000000} Account Whose Credentials Were Used: Account Name: DWM-1 Account Domain: Window Manager Logon GUID: {00000000-0000-0000-0000-000000000000} Target Server: Target Server Name: localhost Additional Information: localhost Process Information: Process ID: 0x204 Process Name: C:\Windows\System32\winlogon.exe Network Information: Network Address: - Port: - This event is generated when a process attempts to log on an account by explicitly specifying that account's credentials. This most commonly occurs in batch-type configurations such as scheduled tasks, or when using the RUNAS command.
Security	Audit Success	12544	2015-04-24 20:49:11	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: LTRANPHD$ Account Domain: WORKGROUP Logon ID: 0x3e7 Logon Type: 2 Impersonation Level: %%1833 New Logon: Security ID: S-1-5-90-1 Account Name: DWM-1 Account Domain: Window Manager Logon ID: 0xc9d0 Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x204 Process Name: C:\Windows\System32\winlogon.exe Network Information: Workstation Name: Source Network Address: - Source Port: - Detailed Authentication Information: Logon Process: Advapi Authentication Package: Negotiate Transited Services: - Package Name (NTLM only): - Key Length: 0 This event is generated when a logon session is created. It is generated on the computer that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service such as the Server service, or a local process such as Winlogon.exe or Services.exe. The logon type field indicates the kind of logon that occurred. The most common types are 2 (interactive) and 3 (network). The New Logon fields indicate the account for whom the new logon was created, i.e. the account that was logged on. The network fields indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impersonation level field indicates the extent to which a process in the logon session can impersonate. The authentication information fields provide detailed information about this specific logon request. - Logon GUID is a unique identifier that can be used to correlate this event with a KDC event. - Transited services indicate which intermediate services have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indicates the length of the generated session key. This will be 0 if no session key was requested.
Security	Audit Success	12544	2015-04-24 20:49:11	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: LTRANPHD$ Account Domain: WORKGROUP Logon ID: 0x3e7 Logon Type: 2 Impersonation Level: %%1833 New Logon: Security ID: S-1-5-90-1 Account Name: DWM-1 Account Domain: Window Manager Logon ID: 0xc9f0 Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x204 Process Name: C:\Windows\System32\winlogon.exe Network Information: Workstation Name: Source Network Address: - Source Port: - Detailed Authentication Information: Logon Process: Advapi Authentication Package: Negotiate Transited Services: - Package Name (NTLM only): - Key Length: 0 This event is generated when a logon session is created. It is generated on the computer that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service such as the Server service, or a local process such as Winlogon.exe or Services.exe. The logon type field indicates the kind of logon that occurred. The most common types are 2 (interactive) and 3 (network). The New Logon fields indicate the account for whom the new logon was created, i.e. the account that was logged on. The network fields indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impersonation level field indicates the extent to which a process in the logon session can impersonate. The authentication information fields provide detailed information about this specific logon request. - Logon GUID is a unique identifier that can be used to correlate this event with a KDC event. - Transited services indicate which intermediate services have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indicates the length of the generated session key. This will be 0 if no session key was requested.
Security	Audit Success	12544	2015-04-24 20:49:11	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-19 Account Name: LOCAL SERVICE Account Domain: NT AUTHORITY Logon ID: 0x3e5 Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x234 Process Name: C:\Windows\System32\services.exe Network Information: Workstation Name: Source Network Address: - Source Port: - Detailed Authentication Information: Logon Process: Advapi Authentication Package: Negotiate Transited Services: - Package Name (NTLM only): - Key Length: 0 This event is generated when a logon session is created. It is generated on the computer that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service such as the Server service, or a local process such as Winlogon.exe or Services.exe. The logon type field indicates the kind of logon that occurred. The most common types are 2 (interactive) and 3 (network). The New Logon fields indicate the account for whom the new logon was created, i.e. the account that was logged on. The network fields indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impersonation level field indicates the extent to which a process in the logon session can impersonate. The authentication information fields provide detailed information about this specific logon request. - Logon GUID is a unique identifier that can be used to correlate this event with a KDC event. - Transited services indicate which intermediate services have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indicates the length of the generated session key. This will be 0 if no session key was requested.
					4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: LTRANPHD$ Account Domain: WORKGROUP Logon ID: 0x3e7 Logon Type: 5 Impersonation Level: %%1833 New Logon:

Security	Audit Success	12544	2015-04-24 20:49:11	Microsoft-Windows-Security-Auditing	Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Logon ID: 0x3e7 Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x234 Process Name: C:\Windows\System32\services.exe Network Information: Workstation Name: Source Network Address: - Source Port: - Detailed Authentication Information: Logon Process: Advapi Authentication Package: Negotiate Transited Services: - Package Name (NTLM only): - Key Length: 0 This event is generated when a logon session is created. It is generated on the computer that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service such as the Server service, or a local process such as Winlogon.exe or Services.exe. The logon type field indicates the kind of logon that occurred. The most common types are 2 (interactive) and 3 (network). The New Logon fields indicate the account for whom the new logon was created, i.e. the account that was logged on. The network fields indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impersonation level field indicates the extent to which a process in the logon session can impersonate. The authentication information fields provide detailed information about this specific logon request. - Logon GUID is a unique identifier that can be used to correlate this event with a KDC event. - Transited services indicate which intermediate services have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indicates the length of the generated session key. This will be 0 if no session key was requested.
Security	Audit Success	12544	2015-04-24 20:49:11	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: LTRANPHD$ Account Domain: WORKGROUP Logon ID: 0x3e7 Logon Type: 5 Impersonation Level: %%1833 New Logon: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Logon ID: 0x3e7 Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x234 Process Name: C:\Windows\System32\services.exe Network Information: Workstation Name: Source Network Address: - Source Port: - Detailed Authentication Information: Logon Process: Advapi Authentication Package: Negotiate Transited Services: - Package Name (NTLM only): - Key Length: 0 This event is generated when a logon session is created. It is generated on the computer that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service such as the Server service, or a local process such as Winlogon.exe or Services.exe. The logon type field indicates the kind of logon that occurred. The most common types are 2 (interactive) and 3 (network). The New Logon fields indicate the account for whom the new logon was created, i.e. the account that was logged on. The network fields indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impersonation level field indicates the extent to which a process in the logon session can impersonate. The authentication information fields provide detailed information about this specific logon request. - Logon GUID is a unique identifier that can be used to correlate this event with a KDC event. - Transited services indicate which intermediate services have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indicates the length of the generated session key. This will be 0 if no session key was requested.
Security	Audit Success	12544	2015-04-24 20:49:11	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: LTRANPHD$ Account Domain: WORKGROUP Logon ID: 0x3e7 Logon Type: 5 Impersonation Level: %%1833 New Logon: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Logon ID: 0x3e7 Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x234 Process Name: C:\Windows\System32\services.exe Network Information: Workstation Name: Source Network Address: - Source Port: - Detailed Authentication Information: Logon Process: Advapi Authentication Package: Negotiate Transited Services: - Package Name (NTLM only): - Key Length: 0 This event is generated when a logon session is created. It is generated on the computer that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service such as the Server service, or a local process such as Winlogon.exe or Services.exe. The logon type field indicates the kind of logon that occurred. The most common types are 2 (interactive) and 3 (network). The New Logon fields indicate the account for whom the new logon was created, i.e. the account that was logged on. The network fields indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impersonation level field indicates the extent to which a process in the logon session can impersonate. The authentication information fields provide detailed information about this specific logon request. - Logon GUID is a unique identifier that can be used to correlate this event with a KDC event. - Transited services indicate which intermediate services have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indicates the length of the generated session key. This will be 0 if no session key was requested.
Security	Audit Success	12544	2015-04-24 20:49:11	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: LTRANPHD$ Account Domain: WORKGROUP Logon ID: 0x3e7 Logon Type: 5 Impersonation Level: %%1833 New Logon: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Logon ID: 0x3e7 Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x234 Process Name: C:\Windows\System32\services.exe Network Information: Workstation Name: Source Network Address: - Source Port: - Detailed Authentication Information: Logon Process: Advapi Authentication Package: Negotiate Transited Services: - Package Name (NTLM only): - Key Length: 0 This event is generated when a logon session is created. It is generated on the computer that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service such as the Server service, or a local process such as Winlogon.exe or Services.exe. The logon type field indicates the kind of logon that occurred. The most common types are 2 (interactive) and 3 (network). The New Logon fields indicate the account for whom the new logon was created, i.e. the account that was logged on. The network fields indicate where a

						remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impersonation level field indicates the extent to which a process in the logon session can impersonate. The authentication information fields provide detailed information about this specific logon request. - Logon GUID is a unique identifier that can be used to correlate this event with a KDC event. - Transited services indicate which intermediate services have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indicates the length of the generated session key. This will be 0 if no session key was requested.
Security	Audit Success	12548	2015-04-24 20:49:11		Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Logon ID: 0x3e7 Privileges: SeAssignPrimaryTokenPrivilege SeTcbPrivilege SeSecurityPrivilege SeTakeOwnershipPrivilege SeLoadDriverPrivilege SeBackupPrivilege SeRestorePrivilege SeDebugPrivilege SeAuditPrivilege SeSystemEnvironmentPrivilege SeImpersonatePrivilege
Security	Audit Success	12548	2015-04-24 20:49:11		Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-20 Account Name: NETWORK SERVICE Account Domain: NT AUTHORITY Logon ID: 0x3e4 Privileges: SeAssignPrimaryTokenPrivilege SeAuditPrivilege SeImpersonatePrivilege
Security	Audit Success	12548	2015-04-24 20:49:11		Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-90-1 Account Name: DWM-1 Account Domain: Window Manager Logon ID: 0xc9d0 Privileges: SeAssignPrimaryTokenPrivilege SeAuditPrivilege SeImpersonatePrivilege
Security	Audit Success	12548	2015-04-24 20:49:11		Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-90-1 Account Name: DWM-1 Account Domain: Window Manager Logon ID: 0xc9f0 Privileges: SeAssignPrimaryTokenPrivilege SeAuditPrivilege
Security	Audit Success	12548	2015-04-24 20:49:11		Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-19 Account Name: LOCAL SERVICE Account Domain: NT AUTHORITY Logon ID: 0x3e5 Privileges: SeAssignPrimaryTokenPrivilege SeAuditPrivilege SeImpersonatePrivilege
Security	Audit Success	12548	2015-04-24 20:49:11		Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Logon ID: 0x3e7 Privileges: SeAssignPrimaryTokenPrivilege SeTcbPrivilege SeSecurityPrivilege SeTakeOwnershipPrivilege SeLoadDriverPrivilege SeBackupPrivilege SeRestorePrivilege SeDebugPrivilege SeAuditPrivilege SeSystemEnvironmentPrivilege SeImpersonatePrivilege
Security	Audit Success	12548	2015-04-24 20:49:11		Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Logon ID: 0x3e7 Privileges: SeAssignPrimaryTokenPrivilege SeTcbPrivilege SeSecurityPrivilege SeTakeOwnershipPrivilege SeLoadDriverPrivilege SeBackupPrivilege SeRestorePrivilege SeDebugPrivilege SeAuditPrivilege SeSystemEnvironmentPrivilege SeImpersonatePrivilege
Security	Audit Success	12548	2015-04-24 20:49:11		Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Logon ID: 0x3e7 Privileges: SeAssignPrimaryTokenPrivilege SeTcbPrivilege SeSecurityPrivilege SeTakeOwnershipPrivilege SeLoadDriverPrivilege SeBackupPrivilege SeRestorePrivilege SeDebugPrivilege SeAuditPrivilege SeSystemEnvironmentPrivilege SeImpersonatePrivilege
Security	Audit Success	12548	2015-04-24 20:49:11		Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Logon ID: 0x3e7 Privileges: SeAssignPrimaryTokenPrivilege SeTcbPrivilege SeSecurityPrivilege SeTakeOwnershipPrivilege SeLoadDriverPrivilege SeBackupPrivilege SeRestorePrivilege SeDebugPrivilege SeAuditPrivilege SeSystemEnvironmentPrivilege SeImpersonatePrivilege
Security	Audit Success	13568	2015-04-24 20:49:11		Microsoft-Windows-Security-Auditing	4902: The Per-user audit policy table was created. Number of Elements: 0 Policy ID: 0x7b32
Security	Audit Success	12292	2015-04-24 20:49:12		Microsoft-Windows-Security-Auditing	5024: The Windows Firewall service started successfully.
Security	Audit Success	12544	2015-04-24 20:49:12		Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: LTRANPHD$ Account Domain: WORKGROUP Logon ID: 0x3e7 Logon Type: 5 Impersonation Level: %%1833 New Logon: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Logon ID: 0x3e7 Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x234 Process Name: C:\Windows\System32\services.exe Network Information: Workstation Name: Source Network Address: - Source Port: - Detailed Authentication Information: Logon Process: Advapi Authentication Package: Negotiate Transited Services: - Package Name (NTLM only): - Key Length: 0 This event is generated when a logon session is created. It is generated on the computer that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service such as the Server service, or a local process such as Winlogon.exe or Services.exe. The logon type field indicates the kind of logon that occurred. The most common types are 2 (interactive) and 3 (network). The New Logon fields indicate the account for whom the new logon was created, i.e. the account that was logged on. The network fields indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impersonation level field indicates the extent to which a process in the logon session can impersonate. The authentication information fields provide detailed information about this specific logon request. - Logon GUID is a unique identifier that can be used to correlate this event with a KDC event. - Transited services indicate which intermediate services have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indicates the length of the generated session key. This will be 0 if no session key was requested.

Security	Audit Success	12544	2015-04-24 20:49:12	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-0-0 Account Name: - Account Domain: - Logon ID: 0x0 Logon Type: 3 Impersonation Level: %%1833 New Logon: Security ID: S-1-5-7 Account Name: ANONYMOUS LOGON Account Domain: NT AUTHORITY Logon ID: 0x18846 Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x0 Process Name: - Network Information: Workstation Name: Source Network Address: - Source Port: - Detailed Authentication Information: Logon Process: NtLmSsp Authentication Package: NTLM Transited Services: - Package Name (NTLM only): NTLM V1 Key Length: 0 This event is generated when a logon session is created. It is generated on the computer that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service such as the Server service, or a local process such as Winlogon.exe or Services.exe. The logon type field indicates the kind of logon that occurred. The most common types are 2 (interactive) and 3 (network). The New Logon fields indicate the account for whom the new logon was created, i.e. the account that was logged on. The network fields indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impersonation level field indicates the extent to which a process in the logon session can impersonate. The authentication information fields provide detailed information about this specific logon request. - Logon GUID is a unique identifier that can be used to correlate this event with a KDC event. - Transited services indicate which intermediate services have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indicates the length of the generated session key. This will be 0 if no session key was requested.
Security	Audit Success	12548	2015-04-24 20:49:12	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Logon ID: 0x3e7 Privileges: SeAssignPrimaryTokenPrivilege SeTcbPrivilege SeSecurityPrivilege SeTakeOwnershipPrivilege SeLoadDriverPrivilege SeBackupPrivilege SeRestorePrivilege SeDebugPrivilege SeAuditPrivilege SeSystemEnvironmentPrivilege SeImpersonatePrivilege
Security	Audit Success	12544	2015-04-24 20:49:13	Microsoft-Windows-Security-Auditing	4648: A logon was attempted using explicit credentials. Subject: Security ID: S-1-5-18 Account Name: LTRANPHD$ Account Domain: WORKGROUP Logon ID: 0x3e7 Logon GUID: {00000000-0000-0000-0000-000000000000} Account Whose Credentials Were Used: Account Name: Liem Account Domain: LTRANPHD Logon GUID: {00000000-0000-0000-0000-000000000000} Target Server: Target Server Name: localhost Additional Information: localhost Process Information: Process ID: 0x204 Process Name: C:\Windows\System32\winlogon.exe Network Information: Network Address: 127.0.0.1 Port: 0 This event is generated when a process attempts to log on an account by explicitly specifying that account's credentials. This most commonly occurs in batch-type configurations such as scheduled tasks, or when using the RUNAS command.
Security	Audit Success	12544	2015-04-24 20:49:13	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: LTRANPHD$ Account Domain: WORKGROUP Logon ID: 0x3e7 Logon Type: 2 Impersonation Level: %%1833 New Logon: Security ID: S-1-5-21-1888849264-3803429180-4108621888-1001 Account Name: Liem Account Domain: LTRANPHD Logon ID: 0x1bcc3 Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x204 Process Name: C:\Windows\System32\winlogon.exe Network Information: Workstation Name: LTRANPHD Source Network Address: 127.0.0.1 Source Port: 0 Detailed Authentication Information: Logon Process: User32 Authentication Package: Negotiate Transited Services: - Package Name (NTLM only): - Key Length: 0 This event is generated when a logon session is created. It is generated on the computer that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service such as the Server service, or a local process such as Winlogon.exe or Services.exe. The logon type field indicates the kind of logon that occurred. The most common types are 2 (interactive) and 3 (network). The New Logon fields indicate the account for whom the new logon was created, i.e. the account that was logged on. The network fields indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impersonation level field indicates the extent to which a process in the logon session can impersonate. The authentication information fields provide detailed information about this specific logon request. - Logon GUID is a unique identifier that can be used to correlate this event with a KDC event. - Transited services indicate which intermediate services have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indicates the length of the generated session key. This will be 0 if no session key was requested.
Security	Audit Success	12544	2015-04-24 20:49:13	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: LTRANPHD$ Account Domain: WORKGROUP Logon ID: 0x3e7 Logon Type: 2 Impersonation Level: %%1833 New Logon: Security ID: S-1-5-21-1888849264-3803429180-4108621888-1001 Account Name: Liem Account Domain: LTRANPHD Logon ID: 0x1bcf6 Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x204 Process Name: C:\Windows\System32\winlogon.exe Network Information: Workstation Name: LTRANPHD Source Network Address: 127.0.0.1 Source Port: 0 Detailed Authentication Information: Logon Process: User32 Authentication Package: Negotiate Transited Services: - Package Name (NTLM only): - Key Length: 0 This event is generated when a logon session is created. It is generated on the computer that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service such as the Server service, or a local process such as Winlogon.exe or Services.exe. The logon type field indicates the kind of logon that occurred. The most common types are 2 (interactive) and 3 (network). The New Logon fields indicate the account for whom the new logon was created, i.e. the account that was logged on. The network fields indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impersonation level field indicates the extent to which a process in the logon session can impersonate. The authentication information fields provide detailed information about this specific logon request. - Logon GUID is a unique identifier that can be used to correlate this event with a KDC event. - Transited services indicate which intermediate services have participated in this

					logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indicates the length of the generated session key. This will be 0 if no session key was requested.
	Security	Audit Success	12548	2015-04-24 20:49:13	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-21-1888849264-3803429180-4108621888-1001 Account Name: Liem Account Domain: LTRANPHD Logon ID: 0x1bcc3 Privileges: SeSecurityPrivilege SeTakeOwnershipPrivilege SeLoadDriverPrivilege SeBackupPrivilege SeRestorePrivilege SeDebugPrivilege SeSystemEnvironmentPrivilege SeImpersonatePrivilege
	Security	Audit Success	12544	2015-04-24 20:49:14	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: LTRANPHD$ Account Domain: WORKGROUP Logon ID: 0x3e7 Logon Type: 5 Impersonation Level: %%1833 New Logon: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Logon ID: 0x3e7 Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x234 Process Name: C:\Windows\System32\services.exe Network Information: Workstation Name: Source Network Address: - Source Port: - Detailed Authentication Information: Logon Process: Advapi Authentication Package: Negotiate Transited Services: - Package Name (NTLM only): - Key Length: 0 This event is generated when a logon session is created. It is generated on the computer that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service such as the Server service, or a local process such as Winlogon.exe or Services.exe. The logon type field indicates the kind of logon that occurred. The most common types are 2 (interactive) and 3 (network). The New Logon fields indicate the account for whom the new logon was created, i.e. the account that was logged on. The network fields indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impersonation level field indicates the extent to which a process in the logon session can impersonate. The authentication information fields provide detailed information about this specific logon request. - Logon GUID is a unique identifier that can be used to correlate this event with a KDC event. - Transited services indicate which intermediate services have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indicates the length of the generated session key. This will be 0 if no session key was requested.
	Security	Audit Success	12548	2015-04-24 20:49:14	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Logon ID: 0x3e7 Privileges: SeAssignPrimaryTokenPrivilege SeTcbPrivilege SeSecurityPrivilege SeTakeOwnershipPrivilege SeLoadDriverPrivilege SeBackupPrivilege SeRestorePrivilege SeDebugPrivilege SeAuditPrivilege SeSystemEnvironmentPrivilege SeImpersonatePrivilege
	Security	Audit Success	13824	2015-04-24 20:49:16	Microsoft-Windows-Security-Auditing	4797: An attempt was made to query the existence of a blank password for an account. Subject: Security ID: S-1-5-21-1888849264-3803429180-4108621888-1001 Account Name: Liem Account Domain: LTRANPHD Logon ID: 0x1bcf6 Additional Information: Caller Workstation: LTRANPHD Target Account Name: Administrator Target Account Domain: LTRANPHD
	Security	Audit Success	13824	2015-04-24 20:49:16	Microsoft-Windows-Security-Auditing	4797: An attempt was made to query the existence of a blank password for an account. Subject: Security ID: S-1-5-21-1888849264-3803429180-4108621888-1001 Account Name: Liem Account Domain: LTRANPHD Logon ID: 0x1bcf6 Additional Information: Caller Workstation: LTRANPHD Target Account Name: Guest Target Account Domain: LTRANPHD
	Security	Audit Success	13824	2015-04-24 20:49:16	Microsoft-Windows-Security-Auditing	4797: An attempt was made to query the existence of a blank password for an account. Subject: Security ID: S-1-5-21-1888849264-3803429180-4108621888-1001 Account Name: Liem Account Domain: LTRANPHD Logon ID: 0x1bcf6 Additional Information: Caller Workstation: LTRANPHD Target Account Name: Administrator Target Account Domain: LTRANPHD
	Security	Audit Success	13824	2015-04-24 20:49:16	Microsoft-Windows-Security-Auditing	4797: An attempt was made to query the existence of a blank password for an account. Subject: Security ID: S-1-5-21-1888849264-3803429180-4108621888-1001 Account Name: Liem Account Domain: LTRANPHD Logon ID: 0x1bcf6 Additional Information: Caller Workstation: LTRANPHD Target Account Name: Guest Target Account Domain: LTRANPHD
	Security	Audit Success	13824	2015-04-24 20:49:20	Microsoft-Windows-Security-Auditing	4797: An attempt was made to query the existence of a blank password for an account. Subject: Security ID: S-1-5-19 Account Name: LOCAL SERVICE Account Domain: NT AUTHORITY Logon ID: 0x3e5 Additional Information: Caller Workstation: LTRANPHD Target Account Name: Administrator Target Account Domain: LTRANPHD
	Security	Audit Success	13824	2015-04-24 20:49:20	Microsoft-Windows-Security-Auditing	4797: An attempt was made to query the existence of a blank password for an account. Subject: Security ID: S-1-5-19 Account Name: LOCAL SERVICE Account Domain: NT AUTHORITY Logon ID: 0x3e5 Additional Information: Caller Workstation: LTRANPHD Target Account Name: Administrator Target Account Domain: LTRANPHD
	Security	Audit Success	13824	2015-04-24 20:49:20	Microsoft-Windows-Security-Auditing	4797: An attempt was made to query the existence of a blank password for an account. Subject: Security ID: S-1-5-19 Account Name: LOCAL SERVICE Account Domain: NT AUTHORITY Logon ID: 0x3e5 Additional Information: Caller Workstation: LTRANPHD Target Account Name: Guest Target Account Domain: LTRANPHD
	Security	Audit Success	13824	2015-04-24 20:49:20	Microsoft-Windows-Security-Auditing	4797: An attempt was made to query the existence of a blank password for an account. Subject: Security ID: S-1-5-19 Account Name: LOCAL SERVICE Account Domain: NT AUTHORITY Logon ID: 0x3e5 Additional Information: Caller Workstation: LTRANPHD Target Account Name: Guest Target Account Domain: LTRANPHD
	Security	Audit Success	13824	2015-04-24 20:49:20	Microsoft-Windows-Security-Auditing	4797: An attempt was made to query the existence of a blank password for an account. Subject: Security ID: S-1-5-19 Account Name: LOCAL SERVICE Account Domain: NT AUTHORITY Logon ID: 0x3e5 Additional Information: Caller Workstation: LTRANPHD Target Account Name: Liem Target Account Domain: LTRANPHD
	Security	Audit Success	13824	2015-04-24	Microsoft-Windows-Security-Auditing	4797: An attempt was made to query the existence of a blank password for an account. Subject: Security ID: S-1-5-19 Account Name: LOCAL SERVICE Account Domain: NT AUTHORITY Logon ID: 0x3e5 Additional

			20:49:20		Information: Caller Workstation: LTRANPHD Target Account Name: Liem Target Account Domain: LTRANPHD
Security	Audit Success	13824	2015-04-24 20:49:20	Microsoft-Windows-Security-Auditing	4797: An attempt was made to query the existence of a blank password for an account. Subject: Security ID: S-1-5-19 Account Name: LOCAL SERVICE Account Domain: NT AUTHORITY Logon ID: 0x3e5 Additional Information: Caller Workstation: LTRANPHD Target Account Name: Liem Target Account Domain: LTRANPHD
Security	Audit Success	13824	2015-04-24 20:49:20	Microsoft-Windows-Security-Auditing	4797: An attempt was made to query the existence of a blank password for an account. Subject: Security ID: S-1-5-19 Account Name: LOCAL SERVICE Account Domain: NT AUTHORITY Logon ID: 0x3e5 Additional Information: Caller Workstation: LTRANPHD Target Account Name: Liem Target Account Domain: LTRANPHD
Security	Audit Success	12544	2015-04-24 20:58:16	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: LTRANPHD$ Account Domain: WORKGROUP Logon ID: 0x3e7 Logon Type: 5 Impersonation Level: %%1833 New Logon: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Logon ID: 0x3e7 Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x234 Process Name: C:\Windows\System32\services.exe Network Information: Workstation Name: Source Network Address: - Source Port: - Detailed Authentication Information: Logon Process: Advapi Authentication Package: Negotiate Transited Services: - Package Name (NTLM only): - Key Length: 0 This event is generated when a logon session is created. It is generated on the computer that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service such as the Server service, or a local process such as Winlogon.exe or Services.exe. The logon type field indicates the kind of logon that occurred. The most common types are 2 (interactive) and 3 (network). The New Logon fields indicate the account for whom the new logon was created, i.e. the account that was logged on. The network fields indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impersonation level field indicates the extent to which a process in the logon session can impersonate. The authentication information fields provide detailed information about this specific logon request. - Logon GUID is a unique identifier that can be used to correlate this event with a KDC event. - Transited services indicate which intermediate services have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indicates the length of the generated session key. This will be 0 if no session key was requested.
Security	Audit Success	12548	2015-04-24 20:58:16	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Logon ID: 0x3e7 Privileges: SeAssignPrimaryTokenPrivilege SeTcbPrivilege SeSecurityPrivilege SeTakeOwnershipPrivilege SeLoadDriverPrivilege SeBackupPrivilege SeRestorePrivilege SeDebugPrivilege SeAuditPrivilege SeSystemEnvironmentPrivilege SeImpersonatePrivilege
Security	Audit Success	12544	2015-04-24 20:58:17	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: LTRANPHD$ Account Domain: WORKGROUP Logon ID: 0x3e7 Logon Type: 5 Impersonation Level: %%1833 New Logon: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Logon ID: 0x3e7 Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x234 Process Name: C:\Windows\System32\services.exe Network Information: Workstation Name: Source Network Address: - Source Port: - Detailed Authentication Information: Logon Process: Advapi Authentication Package: Negotiate Transited Services: - Package Name (NTLM only): - Key Length: 0 This event is generated when a logon session is created. It is generated on the computer that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service such as the Server service, or a local process such as Winlogon.exe or Services.exe. The logon type field indicates the kind of logon that occurred. The most common types are 2 (interactive) and 3 (network). The New Logon fields indicate the account for whom the new logon was created, i.e. the account that was logged on. The network fields indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impersonation level field indicates the extent to which a process in the logon session can impersonate. The authentication information fields provide detailed information about this specific logon request. - Logon GUID is a unique identifier that can be used to correlate this event with a KDC event. - Transited services indicate which intermediate services have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indicates the length of the generated session key. This will be 0 if no session key was requested.
Security	Audit Success	12548	2015-04-24 20:58:17	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Logon ID: 0x3e7 Privileges: SeAssignPrimaryTokenPrivilege SeTcbPrivilege SeSecurityPrivilege SeTakeOwnershipPrivilege SeLoadDriverPrivilege SeBackupPrivilege SeRestorePrivilege SeDebugPrivilege SeAuditPrivilege SeSystemEnvironmentPrivilege SeImpersonatePrivilege
Security	Audit Success	12545	2015-04-24 21:04:18	Microsoft-Windows-Security-Auditing	4647: User initiated logoff: Subject: Security ID: S-1-5-21-1888849264-3803429180-4108621888-1001 Account Name: Liem Account Domain: LTRANPHD Logon ID: 0x1bcf6 This event is generated when a logoff is initiated. No further user-initiated activity can occur. This event can be interpreted as a logoff event.
Security	Audit Success	103	2015-04-24 21:04:19	Microsoft-Windows-Eventlog	1100: The event logging service has shut down.
Security	Audit Success	12288	2015-04-24 21:04:46	Microsoft-Windows-Security-Auditing	4608: Windows is starting up. This event is logged when LSASS.EXE starts and the auditing subsystem is initialized.
					4624: An account was successfully logged on. Subject: Security ID: S-1-0-0 Account Name: - Account Domain: - Logon ID: 0x0 Logon Type: 0 Impersonation Level: - New Logon: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Logon ID: 0x3e7 Logon GUID: {00000000-0000-0000-0000-

Security	Audit Success	12544	2015-04-24 21:04:46	Microsoft-Windows-Security-Auditing	000000000000} Process Information: Process ID: 0x4 Process Name: Network Information: Workstation Name: - Source Network Address: - Source Port: - Detailed Authentication Information: Logon Process: - Authentication Package: - Transited Services: - Package Name (NTLM only): - Key Length: 0 This event is generated when a logon session is created. It is generated on the computer that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service such as the Server service, or a local process such as Winlogon.exe or Services.exe. The logon type field indicates the kind of logon that occurred. The most common types are 2 (interactive) and 3 (network). The New Logon fields indicate the account for whom the new logon was created, i.e. the account that was logged on. The network fields indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impersonation level field indicates the extent to which a process in the logon session can impersonate. The authentication information fields provide detailed information about this specific logon request. - Logon GUID is a unique identifier that can be used to correlate this event with a KDC event. - Transited services indicate which intermediate services have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indicates the length of the generated session key. This will be 0 if no session key was requested.
Security	Audit Success	12544	2015-04-24 21:04:46	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: LTRANPHD$ Account Domain: WORKGROUP Logon ID: 0x3e7 Logon Type: 5 Impersonation Level: %%1833 New Logon: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Logon ID: 0x3e7 Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x230 Process Name: C:\Windows\System32\services.exe Network Information: Workstation Name: Source Network Address: - Source Port: - Detailed Authentication Information: Logon Process: Advapi Authentication Package: Negotiate Transited Services: - Package Name (NTLM only): - Key Length: 0 This event is generated when a logon session is created. It is generated on the computer that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service such as the Server service, or a local process such as Winlogon.exe or Services.exe. The logon type field indicates the kind of logon that occurred. The most common types are 2 (interactive) and 3 (network). The New Logon fields indicate the account for whom the new logon was created, i.e. the account that was logged on. The network fields indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impersonation level field indicates the extent to which a process in the logon session can impersonate. The authentication information fields provide detailed information about this specific logon request. - Logon GUID is a unique identifier that can be used to correlate this event with a KDC event. - Transited services indicate which intermediate services have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indicates the length of the generated session key. This will be 0 if no session key was requested.
Security	Audit Success	12544	2015-04-24 21:04:46	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: LTRANPHD$ Account Domain: WORKGROUP Logon ID: 0x3e7 Logon Type: 5 Impersonation Level: %%1833 New Logon: Security ID: S-1-5-20 Account Name: NETWORK SERVICE Account Domain: NT AUTHORITY Logon ID: 0x3e4 Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x230 Process Name: C:\Windows\System32\services.exe Network Information: Workstation Name: Source Network Address: - Source Port: - Detailed Authentication Information: Logon Process: Advapi Authentication Package: Negotiate Transited Services: - Package Name (NTLM only): - Key Length: 0 This event is generated when a logon session is created. It is generated on the computer that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service such as the Server service, or a local process such as Winlogon.exe or Services.exe. The logon type field indicates the kind of logon that occurred. The most common types are 2 (interactive) and 3 (network). The New Logon fields indicate the account for whom the new logon was created, i.e. the account that was logged on. The network fields indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impersonation level field indicates the extent to which a process in the logon session can impersonate. The authentication information fields provide detailed information about this specific logon request. - Logon GUID is a unique identifier that can be used to correlate this event with a KDC event. - Transited services indicate which intermediate services have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indicates the length of the generated session key. This will be 0 if no session key was requested.
Security	Audit Success	12544	2015-04-24 21:04:46	Microsoft-Windows-Security-Auditing	4648: A logon was attempted using explicit credentials. Subject: Security ID: S-1-5-18 Account Name: LTRANPHD$ Account Domain: WORKGROUP Logon ID: 0x3e7 Logon GUID: {00000000-0000-0000-0000-000000000000} Account Whose Credentials Were Used: Account Name: DWM-1 Account Domain: Window Manager Logon GUID: {00000000-0000-0000-0000-000000000000} Target Server: Target Server Name: localhost Additional Information: localhost Process Information: Process ID: 0x200 Process Name: C:\Windows\System32\winlogon.exe Network Information: Network Address: - Port: - This event is generated when a process attempts to log on an account by explicitly specifying that account's credentials. This most commonly occurs in batch-type configurations such as scheduled tasks, or when using the RUNAS command.
					4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: LTRANPHD$ Account Domain: WORKGROUP Logon ID: 0x3e7 Logon Type: 2 Impersonation Level: %%1833 New Logon: Security ID: S-1-5-90-1 Account Name: DWM-1 Account Domain: Window Manager Logon ID: 0xcb1e Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x200 Process Name: C:\Windows\System32\winlogon.exe Network Information: Workstation Name: Source Network Address: - Source Port: - Detailed Authentication Information: Logon Process: Advapi Authentication Package: Negotiate

Security	Audit Success	12544	2015-04-24 21:04:46	Microsoft-Windows-Security-Auditing	Transited Services: - Package Name (NTLM only): - Key Length: 0 This event is generated when a logon session is created. It is generated on the computer that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service such as the Server service, or a local process such as Winlogon.exe or Services.exe. The logon type field indicates the kind of logon that occurred. The most common types are 2 (interactive) and 3 (network). The New Logon fields indicate the account for whom the new logon was created, i.e. the account that was logged on. The network fields indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impersonation level field indicates the extent to which a process in the logon session can impersonate. The authentication information fields provide detailed information about this specific logon request. - Logon GUID is a unique identifier that can be used to correlate this event with a KDC event. - Transited services indicate which intermediate services have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indicates the length of the generated session key. This will be 0 if no session key was requested.
Security	Audit Success	12544	2015-04-24 21:04:46	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: LTRANPHD$ Account Domain: WORKGROUP Logon ID: 0x3e7 Logon Type: 2 Impersonation Level: %%1833 New Logon: Security ID: S-1-5-90-1 Account Name: DWM-1 Account Domain: Window Manager Logon ID: 0xcb38 Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x200 Process Name: C:\Windows\System32\winlogon.exe Network Information: Workstation Name: Source Network Address: - Source Port: - Detailed Authentication Information: Logon Process: Advapi Authentication Package: Negotiate Transited Services: - Package Name (NTLM only): - Key Length: 0 This event is generated when a logon session is created. It is generated on the computer that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service such as the Server service, or a local process such as Winlogon.exe or Services.exe. The logon type field indicates the kind of logon that occurred. The most common types are 2 (interactive) and 3 (network). The New Logon fields indicate the account for whom the new logon was created, i.e. the account that was logged on. The network fields indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impersonation level field indicates the extent to which a process in the logon session can impersonate. The authentication information fields provide detailed information about this specific logon request. - Logon GUID is a unique identifier that can be used to correlate this event with a KDC event. - Transited services indicate which intermediate services have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indicates the length of the generated session key. This will be 0 if no session key was requested.
Security	Audit Success	12544	2015-04-24 21:04:46	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: LTRANPHD$ Account Domain: WORKGROUP Logon ID: 0x3e7 Logon Type: 5 Impersonation Level: %%1833 New Logon: Security ID: S-1-5-19 Account Name: LOCAL SERVICE Account Domain: NT AUTHORITY Logon ID: 0x3e5 Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x230 Process Name: C:\Windows\System32\services.exe Network Information: Workstation Name: Source Network Address: - Source Port: - Detailed Authentication Information: Logon Process: Advapi Authentication Package: Negotiate Transited Services: - Package Name (NTLM only): - Key Length: 0 This event is generated when a logon session is created. It is generated on the computer that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service such as the Server service, or a local process such as Winlogon.exe or Services.exe. The logon type field indicates the kind of logon that occurred. The most common types are 2 (interactive) and 3 (network). The New Logon fields indicate the account for whom the new logon was created, i.e. the account that was logged on. The network fields indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impersonation level field indicates the extent to which a process in the logon session can impersonate. The authentication information fields provide detailed information about this specific logon request. - Logon GUID is a unique identifier that can be used to correlate this event with a KDC event. - Transited services indicate which intermediate services have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indicates the length of the generated session key. This will be 0 if no session key was requested.
Security	Audit Success	12544	2015-04-24 21:04:46	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: LTRANPHD$ Account Domain: WORKGROUP Logon ID: 0x3e7 Logon Type: 5 Impersonation Level: %%1833 New Logon: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Logon ID: 0x3e7 Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x230 Process Name: C:\Windows\System32\services.exe Network Information: Workstation Name: Source Network Address: - Source Port: - Detailed Authentication Information: Logon Process: Advapi Authentication Package: Negotiate Transited Services: - Package Name (NTLM only): - Key Length: 0 This event is generated when a logon session is created. It is generated on the computer that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service such as the Server service, or a local process such as Winlogon.exe or Services.exe. The logon type field indicates the kind of logon that occurred. The most common types are 2 (interactive) and 3 (network). The New Logon fields indicate the account for whom the new logon was created, i.e. the account that was logged on. The network fields indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impersonation level field indicates the extent to which a process in the logon session can impersonate. The authentication information fields provide detailed information about this specific logon request. - Logon GUID is a unique identifier that can be used to correlate this event with a KDC event. - Transited

					services indicate which intermediate services have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indicates the length of the generated session key. This will be 0 if no session key was requested.
Security	Audit Success	12544	2015-04-24 21:04:46	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: LTRANPHD$ Account Domain: WORKGROUP Logon ID: 0x3e7 Logon Type: 5 Impersonation Level: %%1833 New Logon: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Logon ID: 0x3e7 Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x230 Process Name: C:\Windows\System32\services.exe Network Information: Workstation Name: Source Network Address: - Source Port: - Detailed Authentication Information: Logon Process: Advapi Authentication Package: Negotiate Transited Services: - Package Name (NTLM only): - Key Length: 0 This event is generated when a logon session is created. It is generated on the computer that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service such as the Server service, or a local process such as Winlogon.exe or Services.exe. The logon type field indicates the kind of logon that occurred. The most common types are 2 (interactive) and 3 (network). The New Logon fields indicate the account for whom the new logon was created, i.e. the account that was logged on. The network fields indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impersonation level field indicates the extent to which a process in the logon session can impersonate. The authentication information fields provide detailed information about this specific logon request. - Logon GUID is a unique identifier that can be used to correlate this event with a KDC event. - Transited services indicate which intermediate services have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indicates the length of the generated session key. This will be 0 if no session key was requested.
Security	Audit Success	12548	2015-04-24 21:04:46	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Logon ID: 0x3e7 Privileges: SeAssignPrimaryTokenPrivilege SeTcbPrivilege SeSecurityPrivilege SeTakeOwnershipPrivilege SeLoadDriverPrivilege SeBackupPrivilege SeRestorePrivilege SeDebugPrivilege SeAuditPrivilege SeSystemEnvironmentPrivilege SeImpersonatePrivilege
Security	Audit Success	12548	2015-04-24 21:04:46	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-20 Account Name: NETWORK SERVICE Account Domain: NT AUTHORITY Logon ID: 0x3e4 Privileges: SeAssignPrimaryTokenPrivilege SeAuditPrivilege SeImpersonatePrivilege
Security	Audit Success	12548	2015-04-24 21:04:46	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-90-1 Account Name: DWM-1 Account Domain: Window Manager Logon ID: 0xcb1e Privileges: SeAssignPrimaryTokenPrivilege SeAuditPrivilege SeImpersonatePrivilege
Security	Audit Success	12548	2015-04-24 21:04:46	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-90-1 Account Name: DWM-1 Account Domain: Window Manager Logon ID: 0xcb38 Privileges: SeAssignPrimaryTokenPrivilege SeAuditPrivilege
Security	Audit Success	12548	2015-04-24 21:04:46	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-19 Account Name: LOCAL SERVICE Account Domain: NT AUTHORITY Logon ID: 0x3e5 Privileges: SeAssignPrimaryTokenPrivilege SeAuditPrivilege SeImpersonatePrivilege
Security	Audit Success	12548	2015-04-24 21:04:46	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Logon ID: 0x3e7 Privileges: SeAssignPrimaryTokenPrivilege SeTcbPrivilege SeSecurityPrivilege SeTakeOwnershipPrivilege SeLoadDriverPrivilege SeBackupPrivilege SeRestorePrivilege SeDebugPrivilege SeAuditPrivilege SeSystemEnvironmentPrivilege SeImpersonatePrivilege
Security	Audit Success	12548	2015-04-24 21:04:46	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Logon ID: 0x3e7 Privileges: SeAssignPrimaryTokenPrivilege SeTcbPrivilege SeSecurityPrivilege SeTakeOwnershipPrivilege SeLoadDriverPrivilege SeBackupPrivilege SeRestorePrivilege SeDebugPrivilege SeAuditPrivilege SeSystemEnvironmentPrivilege SeImpersonatePrivilege
Security	Audit Success	13568	2015-04-24 21:04:46	Microsoft-Windows-Security-Auditing	4902: The Per-user audit policy table was created. Number of Elements: 0 Policy ID: 0x7c72
Security	Audit Success	12292	2015-04-24 21:04:47	Microsoft-Windows-Security-Auditing	5033: The Windows Firewall Driver started successfully.
Security	Audit Success	12292	2015-04-24 21:04:47	Microsoft-Windows-Security-Auditing	5024: The Windows Firewall service started successfully.
Security	Audit	12544	2015-04-24	Microsoft-Windows-Security-	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: LTRANPHD$ Account Domain: WORKGROUP Logon ID: 0x3e7 Logon Type: 5 Impersonation Level: %%1833 New Logon: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Logon ID: 0x3e7 Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x230 Process Name: C:\Windows\System32\services.exe Network Information: Workstation Name: Source Network Address: - Source Port: - Detailed Authentication Information: Logon Process: Advapi Authentication Package: Negotiate Transited Services: - Package Name (NTLM only): - Key Length: 0 This event is generated when a logon session is created. It is generated on the computer that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service such as the Server service, or a local process such as Winlogon.exe or Services.exe. The logon type field indicates the kind of logon that occurred.

	Success		21:04:47	Auditing	The most common types are 2 (interactive) and 3 (network). The New Logon fields indicate the account for whom the new logon was created, i.e. the account that was logged on. The network fields indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impersonation level field indicates the extent to which a process in the logon session can impersonate. The authentication information fields provide detailed information about this specific logon request. - Logon GUID is a unique identifier that can be used to correlate this event with a KDC event. - Transited services indicate which intermediate services have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indicates the length of the generated session key. This will be 0 if no session key was requested.
Security	Audit Success	12544	2015-04-24 21:04:47	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: LTRANPHD$ Account Domain: WORKGROUP Logon ID: 0x3e7 Logon Type: 5 Impersonation Level: %%1833 New Logon: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Logon ID: 0x3e7 Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x230 Process Name: C:\Windows\System32\services.exe Network Information: Workstation Name: Source Network Address: - Source Port: - Detailed Authentication Information: Logon Process: Advapi Authentication Package: Negotiate Transited Services: - Package Name (NTLM only): - Key Length: 0 This event is generated when a logon session is created. It is generated on the computer that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service such as the Server service, or a local process such as Winlogon.exe or Services.exe. The logon type field indicates the kind of logon that occurred. The most common types are 2 (interactive) and 3 (network). The New Logon fields indicate the account for whom the new logon was created, i.e. the account that was logged on. The network fields indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impersonation level field indicates the extent to which a process in the logon session can impersonate. The authentication information fields provide detailed information about this specific logon request. - Logon GUID is a unique identifier that can be used to correlate this event with a KDC event. - Transited services indicate which intermediate services have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indicates the length of the generated session key. This will be 0 if no session key was requested.
Security	Audit Success	12544	2015-04-24 21:04:47	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: LTRANPHD$ Account Domain: WORKGROUP Logon ID: 0x3e7 Logon Type: 5 Impersonation Level: %%1833 New Logon: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Logon ID: 0x3e7 Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x230 Process Name: C:\Windows\System32\services.exe Network Information: Workstation Name: Source Network Address: - Source Port: - Detailed Authentication Information: Logon Process: Advapi Authentication Package: Negotiate Transited Services: - Package Name (NTLM only): - Key Length: 0 This event is generated when a logon session is created. It is generated on the computer that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service such as the Server service, or a local process such as Winlogon.exe or Services.exe. The logon type field indicates the kind of logon that occurred. The most common types are 2 (interactive) and 3 (network). The New Logon fields indicate the account for whom the new logon was created, i.e. the account that was logged on. The network fields indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impersonation level field indicates the extent to which a process in the logon session can impersonate. The authentication information fields provide detailed information about this specific logon request. - Logon GUID is a unique identifier that can be used to correlate this event with a KDC event. - Transited services indicate which intermediate services have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indicates the length of the generated session key. This will be 0 if no session key was requested.
Security	Audit Success	12544	2015-04-24 21:04:47	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-0-0 Account Name: - Account Domain: - Logon ID: 0x0 Logon Type: 3 Impersonation Level: %%1833 New Logon: Security ID: S-1-5-7 Account Name: ANONYMOUS LOGON Account Domain: NT AUTHORITY Logon ID: 0x18e17 Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x0 Process Name: - Network Information: Workstation Name: Source Network Address: - Source Port: - Detailed Authentication Information: Logon Process: NtLmSsp Authentication Package: NTLM Transited Services: - Package Name (NTLM only): NTLM V1 Key Length: 0 This event is generated when a logon session is created. It is generated on the computer that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service such as the Server service, or a local process such as Winlogon.exe or Services.exe. The logon type field indicates the kind of logon that occurred. The most common types are 2 (interactive) and 3 (network). The New Logon fields indicate the account for whom the new logon was created, i.e. the account that was logged on. The network fields indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impersonation level field indicates the extent to which a process in the logon session can impersonate. The authentication information fields provide detailed information about this specific logon request. - Logon GUID is a unique identifier that can be used to correlate this event with a KDC event. - Transited services indicate which intermediate services have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indicates the length of the generated session key. This will be 0 if no session key was requested.
			2015-04-		4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account

Security	Audit Success	12548	24 21:04:47	Microsoft-Windows-Security-Auditing	Domain: NT AUTHORITY Logon ID: 0x3e7 Privileges: SeAssignPrimaryTokenPrivilege SeTcbPrivilege SeSecurityPrivilege SeTakeOwnershipPrivilege SeLoadDriverPrivilege SeBackupPrivilege SeRestorePrivilege SeDebugPrivilege SeAuditPrivilege SeSystemEnvironmentPrivilege SeImpersonatePrivilege
Security	Audit Success	12548	2015-04-24 21:04:47	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Logon ID: 0x3e7 Privileges: SeAssignPrimaryTokenPrivilege SeTcbPrivilege SeSecurityPrivilege SeTakeOwnershipPrivilege SeLoadDriverPrivilege SeBackupPrivilege SeRestorePrivilege SeDebugPrivilege SeAuditPrivilege SeSystemEnvironmentPrivilege SeImpersonatePrivilege
Security	Audit Success	12548	2015-04-24 21:04:47	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Logon ID: 0x3e7 Privileges: SeAssignPrimaryTokenPrivilege SeTcbPrivilege SeSecurityPrivilege SeTakeOwnershipPrivilege SeLoadDriverPrivilege SeBackupPrivilege SeRestorePrivilege SeDebugPrivilege SeAuditPrivilege SeSystemEnvironmentPrivilege SeImpersonatePrivilege
Security	Audit Success	12544	2015-04-24 21:04:48	Microsoft-Windows-Security-Auditing	4648: A logon was attempted using explicit credentials. Subject: Security ID: S-1-5-18 Account Name: LTRANPHD$ Account Domain: WORKGROUP Logon ID: 0x3e7 Logon GUID: {00000000-0000-0000-0000-000000000000} Account Whose Credentials Were Used: Account Name: Liem Account Domain: LTRANPHD Logon GUID: {00000000-0000-0000-0000-000000000000} Target Server: Target Server Name: localhost Additional Information: localhost Process Information: Process ID: 0x200 Process Name: C:\Windows\System32\winlogon.exe Network Information: Network Address: 127.0.0.1 Port: 0 This event is generated when a process attempts to log on an account by explicitly specifying that account's credentials. This most commonly occurs in batch-type configurations such as scheduled tasks, or when using the RUNAS command.
Security	Audit Success	12544	2015-04-24 21:04:48	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: LTRANPHD$ Account Domain: WORKGROUP Logon ID: 0x3e7 Logon Type: 2 Impersonation Level: %%1833 New Logon: Security ID: S-1-5-21-1888849264-3803429180-4108621888-1001 Account Name: Liem Account Domain: LTRANPHD Logon ID: 0x1d1d9 Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x200 Process Name: C:\Windows\System32\winlogon.exe Network Information: Workstation Name: LTRANPHD Source Network Address: 127.0.0.1 Source Port: 0 Detailed Authentication Information: Logon Process: User32 Authentication Package: Negotiate Transited Services: - Package Name (NTLM only): - Key Length: 0 This event is generated when a logon session is created. It is generated on the computer that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service such as the Server service, or a local process such as Winlogon.exe or Services.exe. The logon type field indicates the kind of logon that occurred. The most common types are 2 (interactive) and 3 (network). The New Logon fields indicate the account for whom the new logon was created, i.e. the account that was logged on. The network fields indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impersonation level field indicates the extent to which a process in the logon session can impersonate. The authentication information fields provide detailed information about this specific logon request. - Logon GUID is a unique identifier that can be used to correlate this event with a KDC event. - Transited services indicate which intermediate services have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indicates the length of the generated session key. This will be 0 if no session key was requested.
Security	Audit Success	12544	2015-04-24 21:04:48	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: LTRANPHD$ Account Domain: WORKGROUP Logon ID: 0x3e7 Logon Type: 2 Impersonation Level: %%1833 New Logon: Security ID: S-1-5-21-1888849264-3803429180-4108621888-1001 Account Name: Liem Account Domain: LTRANPHD Logon ID: 0x1d208 Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x200 Process Name: C:\Windows\System32\winlogon.exe Network Information: Workstation Name: LTRANPHD Source Network Address: 127.0.0.1 Source Port: 0 Detailed Authentication Information: Logon Process: User32 Authentication Package: Negotiate Transited Services: - Package Name (NTLM only): - Key Length: 0 This event is generated when a logon session is created. It is generated on the computer that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service such as the Server service, or a local process such as Winlogon.exe or Services.exe. The logon type field indicates the kind of logon that occurred. The most common types are 2 (interactive) and 3 (network). The New Logon fields indicate the account for whom the new logon was created, i.e. the account that was logged on. The network fields indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impersonation level field indicates the extent to which a process in the logon session can impersonate. The authentication information fields provide detailed information about this specific logon request. - Logon GUID is a unique identifier that can be used to correlate this event with a KDC event. - Transited services indicate which intermediate services have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indicates the length of the generated session key. This will be 0 if no session key was requested.
Security	Audit Success	12548	2015-04-24 21:04:48	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-21-1888849264-3803429180-4108621888-1001 Account Name: Liem Account Domain: LTRANPHD Logon ID: 0x1d1d9 Privileges: SeSecurityPrivilege SeTakeOwnershipPrivilege SeLoadDriverPrivilege SeBackupPrivilege SeRestorePrivilege SeDebugPrivilege SeSystemEnvironmentPrivilege SeImpersonatePrivilege
					4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: LTRANPHD$ Account Domain: WORKGROUP Logon ID: 0x3e7 Logon Type: 5 Impersonation Level: %%1833 New Logon: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Logon ID: 0x3e7 Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x230 Process Name:

Security	Audit Success	12544	2015-04-24 21:04:50		Microsoft-Windows-Security-Auditing	C:\Windows\System32\services.exe Network Information: Workstation Name: Source Network Address: - Source Port: - Detailed Authentication Information: Logon Process: Advapi Authentication Package: Negotiate Transited Services: - Package Name (NTLM only): - Key Length: 0 This event is generated when a logon session is created. It is generated on the computer that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service such as the Server service, or a local process such as Winlogon.exe or Services.exe. The logon type field indicates the kind of logon that occurred. The most common types are 2 (interactive) and 3 (network). The New Logon fields indicate the account for whom the new logon was created, i.e. the account that was logged on. The network fields indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impersonation level field indicates the extent to which a process in the logon session can impersonate. The authentication information fields provide detailed information about this specific logon request. - Logon GUID is a unique identifier that can be used to correlate this event with a KDC event. - Transited services indicate which intermediate services have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indicates the length of the generated session key. This will be 0 if no session key was requested.
Security	Audit Success	12548	2015-04-24 21:04:50		Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Logon ID: 0x3e7 Privileges: SeAssignPrimaryTokenPrivilege SeTcbPrivilege SeSecurityPrivilege SeTakeOwnershipPrivilege SeLoadDriverPrivilege SeBackupPrivilege SeRestorePrivilege SeDebugPrivilege SeAuditPrivilege SeSystemEnvironmentPrivilege SeImpersonatePrivilege
Security	Audit Success	13824	2015-04-24 21:04:52		Microsoft-Windows-Security-Auditing	4797: An attempt was made to query the existence of a blank password for an account. Subject: Security ID: S-1-5-21-1888849264-3803429180-4108621888-1001 Account Name: Liem Account Domain: LTRANPHD Logon ID: 0x1d208 Additional Information: Caller Workstation: LTRANPHD Target Account Name: Administrator Target Account Domain: LTRANPHD
Security	Audit Success	13824	2015-04-24 21:04:52		Microsoft-Windows-Security-Auditing	4797: An attempt was made to query the existence of a blank password for an account. Subject: Security ID: S-1-5-21-1888849264-3803429180-4108621888-1001 Account Name: Liem Account Domain: LTRANPHD Logon ID: 0x1d208 Additional Information: Caller Workstation: LTRANPHD Target Account Name: Guest Target Account Domain: LTRANPHD
Security	Audit Success	13824	2015-04-24 21:04:52		Microsoft-Windows-Security-Auditing	4797: An attempt was made to query the existence of a blank password for an account. Subject: Security ID: S-1-5-21-1888849264-3803429180-4108621888-1001 Account Name: Liem Account Domain: LTRANPHD Logon ID: 0x1d208 Additional Information: Caller Workstation: LTRANPHD Target Account Name: Administrator Target Account Domain: LTRANPHD
Security	Audit Success	13824	2015-04-24 21:04:52		Microsoft-Windows-Security-Auditing	4797: An attempt was made to query the existence of a blank password for an account. Subject: Security ID: S-1-5-21-1888849264-3803429180-4108621888-1001 Account Name: Liem Account Domain: LTRANPHD Logon ID: 0x1d208 Additional Information: Caller Workstation: LTRANPHD Target Account Name: Guest Target Account Domain: LTRANPHD
Security	Audit Success	13824	2015-04-24 21:04:54		Microsoft-Windows-Security-Auditing	4797: An attempt was made to query the existence of a blank password for an account. Subject: Security ID: S-1-5-19 Account Name: LOCAL SERVICE Account Domain: NT AUTHORITY Logon ID: 0x3e5 Additional Information: Caller Workstation: LTRANPHD Target Account Name: Administrator Target Account Domain: LTRANPHD
Security	Audit Success	13824	2015-04-24 21:04:54		Microsoft-Windows-Security-Auditing	4797: An attempt was made to query the existence of a blank password for an account. Subject: Security ID: S-1-5-19 Account Name: LOCAL SERVICE Account Domain: NT AUTHORITY Logon ID: 0x3e5 Additional Information: Caller Workstation: LTRANPHD Target Account Name: Administrator Target Account Domain: LTRANPHD
Security	Audit Success	13824	2015-04-24 21:04:54		Microsoft-Windows-Security-Auditing	4797: An attempt was made to query the existence of a blank password for an account. Subject: Security ID: S-1-5-19 Account Name: LOCAL SERVICE Account Domain: NT AUTHORITY Logon ID: 0x3e5 Additional Information: Caller Workstation: LTRANPHD Target Account Name: Guest Target Account Domain: LTRANPHD
Security	Audit Success	13824	2015-04-24 21:04:54		Microsoft-Windows-Security-Auditing	4797: An attempt was made to query the existence of a blank password for an account. Subject: Security ID: S-1-5-19 Account Name: LOCAL SERVICE Account Domain: NT AUTHORITY Logon ID: 0x3e5 Additional Information: Caller Workstation: LTRANPHD Target Account Name: Guest Target Account Domain: LTRANPHD
Security	Audit Success	13824	2015-04-24 21:04:54		Microsoft-Windows-Security-Auditing	4797: An attempt was made to query the existence of a blank password for an account. Subject: Security ID: S-1-5-19 Account Name: LOCAL SERVICE Account Domain: NT AUTHORITY Logon ID: 0x3e5 Additional Information: Caller Workstation: LTRANPHD Target Account Name: Liem Target Account Domain: LTRANPHD
Security	Audit Success	13824	2015-04-24 21:04:54		Microsoft-Windows-Security-Auditing	4797: An attempt was made to query the existence of a blank password for an account. Subject: Security ID: S-1-5-19 Account Name: LOCAL SERVICE Account Domain: NT AUTHORITY Logon ID: 0x3e5 Additional Information: Caller Workstation: LTRANPHD Target Account Name: Liem Target Account Domain: LTRANPHD
Security	Audit Success	13824	2015-04-24 21:04:54		Microsoft-Windows-Security-Auditing	4797: An attempt was made to query the existence of a blank password for an account. Subject: Security ID: S-1-5-19 Account Name: LOCAL SERVICE Account Domain: NT AUTHORITY Logon ID: 0x3e5 Additional Information: Caller Workstation: LTRANPHD Target Account Name: Liem Target Account Domain: LTRANPHD
Security	Audit Success	13824	2015-04-24 21:04:54		Microsoft-Windows-Security-Auditing	4797: An attempt was made to query the existence of a blank password for an account. Subject: Security ID: S-1-5-19 Account Name: LOCAL SERVICE Account Domain: NT AUTHORITY Logon ID: 0x3e5 Additional Information: Caller Workstation: LTRANPHD Target Account Name: Liem Target Account Domain: LTRANPHD
						4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: LTRANPHD$ Account Domain: WORKGROUP Logon ID: 0x3e7 Logon Type: 5 Impersonation Level: %%1833 New Logon: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Logon ID: 0x3e7 Logon GUID:

Security	Audit Success	12544	2015-04-24 21:04:55	Microsoft-Windows-Security-Auditing	{00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x230 Process Name: C:\Windows\System32\services.exe Network Information: Workstation Name: Source Network Address: - Source Port: - Detailed Authentication Information: Logon Process: Advapi Authentication Package: Negotiate Transited Services: - Package Name (NTLM only): - Key Length: 0 This event is generated when a logon session is created. It is generated on the computer that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service such as the Server service, or a local process such as Winlogon.exe or Services.exe. The logon type field indicates the kind of logon that occurred. The most common types are 2 (interactive) and 3 (network). The New Logon fields indicate the account for whom the new logon was created, i.e. the account that was logged on. The network fields indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impersonation level field indicates the extent to which a process in the logon session can impersonate. The authentication information fields provide detailed information about this specific logon request. - Logon GUID is a unique identifier that can be used to correlate this event with a KDC event. - Transited services indicate which intermediate services have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indicates the length of the generated session key. This will be 0 if no session key was requested.
Security	Audit Success	12548	2015-04-24 21:04:55	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Logon ID: 0x3e7 Privileges: SeAssignPrimaryTokenPrivilege SeTcbPrivilege SeSecurityPrivilege SeTakeOwnershipPrivilege SeLoadDriverPrivilege SeBackupPrivilege SeRestorePrivilege SeDebugPrivilege SeAuditPrivilege SeSystemEnvironmentPrivilege SeImpersonatePrivilege
Security	Audit Success	12544	2015-04-24 21:04:56	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: LTRANPHD$ Account Domain: WORKGROUP Logon ID: 0x3e7 Logon Type: 5 Impersonation Level: %%1833 New Logon: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Logon ID: 0x3e7 Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x230 Process Name: C:\Windows\System32\services.exe Network Information: Workstation Name: Source Network Address: - Source Port: - Detailed Authentication Information: Logon Process: Advapi Authentication Package: Negotiate Transited Services: - Package Name (NTLM only): - Key Length: 0 This event is generated when a logon session is created. It is generated on the computer that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service such as the Server service, or a local process such as Winlogon.exe or Services.exe. The logon type field indicates the kind of logon that occurred. The most common types are 2 (interactive) and 3 (network). The New Logon fields indicate the account for whom the new logon was created, i.e. the account that was logged on. The network fields indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impersonation level field indicates the extent to which a process in the logon session can impersonate. The authentication information fields provide detailed information about this specific logon request. - Logon GUID is a unique identifier that can be used to correlate this event with a KDC event. - Transited services indicate which intermediate services have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indicates the length of the generated session key. This will be 0 if no session key was requested.
Security	Audit Success	12548	2015-04-24 21:04:56	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Logon ID: 0x3e7 Privileges: SeAssignPrimaryTokenPrivilege SeTcbPrivilege SeSecurityPrivilege SeTakeOwnershipPrivilege SeLoadDriverPrivilege SeBackupPrivilege SeRestorePrivilege SeDebugPrivilege SeAuditPrivilege SeSystemEnvironmentPrivilege SeImpersonatePrivilege
Security	Audit Success	12545	2015-04-24 21:05:01	Microsoft-Windows-Security-Auditing	4647: User initiated logoff: Subject: Security ID: S-1-5-21-1888849264-3803429180-4108621888-1001 Account Name: Liem Account Domain: LTRANPHD Logon ID: 0x1d208 This event is generated when a logoff is initiated. No further user-initiated activity can occur. This event can be interpreted as a logoff event.
Security	Audit Success	103	2015-04-24 21:05:02	Microsoft-Windows-Eventlog	1100: The event logging service has shut down.
Security	Audit Success	12288	2015-04-24 21:05:12	Microsoft-Windows-Security-Auditing	4608: Windows is starting up. This event is logged when LSASS.EXE starts and the auditing subsystem is initialized.
Security	Audit Success	12544	2015-04-24 21:05:12	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-0-0 Account Name: - Account Domain: - Logon ID: 0x0 Logon Type: 0 Impersonation Level: - New Logon: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Logon ID: 0x3e7 Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x4 Process Name: Network Information: Workstation Name: - Source Network Address: - Source Port: - Detailed Authentication Information: Logon Process: - Authentication Package: - Transited Services: - Package Name (NTLM only): - Key Length: 0 This event is generated when a logon session is created. It is generated on the computer that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service such as the Server service, or a local process such as Winlogon.exe or Services.exe. The logon type field indicates the kind of logon that occurred. The most common types are 2 (interactive) and 3 (network). The New Logon fields indicate the account for whom the new logon was created, i.e. the account that was logged on. The network fields indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impersonation level field indicates the extent to which a process in the logon session can impersonate. The authentication information fields provide detailed information

					about this specific logon request. - Logon GUID is a unique identifier that can be used to correlate this event with a KDC event. - Transited services indicate which intermediate services have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indicates the length of the generated session key. This will be 0 if no session key was requested.
Security	Audit Success	12544	2015-04-24 21:05:12	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: LTRANPHD$ Account Domain: WORKGROUP Logon ID: 0x3e7 Logon Type: 5 Impersonation Level: %%1833 New Logon: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Logon ID: 0x3e7 Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x230 Process Name: C:\Windows\System32\services.exe Network Information: Workstation Name: Source Network Address: - Source Port: - Detailed Authentication Information: Logon Process: Advapi Authentication Package: Negotiate Transited Services: - Package Name (NTLM only): - Key Length: 0 This event is generated when a logon session is created. It is generated on the computer that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service such as the Server service, or a local process such as Winlogon.exe or Services.exe. The logon type field indicates the kind of logon that occurred. The most common types are 2 (interactive) and 3 (network). The New Logon fields indicate the account for whom the new logon was created, i.e. the account that was logged on. The network fields indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impersonation level field indicates the extent to which a process in the logon session can impersonate. The authentication information fields provide detailed information about this specific logon request. - Logon GUID is a unique identifier that can be used to correlate this event with a KDC event. - Transited services indicate which intermediate services have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indicates the length of the generated session key. This will be 0 if no session key was requested.
Security	Audit Success	12544	2015-04-24 21:05:12	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: LTRANPHD$ Account Domain: WORKGROUP Logon ID: 0x3e7 Logon Type: 5 Impersonation Level: %%1833 New Logon: Security ID: S-1-5-20 Account Name: NETWORK SERVICE Account Domain: NT AUTHORITY Logon ID: 0x3e4 Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x230 Process Name: C:\Windows\System32\services.exe Network Information: Workstation Name: Source Network Address: - Source Port: - Detailed Authentication Information: Logon Process: Advapi Authentication Package: Negotiate Transited Services: - Package Name (NTLM only): - Key Length: 0 This event is generated when a logon session is created. It is generated on the computer that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service such as the Server service, or a local process such as Winlogon.exe or Services.exe. The logon type field indicates the kind of logon that occurred. The most common types are 2 (interactive) and 3 (network). The New Logon fields indicate the account for whom the new logon was created, i.e. the account that was logged on. The network fields indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impersonation level field indicates the extent to which a process in the logon session can impersonate. The authentication information fields provide detailed information about this specific logon request. - Logon GUID is a unique identifier that can be used to correlate this event with a KDC event. - Transited services indicate which intermediate services have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indicates the length of the generated session key. This will be 0 if no session key was requested.
Security	Audit Success	12544	2015-04-24 21:05:12	Microsoft-Windows-Security-Auditing	4648: A logon was attempted using explicit credentials. Subject: Security ID: S-1-5-18 Account Name: LTRANPHD$ Account Domain: WORKGROUP Logon ID: 0x3e7 Logon GUID: {00000000-0000-0000-0000-000000000000} Account Whose Credentials Were Used: Account Name: DWM-1 Account Domain: Window Manager Logon GUID: {00000000-0000-0000-0000-000000000000} Target Server: Target Server Name: localhost Additional Information: localhost Process Information: Process ID: 0x200 Process Name: C:\Windows\System32\winlogon.exe Network Information: Network Address: - Port: - This event is generated when a process attempts to log on an account by explicitly specifying that account's credentials. This most commonly occurs in batch-type configurations such as scheduled tasks, or when using the RUNAS command.
Security	Audit Success	12544	2015-04-24 21:05:12	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: LTRANPHD$ Account Domain: WORKGROUP Logon ID: 0x3e7 Logon Type: 2 Impersonation Level: %%1833 New Logon: Security ID: S-1-5-90-1 Account Name: DWM-1 Account Domain: Window Manager Logon ID: 0xca4c Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x200 Process Name: C:\Windows\System32\winlogon.exe Network Information: Workstation Name: Source Network Address: - Source Port: - Detailed Authentication Information: Logon Process: Advapi Authentication Package: Negotiate Transited Services: - Package Name (NTLM only): - Key Length: 0 This event is generated when a logon session is created. It is generated on the computer that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service such as the Server service, or a local process such as Winlogon.exe or Services.exe. The logon type field indicates the kind of logon that occurred. The most common types are 2 (interactive) and 3 (network). The New Logon fields indicate the account for whom the new logon was created, i.e. the account that was logged on. The network fields indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impersonation level field indicates the extent to which a process in the logon session can impersonate. The authentication information fields provide detailed information about this specific logon request. - Logon GUID is a unique identifier that can be used to correlate this event with a KDC event. - Transited services indicate which intermediate services have participated in this logon request. - Package name indicates

					which sub-protocol was used among the NTLM protocols. - Key length indicates the length of the generated session key. This will be 0 if no session key was requested.
Security	Audit Success	12544	2015-04-24 21:05:12	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: LTRANPHD$ Account Domain: WORKGROUP Logon ID: 0x3e7 Logon Type: 2 Impersonation Level: %%1833 New Logon: Security ID: S-1-5-90-1 Account Name: DWM-1 Account Domain: Window Manager Logon ID: 0xca5e Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x200 Process Name: C:\Windows\System32\winlogon.exe Network Information: Workstation Name: Source Network Address: - Source Port: - Detailed Authentication Information: Logon Process: Advapi Authentication Package: Negotiate Transited Services: - Package Name (NTLM only): - Key Length: 0 This event is generated when a logon session is created. It is generated on the computer that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service such as the Server service, or a local process such as Winlogon.exe or Services.exe. The logon type field indicates the kind of logon that occurred. The most common types are 2 (interactive) and 3 (network). The New Logon fields indicate the account for whom the new logon was created, i.e. the account that was logged on. The network fields indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impersonation level field indicates the extent to which a process in the logon session can impersonate. The authentication information fields provide detailed information about this specific logon request. - Logon GUID is a unique identifier that can be used to correlate this event with a KDC event. - Transited services indicate which intermediate services have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indicates the length of the generated session key. This will be 0 if no session key was requested.
Security	Audit Success	12544	2015-04-24 21:05:12	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: LTRANPHD$ Account Domain: WORKGROUP Logon ID: 0x3e7 Logon Type: 5 Impersonation Level: %%1833 New Logon: Security ID: S-1-5-19 Account Name: LOCAL SERVICE Account Domain: NT AUTHORITY Logon ID: 0x3e5 Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x230 Process Name: C:\Windows\System32\services.exe Network Information: Workstation Name: Source Network Address: - Source Port: - Detailed Authentication Information: Logon Process: Advapi Authentication Package: Negotiate Transited Services: - Package Name (NTLM only): - Key Length: 0 This event is generated when a logon session is created. It is generated on the computer that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service such as the Server service, or a local process such as Winlogon.exe or Services.exe. The logon type field indicates the kind of logon that occurred. The most common types are 2 (interactive) and 3 (network). The New Logon fields indicate the account for whom the new logon was created, i.e. the account that was logged on. The network fields indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impersonation level field indicates the extent to which a process in the logon session can impersonate. The authentication information fields provide detailed information about this specific logon request. - Logon GUID is a unique identifier that can be used to correlate this event with a KDC event. - Transited services indicate which intermediate services have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indicates the length of the generated session key. This will be 0 if no session key was requested.
Security	Audit Success	12544	2015-04-24 21:05:12	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: LTRANPHD$ Account Domain: WORKGROUP Logon ID: 0x3e7 Logon Type: 5 Impersonation Level: %%1833 New Logon: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Logon ID: 0x3e7 Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x230 Process Name: C:\Windows\System32\services.exe Network Information: Workstation Name: Source Network Address: - Source Port: - Detailed Authentication Information: Logon Process: Advapi Authentication Package: Negotiate Transited Services: - Package Name (NTLM only): - Key Length: 0 This event is generated when a logon session is created. It is generated on the computer that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service such as the Server service, or a local process such as Winlogon.exe or Services.exe. The logon type field indicates the kind of logon that occurred. The most common types are 2 (interactive) and 3 (network). The New Logon fields indicate the account for whom the new logon was created, i.e. the account that was logged on. The network fields indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impersonation level field indicates the extent to which a process in the logon session can impersonate. The authentication information fields provide detailed information about this specific logon request. - Logon GUID is a unique identifier that can be used to correlate this event with a KDC event. - Transited services indicate which intermediate services have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indicates the length of the generated session key. This will be 0 if no session key was requested.
Security	Audit Success	12548	2015-04-24 21:05:12	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Logon ID: 0x3e7 Privileges: SeAssignPrimaryTokenPrivilege SeTcbPrivilege SeSecurityPrivilege SeTakeOwnershipPrivilege SeLoadDriverPrivilege SeBackupPrivilege SeRestorePrivilege SeDebugPrivilege SeAuditPrivilege SeSystemEnvironmentPrivilege SeImpersonatePrivilege
Security	Audit Success	12548	2015-04-24 21:05:12	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-20 Account Name: NETWORK SERVICE Account Domain: NT AUTHORITY Logon ID: 0x3e4 Privileges: SeAssignPrimaryTokenPrivilege SeAuditPrivilege SeImpersonatePrivilege

Security	Audit Success	12548	2015-04-24 21:05:12	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-90-1 Account Name: DWM-1 Account Domain: Window Manager Logon ID: 0xca4c Privileges: SeAssignPrimaryTokenPrivilege SeAuditPrivilege SeImpersonatePrivilege
Security	Audit Success	12548	2015-04-24 21:05:12	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-90-1 Account Name: DWM-1 Account Domain: Window Manager Logon ID: 0xca5e Privileges: SeAssignPrimaryTokenPrivilege SeAuditPrivilege
Security	Audit Success	12548	2015-04-24 21:05:12	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-19 Account Name: LOCAL SERVICE Account Domain: NT AUTHORITY Logon ID: 0x3e5 Privileges: SeAssignPrimaryTokenPrivilege SeAuditPrivilege SeImpersonatePrivilege
Security	Audit Success	12548	2015-04-24 21:05:12	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Logon ID: 0x3e7 Privileges: SeAssignPrimaryTokenPrivilege SeTcbPrivilege SeSecurityPrivilege SeTakeOwnershipPrivilege SeLoadDriverPrivilege SeBackupPrivilege SeRestorePrivilege SeDebugPrivilege SeAuditPrivilege SeSystemEnvironmentPrivilege SeImpersonatePrivilege
Security	Audit Success	13568	2015-04-24 21:05:12	Microsoft-Windows-Security-Auditing	4902: The Per-user audit policy table was created. Number of Elements: 0 Policy ID: 0x7adb
Security	Audit Success	12292	2015-04-24 21:05:13	Microsoft-Windows-Security-Auditing	5033: The Windows Firewall Driver started successfully.
Security	Audit Success	12544	2015-04-24 21:05:13	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: LTRANPHD$ Account Domain: WORKGROUP Logon ID: 0x3e7 Logon Type: 5 Impersonation Level: %%1833 New Logon: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Logon ID: 0x3e7 Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x230 Process Name: C:\Windows\System32\services.exe Network Information: Workstation Name: Source Network Address: - Source Port: - Detailed Authentication Information: Logon Process: Advapi Authentication Package: Negotiate Transited Services: - Package Name (NTLM only): - Key Length: 0 This event is generated when a logon session is created. It is generated on the computer that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service such as the Server service, or a local process such as Winlogon.exe or Services.exe. The logon type field indicates the kind of logon that occurred. The most common types are 2 (interactive) and 3 (network). The New Logon fields indicate the account for whom the new logon was created, i.e. the account that was logged on. The network fields indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impersonation level field indicates the extent to which a process in the logon session can impersonate. The authentication information fields provide detailed information about this specific logon request. - Logon GUID is a unique identifier that can be used to correlate this event with a KDC event. - Transited services indicate which intermediate services have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indicates the length of the generated session key. This will be 0 if no session key was requested.
Security	Audit Success	12544	2015-04-24 21:05:13	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: LTRANPHD$ Account Domain: WORKGROUP Logon ID: 0x3e7 Logon Type: 5 Impersonation Level: %%1833 New Logon: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Logon ID: 0x3e7 Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x230 Process Name: C:\Windows\System32\services.exe Network Information: Workstation Name: Source Network Address: - Source Port: - Detailed Authentication Information: Logon Process: Advapi Authentication Package: Negotiate Transited Services: - Package Name (NTLM only): - Key Length: 0 This event is generated when a logon session is created. It is generated on the computer that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service such as the Server service, or a local process such as Winlogon.exe or Services.exe. The logon type field indicates the kind of logon that occurred. The most common types are 2 (interactive) and 3 (network). The New Logon fields indicate the account for whom the new logon was created, i.e. the account that was logged on. The network fields indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impersonation level field indicates the extent to which a process in the logon session can impersonate. The authentication information fields provide detailed information about this specific logon request. - Logon GUID is a unique identifier that can be used to correlate this event with a KDC event. - Transited services indicate which intermediate services have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indicates the length of the generated session key. This will be 0 if no session key was requested.
			2015-04-		4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: LTRANPHD$ Account Domain: WORKGROUP Logon ID: 0x3e7 Logon Type: 5 Impersonation Level: %%1833 New Logon: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Logon ID: 0x3e7 Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x230 Process Name: C:\Windows\System32\services.exe Network Information: Workstation Name: Source Network Address: - Source Port: - Detailed Authentication Information: Logon Process: Advapi Authentication Package: Negotiate Transited Services: - Package Name (NTLM only): - Key Length: 0 This event is generated when a logon session is created. It is generated on the computer that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service such as the Server service, or a local

Security	Audit Success	12544	24 21:05:13	Microsoft-Windows-Security-Auditing	process such as Winlogon.exe or Services.exe. The logon type field indicates the kind of logon that occurred. The most common types are 2 (interactive) and 3 (network). The New Logon fields indicate the account for whom the new logon was created, i.e. the account that was logged on. The network fields indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impersonation level field indicates the extent to which a process in the logon session can impersonate. The authentication information fields provide detailed information about this specific logon request. - Logon GUID is a unique identifier that can be used to correlate this event with a KDC event. - Transited services indicate which intermediate services have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indicates the length of the generated session key. This will be 0 if no session key was requested.
Security	Audit Success	12548	2015-04-24 21:05:13	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Logon ID: 0x3e7 Privileges: SeAssignPrimaryTokenPrivilege SeTcbPrivilege SeSecurityPrivilege SeTakeOwnershipPrivilege SeLoadDriverPrivilege SeBackupPrivilege SeRestorePrivilege SeDebugPrivilege SeAuditPrivilege SeSystemEnvironmentPrivilege SeImpersonatePrivilege
Security	Audit Success	12548	2015-04-24 21:05:13	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Logon ID: 0x3e7 Privileges: SeAssignPrimaryTokenPrivilege SeTcbPrivilege SeSecurityPrivilege SeTakeOwnershipPrivilege SeLoadDriverPrivilege SeBackupPrivilege SeRestorePrivilege SeDebugPrivilege SeAuditPrivilege SeSystemEnvironmentPrivilege SeImpersonatePrivilege
Security	Audit Success	12548	2015-04-24 21:05:13	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Logon ID: 0x3e7 Privileges: SeAssignPrimaryTokenPrivilege SeTcbPrivilege SeSecurityPrivilege SeTakeOwnershipPrivilege SeLoadDriverPrivilege SeBackupPrivilege SeRestorePrivilege SeDebugPrivilege SeAuditPrivilege SeSystemEnvironmentPrivilege SeImpersonatePrivilege
Security	Audit Success	12292	2015-04-24 21:05:14	Microsoft-Windows-Security-Auditing	5024: The Windows Firewall service started successfully.
Security	Audit Success	12544	2015-04-24 21:05:14	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: LTRANPHD$ Account Domain: WORKGROUP Logon ID: 0x3e7 Logon Type: 5 Impersonation Level: %%1833 New Logon: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Logon ID: 0x3e7 Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x230 Process Name: C:\Windows\System32\services.exe Network Information: Workstation Name: Source Network Address: - Source Port: - Detailed Authentication Information: Logon Process: Advapi Authentication Package: Negotiate Transited Services: - Package Name (NTLM only): - Key Length: 0 This event is generated when a logon session is created. It is generated on the computer that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service such as the Server service, or a local process such as Winlogon.exe or Services.exe. The logon type field indicates the kind of logon that occurred. The most common types are 2 (interactive) and 3 (network). The New Logon fields indicate the account for whom the new logon was created, i.e. the account that was logged on. The network fields indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impersonation level field indicates the extent to which a process in the logon session can impersonate. The authentication information fields provide detailed information about this specific logon request. - Logon GUID is a unique identifier that can be used to correlate this event with a KDC event. - Transited services indicate which intermediate services have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indicates the length of the generated session key. This will be 0 if no session key was requested.
Security	Audit Success	12544	2015-04-24 21:05:14	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-0-0 Account Name: - Account Domain: - Logon ID: 0x0 Logon Type: 3 Impersonation Level: %%1833 New Logon: Security ID: S-1-5-7 Account Name: ANONYMOUS LOGON Account Domain: NT AUTHORITY Logon ID: 0x1886f Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x0 Process Name: - Network Information: Workstation Name: Source Network Address: - Source Port: - Detailed Authentication Information: Logon Process: NtLmSsp Authentication Package: NTLM Transited Services: - Package Name (NTLM only): NTLM V1 Key Length: 0 This event is generated when a logon session is created. It is generated on the computer that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service such as the Server service, or a local process such as Winlogon.exe or Services.exe. The logon type field indicates the kind of logon that occurred. The most common types are 2 (interactive) and 3 (network). The New Logon fields indicate the account for whom the new logon was created, i.e. the account that was logged on. The network fields indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impersonation level field indicates the extent to which a process in the logon session can impersonate. The authentication information fields provide detailed information about this specific logon request. - Logon GUID is a unique identifier that can be used to correlate this event with a KDC event. - Transited services indicate which intermediate services have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indicates the length of the generated session key. This will be 0 if no session key was requested.
Security	Audit Success	12548	2015-04-24 21:05:14	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Logon ID: 0x3e7 Privileges: SeAssignPrimaryTokenPrivilege SeTcbPrivilege SeSecurityPrivilege SeTakeOwnershipPrivilege SeLoadDriverPrivilege SeBackupPrivilege SeRestorePrivilege

					SeDebugPrivilege SeAuditPrivilege SeSystemEnvironmentPrivilege SeImpersonatePrivilege
Security	Audit Success	103	2015-04-24 21:05:19	Microsoft-Windows-Eventlog	1100: The event logging service has shut down.
Security	Audit Success	12288	2015-04-24 21:05:32	Microsoft-Windows-Security-Auditing	4608: Windows is starting up. This event is logged when LSASS.EXE starts and the auditing subsystem is initialized.
Security	Audit Success	12544	2015-04-24 21:05:32	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-0-0 Account Name: - Account Domain: - Logon ID: 0x0 Logon Type: 0 Impersonation Level: - New Logon: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Logon ID: 0x3e7 Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x4 Process Name: Network Information: Workstation Name: - Source Network Address: - Source Port: - Detailed Authentication Information: Logon Process: - Authentication Package: - Transited Services: - Package Name (NTLM only): - Key Length: 0 This event is generated when a logon session is created. It is generated on the computer that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service such as the Server service, or a local process such as Winlogon.exe or Services.exe. The logon type field indicates the kind of logon that occurred. The most common types are 2 (interactive) and 3 (network). The New Logon fields indicate the account for whom the new logon was created, i.e. the account that was logged on. The network fields indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impersonation level field indicates the extent to which a process in the logon session can impersonate. The authentication information fields provide detailed information about this specific logon request. - Logon GUID is a unique identifier that can be used to correlate this event with a KDC event. - Transited services indicate which intermediate services have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indicates the length of the generated session key. This will be 0 if no session key was requested.
Security	Audit Success	13568	2015-04-24 21:05:32	Microsoft-Windows-Security-Auditing	4902: The Per-user audit policy table was created. Number of Elements: 0 Policy ID: 0x7896
Security	Audit Success	12292	2015-04-24 21:05:33	Microsoft-Windows-Security-Auditing	5033: The Windows Firewall Driver started successfully.
Security	Audit Success	12292	2015-04-24 21:05:33	Microsoft-Windows-Security-Auditing	5024: The Windows Firewall service started successfully.
Security	Audit Success	12544	2015-04-24 21:05:33	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: LTRANPHD$ Account Domain: WORKGROUP Logon ID: 0x3e7 Logon Type: 5 Impersonation Level: %%1833 New Logon: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Logon ID: 0x3e7 Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x230 Process Name: C:\Windows\System32\services.exe Network Information: Workstation Name: Source Network Address: - Source Port: - Detailed Authentication Information: Logon Process: Advapi Authentication Package: Negotiate Transited Services: - Package Name (NTLM only): - Key Length: 0 This event is generated when a logon session is created. It is generated on the computer that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service such as the Server service, or a local process such as Winlogon.exe or Services.exe. The logon type field indicates the kind of logon that occurred. The most common types are 2 (interactive) and 3 (network). The New Logon fields indicate the account for whom the new logon was created, i.e. the account that was logged on. The network fields indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impersonation level field indicates the extent to which a process in the logon session can impersonate. The authentication information fields provide detailed information about this specific logon request. - Logon GUID is a unique identifier that can be used to correlate this event with a KDC event. - Transited services indicate which intermediate services have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indicates the length of the generated session key. This will be 0 if no session key was requested.
Security	Audit Success	12544	2015-04-24 21:05:33	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: LTRANPHD$ Account Domain: WORKGROUP Logon ID: 0x3e7 Logon Type: 5 Impersonation Level: %%1833 New Logon: Security ID: S-1-5-20 Account Name: NETWORK SERVICE Account Domain: NT AUTHORITY Logon ID: 0x3e4 Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x230 Process Name: C:\Windows\System32\services.exe Network Information: Workstation Name: Source Network Address: - Source Port: - Detailed Authentication Information: Logon Process: Advapi Authentication Package: Negotiate Transited Services: - Package Name (NTLM only): - Key Length: 0 This event is generated when a logon session is created. It is generated on the computer that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service such as the Server service, or a local process such as Winlogon.exe or Services.exe. The logon type field indicates the kind of logon that occurred. The most common types are 2 (interactive) and 3 (network). The New Logon fields indicate the account for whom the new logon was created, i.e. the account that was logged on. The network fields indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some

					cases. The impersonation level field indicates the extent to which a process in the logon session can impersonate. The authentication information fields provide detailed information about this specific logon request. - Logon GUID is a unique identifier that can be used to correlate this event with a KDC event. - Transited services indicate which intermediate services have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indicates the length of the generated session key. This will be 0 if no session key was requested.
Security	Audit Success	12544	2015-04-24 21:05:33	Microsoft-Windows-Security-Auditing	4648: A logon was attempted using explicit credentials. Subject: Security ID: S-1-5-18 Account Name: LTRANPHD$ Account Domain: WORKGROUP Logon ID: 0x3e7 Logon GUID: {00000000-0000-0000-0000-000000000000} Account Whose Credentials Were Used: Account Name: DWM-1 Account Domain: Window Manager Logon GUID: {00000000-0000-0000-0000-000000000000} Target Server: Target Server Name: localhost Additional Information: localhost Process Information: Process ID: 0x200 Process Name: C:\Windows\System32\winlogon.exe Network Information: Network Address: - Port: - This event is generated when a process attempts to log on an account by explicitly specifying that account's credentials. This most commonly occurs in batch-type configurations such as scheduled tasks, or when using the RUNAS command.
Security	Audit Success	12544	2015-04-24 21:05:33	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: LTRANPHD$ Account Domain: WORKGROUP Logon ID: 0x3e7 Logon Type: 2 Impersonation Level: %%1833 New Logon: Security ID: S-1-5-90-1 Account Name: DWM-1 Account Domain: Window Manager Logon ID: 0xc9c8 Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x200 Process Name: C:\Windows\System32\winlogon.exe Network Information: Workstation Name: Source Network Address: - Source Port: - Detailed Authentication Information: Logon Process: Advapi Authentication Package: Negotiate Transited Services: - Package Name (NTLM only): - Key Length: 0 This event is generated when a logon session is created. It is generated on the computer that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service such as the Server service, or a local process such as Winlogon.exe or Services.exe. The logon type field indicates the kind of logon that occurred. The most common types are 2 (interactive) and 3 (network). The New Logon fields indicate the account for whom the new logon was created, i.e. the account that was logged on. The network fields indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impersonation level field indicates the extent to which a process in the logon session can impersonate. The authentication information fields provide detailed information about this specific logon request. - Logon GUID is a unique identifier that can be used to correlate this event with a KDC event. - Transited services indicate which intermediate services have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indicates the length of the generated session key. This will be 0 if no session key was requested.
Security	Audit Success	12544	2015-04-24 21:05:33	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: LTRANPHD$ Account Domain: WORKGROUP Logon ID: 0x3e7 Logon Type: 2 Impersonation Level: %%1833 New Logon: Security ID: S-1-5-90-1 Account Name: DWM-1 Account Domain: Window Manager Logon ID: 0xc9dd Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x200 Process Name: C:\Windows\System32\winlogon.exe Network Information: Workstation Name: Source Network Address: - Source Port: - Detailed Authentication Information: Logon Process: Advapi Authentication Package: Negotiate Transited Services: - Package Name (NTLM only): - Key Length: 0 This event is generated when a logon session is created. It is generated on the computer that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service such as the Server service, or a local process such as Winlogon.exe or Services.exe. The logon type field indicates the kind of logon that occurred. The most common types are 2 (interactive) and 3 (network). The New Logon fields indicate the account for whom the new logon was created, i.e. the account that was logged on. The network fields indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impersonation level field indicates the extent to which a process in the logon session can impersonate. The authentication information fields provide detailed information about this specific logon request. - Logon GUID is a unique identifier that can be used to correlate this event with a KDC event. - Transited services indicate which intermediate services have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indicates the length of the generated session key. This will be 0 if no session key was requested.
Security	Audit Success	12544	2015-04-24 21:05:33	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: LTRANPHD$ Account Domain: WORKGROUP Logon ID: 0x3e7 Logon Type: 5 Impersonation Level: %%1833 New Logon: Security ID: S-1-5-19 Account Name: LOCAL SERVICE Account Domain: NT AUTHORITY Logon ID: 0x3e5 Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x230 Process Name: C:\Windows\System32\services.exe Network Information: Workstation Name: Source Network Address: - Source Port: - Detailed Authentication Information: Logon Process: Advapi Authentication Package: Negotiate Transited Services: - Package Name (NTLM only): - Key Length: 0 This event is generated when a logon session is created. It is generated on the computer that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service such as the Server service, or a local process such as Winlogon.exe or Services.exe. The logon type field indicates the kind of logon that occurred. The most common types are 2 (interactive) and 3 (network). The New Logon fields indicate the account for whom the new logon was created, i.e. the account that was logged on. The network fields indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impersonation level field indicates the extent to which a process in the logon session can impersonate. The authentication information fields provide detailed information about this specific logon request.

					- Logon GUID is a unique identifier that can be used to correlate this event with a KDC event. - Transited services indicate which intermediate services have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indicates the length of the generated session key. This will be 0 if no session key was requested.
Security	Audit Success	12544	2015-04-24 21:05:33	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: LTRANPHD$ Account Domain: WORKGROUP Logon ID: 0x3e7 Logon Type: 5 Impersonation Level: %%1833 New Logon: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Logon ID: 0x3e7 Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x230 Process Name: C:\Windows\System32\services.exe Network Information: Workstation Name: Source Network Address: - Source Port: - Detailed Authentication Information: Logon Process: Advapi Authentication Package: Negotiate Transited Services: - Package Name (NTLM only): - Key Length: 0 This event is generated when a logon session is created. It is generated on the computer that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service such as the Server service, or a local process such as Winlogon.exe or Services.exe. The logon type field indicates the kind of logon that occurred. The most common types are 2 (interactive) and 3 (network). The New Logon fields indicate the account for whom the new logon was created, i.e. the account that was logged on. The network fields indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impersonation level field indicates the extent to which a process in the logon session can impersonate. The authentication information fields provide detailed information about this specific logon request. - Logon GUID is a unique identifier that can be used to correlate this event with a KDC event. - Transited services indicate which intermediate services have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indicates the length of the generated session key. This will be 0 if no session key was requested.
Security	Audit Success	12544	2015-04-24 21:05:33	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: LTRANPHD$ Account Domain: WORKGROUP Logon ID: 0x3e7 Logon Type: 5 Impersonation Level: %%1833 New Logon: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Logon ID: 0x3e7 Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x230 Process Name: C:\Windows\System32\services.exe Network Information: Workstation Name: Source Network Address: - Source Port: - Detailed Authentication Information: Logon Process: Advapi Authentication Package: Negotiate Transited Services: - Package Name (NTLM only): - Key Length: 0 This event is generated when a logon session is created. It is generated on the computer that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service such as the Server service, or a local process such as Winlogon.exe or Services.exe. The logon type field indicates the kind of logon that occurred. The most common types are 2 (interactive) and 3 (network). The New Logon fields indicate the account for whom the new logon was created, i.e. the account that was logged on. The network fields indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impersonation level field indicates the extent to which a process in the logon session can impersonate. The authentication information fields provide detailed information about this specific logon request. - Logon GUID is a unique identifier that can be used to correlate this event with a KDC event. - Transited services indicate which intermediate services have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indicates the length of the generated session key. This will be 0 if no session key was requested.
Security	Audit Success	12544	2015-04-24 21:05:33	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: LTRANPHD$ Account Domain: WORKGROUP Logon ID: 0x3e7 Logon Type: 5 Impersonation Level: %%1833 New Logon: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Logon ID: 0x3e7 Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x230 Process Name: C:\Windows\System32\services.exe Network Information: Workstation Name: Source Network Address: - Source Port: - Detailed Authentication Information: Logon Process: Advapi Authentication Package: Negotiate Transited Services: - Package Name (NTLM only): - Key Length: 0 This event is generated when a logon session is created. It is generated on the computer that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service such as the Server service, or a local process such as Winlogon.exe or Services.exe. The logon type field indicates the kind of logon that occurred. The most common types are 2 (interactive) and 3 (network). The New Logon fields indicate the account for whom the new logon was created, i.e. the account that was logged on. The network fields indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impersonation level field indicates the extent to which a process in the logon session can impersonate. The authentication information fields provide detailed information about this specific logon request. - Logon GUID is a unique identifier that can be used to correlate this event with a KDC event. - Transited services indicate which intermediate services have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indicates the length of the generated session key. This will be 0 if no session key was requested.
					4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: LTRANPHD$ Account Domain: WORKGROUP Logon ID: 0x3e7 Logon Type: 5 Impersonation Level: %%1833 New Logon: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Logon ID: 0x3e7 Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x230 Process Name: C:\Windows\System32\services.exe Network Information: Workstation Name: Source Network Address: - Source Port: - Detailed Authentication Information: Logon Process: Advapi Authentication Package: Negotiate Transited

Security	Audit Success	12544	2015-04-24 21:05:33	Microsoft-Windows-Security-Auditing	Services: - Package Name (NTLM only): - Key Length: 0 This event is generated when a logon session is created. It is generated on the computer that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service such as the Server service, or a local process such as Winlogon.exe or Services.exe. The logon type field indicates the kind of logon that occurred. The most common types are 2 (interactive) and 3 (network). The New Logon fields indicate the account for whom the new logon was created, i.e. the account that was logged on. The network fields indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impersonation level field indicates the extent to which a process in the logon session can impersonate. The authentication information fields provide detailed information about this specific logon request. - Logon GUID is a unique identifier that can be used to correlate this event with a KDC event. - Transited services indicate which intermediate services have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indicates the length of the generated session key. This will be 0 if no session key was requested.
Security	Audit Success	12548	2015-04-24 21:05:33	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Logon ID: 0x3e7 Privileges: SeAssignPrimaryTokenPrivilege SeTcbPrivilege SeSecurityPrivilege SeTakeOwnershipPrivilege SeLoadDriverPrivilege SeBackupPrivilege SeRestorePrivilege SeDebugPrivilege SeAuditPrivilege SeSystemEnvironmentPrivilege SeImpersonatePrivilege
Security	Audit Success	12548	2015-04-24 21:05:33	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-20 Account Name: NETWORK SERVICE Account Domain: NT AUTHORITY Logon ID: 0x3e4 Privileges: SeAssignPrimaryTokenPrivilege SeAuditPrivilege SeImpersonatePrivilege
Security	Audit Success	12548	2015-04-24 21:05:33	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-90-1 Account Name: DWM-1 Account Domain: Window Manager Logon ID: 0xc9c8 Privileges: SeAssignPrimaryTokenPrivilege SeAuditPrivilege SeImpersonatePrivilege
Security	Audit Success	12548	2015-04-24 21:05:33	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-90-1 Account Name: DWM-1 Account Domain: Window Manager Logon ID: 0xc9dd Privileges: SeAssignPrimaryTokenPrivilege SeAuditPrivilege
Security	Audit Success	12548	2015-04-24 21:05:33	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-19 Account Name: LOCAL SERVICE Account Domain: NT AUTHORITY Logon ID: 0x3e5 Privileges: SeAssignPrimaryTokenPrivilege SeAuditPrivilege SeImpersonatePrivilege
Security	Audit Success	12548	2015-04-24 21:05:33	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Logon ID: 0x3e7 Privileges: SeAssignPrimaryTokenPrivilege SeTcbPrivilege SeSecurityPrivilege SeTakeOwnershipPrivilege SeLoadDriverPrivilege SeBackupPrivilege SeRestorePrivilege SeDebugPrivilege SeAuditPrivilege SeSystemEnvironmentPrivilege SeImpersonatePrivilege
Security	Audit Success	12548	2015-04-24 21:05:33	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Logon ID: 0x3e7 Privileges: SeAssignPrimaryTokenPrivilege SeTcbPrivilege SeSecurityPrivilege SeTakeOwnershipPrivilege SeLoadDriverPrivilege SeBackupPrivilege SeRestorePrivilege SeDebugPrivilege SeAuditPrivilege SeSystemEnvironmentPrivilege SeImpersonatePrivilege
Security	Audit Success	12548	2015-04-24 21:05:33	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Logon ID: 0x3e7 Privileges: SeAssignPrimaryTokenPrivilege SeTcbPrivilege SeSecurityPrivilege SeTakeOwnershipPrivilege SeLoadDriverPrivilege SeBackupPrivilege SeRestorePrivilege SeDebugPrivilege SeAuditPrivilege SeSystemEnvironmentPrivilege SeImpersonatePrivilege
Security	Audit Success	12548	2015-04-24 21:05:33	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Logon ID: 0x3e7 Privileges: SeAssignPrimaryTokenPrivilege SeTcbPrivilege SeSecurityPrivilege SeTakeOwnershipPrivilege SeLoadDriverPrivilege SeBackupPrivilege SeRestorePrivilege SeDebugPrivilege SeAuditPrivilege SeSystemEnvironmentPrivilege SeImpersonatePrivilege
Security	Audit Success	12544	2015-04-24 21:05:34	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: LTRANPHD$ Account Domain: WORKGROUP Logon ID: 0x3e7 Logon Type: 5 Impersonation Level: %%1833 New Logon: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Logon ID: 0x3e7 Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x230 Process Name: C:\Windows\System32\services.exe Network Information: Workstation Name: Source Network Address: - Source Port: - Detailed Authentication Information: Logon Process: Advapi Authentication Package: Negotiate Transited Services: - Package Name (NTLM only): - Key Length: 0 This event is generated when a logon session is created. It is generated on the computer that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service such as the Server service, or a local process such as Winlogon.exe or Services.exe. The logon type field indicates the kind of logon that occurred. The most common types are 2 (interactive) and 3 (network). The New Logon fields indicate the account for whom the new logon was created, i.e. the account that was logged on. The network fields indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impersonation level field indicates the extent to which a process in the logon session can impersonate. The authentication information fields provide detailed information about this specific logon request. - Logon GUID is a unique identifier that can be used to correlate this event with a KDC event. - Transited services indicate which intermediate services have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indicates the length of the generated session key. This will be 0 if no session key was requested.
					4624: An account was successfully logged on. Subject: Security ID: S-1-0-0 Account Name: - Account Domain:

Security	Audit Success	12544	2015-04-24 21:05:34	Microsoft-Windows-Security-Auditing	- Logon ID: 0x0 Logon Type: 3 Impersonation Level: %%1833 New Logon: Security ID: S-1-5-7 Account Name: ANONYMOUS LOGON Account Domain: NT AUTHORITY Logon ID: 0x18fd5 Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x0 Process Name: - Network Information: Workstation Name: Source Network Address: - Source Port: - Detailed Authentication Information: Logon Process: NtLmSsp Authentication Package: NTLM Transited Services: - Package Name (NTLM only): NTLM V1 Key Length: 0 This event is generated when a logon session is created. It is generated on the computer that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service such as the Server service, or a local process such as Winlogon.exe or Services.exe. The logon type field indicates the kind of logon that occurred. The most common types are 2 (interactive) and 3 (network). The New Logon fields indicate the account for whom the new logon was created, i.e. the account that was logged on. The network fields indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impersonation level field indicates the extent to which a process in the logon session can impersonate. The authentication information fields provide detailed information about this specific logon request. - Logon GUID is a unique identifier that can be used to correlate this event with a KDC event. - Transited services indicate which intermediate services have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indicates the length of the generated session key. This will be 0 if no session key was requested.
Security	Audit Success	12548	2015-04-24 21:05:34	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Logon ID: 0x3e7 Privileges: SeAssignPrimaryTokenPrivilege SeTcbPrivilege SeSecurityPrivilege SeTakeOwnershipPrivilege SeLoadDriverPrivilege SeBackupPrivilege SeRestorePrivilege SeDebugPrivilege SeAuditPrivilege SeSystemEnvironmentPrivilege SeImpersonatePrivilege
Security	Audit Success	103	2015-04-24 21:05:37	Microsoft-Windows-Eventlog	1100: The event logging service has shut down.
Security	Audit Success	12288	2015-04-24 21:06:22	Microsoft-Windows-Security-Auditing	4608: Windows is starting up. This event is logged when LSASS.EXE starts and the auditing subsystem is initialized.
Security	Audit Success	12544	2015-04-24 21:06:22	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-0-0 Account Name: - Account Domain: - Logon ID: 0x0 Logon Type: 0 Impersonation Level: - New Logon: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Logon ID: 0x3e7 Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x4 Process Name: Network Information: Workstation Name: - Source Network Address: - Source Port: - Detailed Authentication Information: Logon Process: - Authentication Package: - Transited Services: - Package Name (NTLM only): - Key Length: 0 This event is generated when a logon session is created. It is generated on the computer that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service such as the Server service, or a local process such as Winlogon.exe or Services.exe. The logon type field indicates the kind of logon that occurred. The most common types are 2 (interactive) and 3 (network). The New Logon fields indicate the account for whom the new logon was created, i.e. the account that was logged on. The network fields indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impersonation level field indicates the extent to which a process in the logon session can impersonate. The authentication information fields provide detailed information about this specific logon request. - Logon GUID is a unique identifier that can be used to correlate this event with a KDC event. - Transited services indicate which intermediate services have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indicates the length of the generated session key. This will be 0 if no session key was requested.
Security	Audit Success	12292	2015-04-24 21:06:23	Microsoft-Windows-Security-Auditing	5033: The Windows Firewall Driver started successfully.
Security	Audit Success	12292	2015-04-24 21:06:23	Microsoft-Windows-Security-Auditing	5024: The Windows Firewall service started successfully.
Security	Audit Success	12544	2015-04-24 21:06:23	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: LTRANPHD$ Account Domain: WORKGROUP Logon ID: 0x3e7 Logon Type: 5 Impersonation Level: %%1833 New Logon: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Logon ID: 0x3e7 Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x230 Process Name: C:\Windows\System32\services.exe Network Information: Workstation Name: Source Network Address: - Source Port: - Detailed Authentication Information: Logon Process: Advapi Authentication Package: Negotiate Transited Services: - Package Name (NTLM only): - Key Length: 0 This event is generated when a logon session is created. It is generated on the computer that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service such as the Server service, or a local process such as Winlogon.exe or Services.exe. The logon type field indicates the kind of logon that occurred. The most common types are 2 (interactive) and 3 (network). The New Logon fields indicate the account for whom the new logon was created, i.e. the account that was logged on. The network fields indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impersonation level field indicates the extent to which a process in the logon session can impersonate. The authentication information fields provide detailed information about this specific logon request.

					- Logon GUID is a unique identifier that can be used to correlate this event with a KDC event. - Transited services indicate which intermediate services have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indicates the length of the generated session key. This will be 0 if no session key was requested.
Security	Audit Success	12544	2015-04-24 21:06:23	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: LTRANPHD$ Account Domain: WORKGROUP Logon ID: 0x3e7 Logon Type: 5 Impersonation Level: %%1833 New Logon: Security ID: S-1-5-20 Account Name: NETWORK SERVICE Account Domain: NT AUTHORITY Logon ID: 0x3e4 Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x230 Process Name: C:\Windows\System32\services.exe Network Information: Workstation Name: Source Network Address: - Source Port: - Detailed Authentication Information: Logon Process: Advapi Authentication Package: Negotiate Transited Services: - Package Name (NTLM only): - Key Length: 0 This event is generated when a logon session is created. It is generated on the computer that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service such as the Server service, or a local process such as Winlogon.exe or Services.exe. The logon type field indicates the kind of logon that occurred. The most common types are 2 (interactive) and 3 (network). The New Logon fields indicate the account for whom the new logon was created, i.e. the account that was logged on. The network fields indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impersonation level field indicates the extent to which a process in the logon session can impersonate. The authentication information fields provide detailed information about this specific logon request. - Logon GUID is a unique identifier that can be used to correlate this event with a KDC event. - Transited services indicate which intermediate services have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indicates the length of the generated session key. This will be 0 if no session key was requested.
Security	Audit Success	12544	2015-04-24 21:06:23	Microsoft-Windows-Security-Auditing	4648: A logon was attempted using explicit credentials. Subject: Security ID: S-1-5-18 Account Name: LTRANPHD$ Account Domain: WORKGROUP Logon ID: 0x3e7 Logon GUID: {00000000-0000-0000-0000-000000000000} Account Whose Credentials Were Used: Account Name: DWM-1 Account Domain: Window Manager Logon GUID: {00000000-0000-0000-0000-000000000000} Target Server: Target Server Name: localhost Additional Information: localhost Process Information: Process ID: 0x200 Process Name: C:\Windows\System32\winlogon.exe Network Information: Network Address: - Port: - This event is generated when a process attempts to log on an account by explicitly specifying that account's credentials. This most commonly occurs in batch-type configurations such as scheduled tasks, or when using the RUNAS command.
Security	Audit Success	12544	2015-04-24 21:06:23	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: LTRANPHD$ Account Domain: WORKGROUP Logon ID: 0x3e7 Logon Type: 2 Impersonation Level: %%1833 New Logon: Security ID: S-1-5-90-1 Account Name: DWM-1 Account Domain: Window Manager Logon ID: 0xc9ca Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x200 Process Name: C:\Windows\System32\winlogon.exe Network Information: Workstation Name: Source Network Address: - Source Port: - Detailed Authentication Information: Logon Process: Advapi Authentication Package: Negotiate Transited Services: - Package Name (NTLM only): - Key Length: 0 This event is generated when a logon session is created. It is generated on the computer that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service such as the Server service, or a local process such as Winlogon.exe or Services.exe. The logon type field indicates the kind of logon that occurred. The most common types are 2 (interactive) and 3 (network). The New Logon fields indicate the account for whom the new logon was created, i.e. the account that was logged on. The network fields indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impersonation level field indicates the extent to which a process in the logon session can impersonate. The authentication information fields provide detailed information about this specific logon request. - Logon GUID is a unique identifier that can be used to correlate this event with a KDC event. - Transited services indicate which intermediate services have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indicates the length of the generated session key. This will be 0 if no session key was requested.
Security	Audit Success	12544	2015-04-24 21:06:23	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: LTRANPHD$ Account Domain: WORKGROUP Logon ID: 0x3e7 Logon Type: 2 Impersonation Level: %%1833 New Logon: Security ID: S-1-5-90-1 Account Name: DWM-1 Account Domain: Window Manager Logon ID: 0xc9e1 Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x200 Process Name: C:\Windows\System32\winlogon.exe Network Information: Workstation Name: Source Network Address: - Source Port: - Detailed Authentication Information: Logon Process: Advapi Authentication Package: Negotiate Transited Services: - Package Name (NTLM only): - Key Length: 0 This event is generated when a logon session is created. It is generated on the computer that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service such as the Server service, or a local process such as Winlogon.exe or Services.exe. The logon type field indicates the kind of logon that occurred. The most common types are 2 (interactive) and 3 (network). The New Logon fields indicate the account for whom the new logon was created, i.e. the account that was logged on. The network fields indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impersonation level field indicates the extent to which a process in the logon session can impersonate. The authentication information fields provide detailed information about this specific logon request. - Logon GUID is a unique identifier that can be used to correlate this event with a KDC event. - Transited services indicate which intermediate services have participated in this logon request. - Package name indicates

					which sub-protocol was used among the NTLM protocols. - Key length indicates the length of the generated session key. This will be 0 if no session key was requested.
Security	Audit Success	12544	2015-04-24 21:06:23	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: LTRANPHD$ Account Domain: WORKGROUP Logon ID: 0x3e7 Logon Type: 5 Impersonation Level: %%1833 New Logon: Security ID: S-1-5-19 Account Name: LOCAL SERVICE Account Domain: NT AUTHORITY Logon ID: 0x3e5 Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x230 Process Name: C:\Windows\System32\services.exe Network Information: Workstation Name: Source Network Address: - Source Port: - Detailed Authentication Information: Logon Process: Advapi Authentication Package: Negotiate Transited Services: - Package Name (NTLM only): - Key Length: 0 This event is generated when a logon session is created. It is generated on the computer that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service such as the Server service, or a local process such as Winlogon.exe or Services.exe. The logon type field indicates the kind of logon that occurred. The most common types are 2 (interactive) and 3 (network). The New Logon fields indicate the account for whom the new logon was created, i.e. the account that was logged on. The network fields indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impersonation level field indicates the extent to which a process in the logon session can impersonate. The authentication information fields provide detailed information about this specific logon request. - Logon GUID is a unique identifier that can be used to correlate this event with a KDC event. - Transited services indicate which intermediate services have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indicates the length of the generated session key. This will be 0 if no session key was requested.
Security	Audit Success	12544	2015-04-24 21:06:23	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: LTRANPHD$ Account Domain: WORKGROUP Logon ID: 0x3e7 Logon Type: 5 Impersonation Level: %%1833 New Logon: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Logon ID: 0x3e7 Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x230 Process Name: C:\Windows\System32\services.exe Network Information: Workstation Name: Source Network Address: - Source Port: - Detailed Authentication Information: Logon Process: Advapi Authentication Package: Negotiate Transited Services: - Package Name (NTLM only): - Key Length: 0 This event is generated when a logon session is created. It is generated on the computer that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service such as the Server service, or a local process such as Winlogon.exe or Services.exe. The logon type field indicates the kind of logon that occurred. The most common types are 2 (interactive) and 3 (network). The New Logon fields indicate the account for whom the new logon was created, i.e. the account that was logged on. The network fields indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impersonation level field indicates the extent to which a process in the logon session can impersonate. The authentication information fields provide detailed information about this specific logon request. - Logon GUID is a unique identifier that can be used to correlate this event with a KDC event. - Transited services indicate which intermediate services have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indicates the length of the generated session key. This will be 0 if no session key was requested.
Security	Audit Success	12544	2015-04-24 21:06:23	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: LTRANPHD$ Account Domain: WORKGROUP Logon ID: 0x3e7 Logon Type: 5 Impersonation Level: %%1833 New Logon: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Logon ID: 0x3e7 Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x230 Process Name: C:\Windows\System32\services.exe Network Information: Workstation Name: Source Network Address: - Source Port: - Detailed Authentication Information: Logon Process: Advapi Authentication Package: Negotiate Transited Services: - Package Name (NTLM only): - Key Length: 0 This event is generated when a logon session is created. It is generated on the computer that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service such as the Server service, or a local process such as Winlogon.exe or Services.exe. The logon type field indicates the kind of logon that occurred. The most common types are 2 (interactive) and 3 (network). The New Logon fields indicate the account for whom the new logon was created, i.e. the account that was logged on. The network fields indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impersonation level field indicates the extent to which a process in the logon session can impersonate. The authentication information fields provide detailed information about this specific logon request. - Logon GUID is a unique identifier that can be used to correlate this event with a KDC event. - Transited services indicate which intermediate services have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indicates the length of the generated session key. This will be 0 if no session key was requested.
					4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: LTRANPHD$ Account Domain: WORKGROUP Logon ID: 0x3e7 Logon Type: 5 Impersonation Level: %%1833 New Logon: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Logon ID: 0x3e7 Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x230 Process Name: C:\Windows\System32\services.exe Network Information: Workstation Name: Source Network Address: - Source Port: - Detailed Authentication Information: Logon Process: Advapi Authentication Package: Negotiate Transited Services: - Package Name (NTLM only): - Key Length: 0 This event is generated when a logon session is created. It is generated on the computer that was accessed. The subject fields indicate the account on the local

Security	Audit Success	12544	2015-04-24 21:06:23		Microsoft-Windows-Security-Auditing	system which requested the logon. This is most commonly a service such as the Server service, or a local process such as Winlogon.exe or Services.exe. The logon type field indicates the kind of logon that occurred. The most common types are 2 (interactive) and 3 (network). The New Logon fields indicate the account for whom the new logon was created, i.e. the account that was logged on. The network fields indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impersonation level field indicates the extent to which a process in the logon session can impersonate. The authentication information fields provide detailed information about this specific logon request. - Logon GUID is a unique identifier that can be used to correlate this event with a KDC event. - Transited services indicate which intermediate services have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indicates the length of the generated session key. This will be 0 if no session key was requested.
Security	Audit Success	12544	2015-04-24 21:06:23		Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: LTRANPHD$ Account Domain: WORKGROUP Logon ID: 0x3e7 Logon Type: 5 Impersonation Level: %%1833 New Logon: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Logon ID: 0x3e7 Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x230 Process Name: C:\Windows\System32\services.exe Network Information: Workstation Name: Source Network Address: - Source Port: - Detailed Authentication Information: Logon Process: Advapi Authentication Package: Negotiate Transited Services: - Package Name (NTLM only): - Key Length: 0 This event is generated when a logon session is created. It is generated on the computer that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service such as the Server service, or a local process such as Winlogon.exe or Services.exe. The logon type field indicates the kind of logon that occurred. The most common types are 2 (interactive) and 3 (network). The New Logon fields indicate the account for whom the new logon was created, i.e. the account that was logged on. The network fields indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impersonation level field indicates the extent to which a process in the logon session can impersonate. The authentication information fields provide detailed information about this specific logon request. - Logon GUID is a unique identifier that can be used to correlate this event with a KDC event. - Transited services indicate which intermediate services have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indicates the length of the generated session key. This will be 0 if no session key was requested.
Security	Audit Success	12548	2015-04-24 21:06:23		Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Logon ID: 0x3e7 Privileges: SeAssignPrimaryTokenPrivilege SeTcbPrivilege SeSecurityPrivilege SeTakeOwnershipPrivilege SeLoadDriverPrivilege SeBackupPrivilege SeRestorePrivilege SeDebugPrivilege SeAuditPrivilege SeSystemEnvironmentPrivilege SeImpersonatePrivilege
Security	Audit Success	12548	2015-04-24 21:06:23		Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-20 Account Name: NETWORK SERVICE Account Domain: NT AUTHORITY Logon ID: 0x3e4 Privileges: SeAssignPrimaryTokenPrivilege SeAuditPrivilege SeImpersonatePrivilege
Security	Audit Success	12548	2015-04-24 21:06:23		Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-90-1 Account Name: DWM-1 Account Domain: Window Manager Logon ID: 0xc9ca Privileges: SeAssignPrimaryTokenPrivilege SeAuditPrivilege SeImpersonatePrivilege
Security	Audit Success	12548	2015-04-24 21:06:23		Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-90-1 Account Name: DWM-1 Account Domain: Window Manager Logon ID: 0xc9e1 Privileges: SeAssignPrimaryTokenPrivilege SeAuditPrivilege
Security	Audit Success	12548	2015-04-24 21:06:23		Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-19 Account Name: LOCAL SERVICE Account Domain: NT AUTHORITY Logon ID: 0x3e5 Privileges: SeAssignPrimaryTokenPrivilege SeAuditPrivilege SeImpersonatePrivilege
Security	Audit Success	12548	2015-04-24 21:06:23		Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Logon ID: 0x3e7 Privileges: SeAssignPrimaryTokenPrivilege SeTcbPrivilege SeSecurityPrivilege SeTakeOwnershipPrivilege SeLoadDriverPrivilege SeBackupPrivilege SeRestorePrivilege SeDebugPrivilege SeAuditPrivilege SeSystemEnvironmentPrivilege SeImpersonatePrivilege
Security	Audit Success	12548	2015-04-24 21:06:23		Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Logon ID: 0x3e7 Privileges: SeAssignPrimaryTokenPrivilege SeTcbPrivilege SeSecurityPrivilege SeTakeOwnershipPrivilege SeLoadDriverPrivilege SeBackupPrivilege SeRestorePrivilege SeDebugPrivilege SeAuditPrivilege SeSystemEnvironmentPrivilege SeImpersonatePrivilege
Security	Audit Success	12548	2015-04-24 21:06:23		Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Logon ID: 0x3e7 Privileges: SeAssignPrimaryTokenPrivilege SeTcbPrivilege SeSecurityPrivilege SeTakeOwnershipPrivilege SeLoadDriverPrivilege SeBackupPrivilege SeRestorePrivilege SeDebugPrivilege SeAuditPrivilege SeSystemEnvironmentPrivilege SeImpersonatePrivilege
Security	Audit Success	12548	2015-04-24 21:06:23		Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Logon ID: 0x3e7 Privileges: SeAssignPrimaryTokenPrivilege SeTcbPrivilege SeSecurityPrivilege SeTakeOwnershipPrivilege SeLoadDriverPrivilege SeBackupPrivilege SeRestorePrivilege SeDebugPrivilege SeAuditPrivilege SeSystemEnvironmentPrivilege SeImpersonatePrivilege
Security	Audit Success	13568	2015-04-24 21:06:23		Microsoft-Windows-Security-Auditing	4902: The Per-user audit policy table was created. Number of Elements: 0 Policy ID: 0x7ac7

Security	Audit Success	12544	2015-04-24 21:06:24	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: LTRANPHD$ Account Domain: WORKGROUP Logon ID: 0x3e7 Logon Type: 5 Impersonation Level: %%1833 New Logon: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Logon ID: 0x3e7 Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x230 Process Name: C:\Windows\System32\services.exe Network Information: Workstation Name: Source Network Address: - Source Port: - Detailed Authentication Information: Logon Process: Advapi Authentication Package: Negotiate Transited Services: - Package Name (NTLM only): - Key Length: 0 This event is generated when a logon session is created. It is generated on the computer that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service such as the Server service, or a local process such as Winlogon.exe or Services.exe. The logon type field indicates the kind of logon that occurred. The most common types are 2 (interactive) and 3 (network). The New Logon fields indicate the account for whom the new logon was created, i.e. the account that was logged on. The network fields indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impersonation level field indicates the extent to which a process in the logon session can impersonate. The authentication information fields provide detailed information about this specific logon request. - Logon GUID is a unique identifier that can be used to correlate this event with a KDC event. - Transited services indicate which intermediate services have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indicates the length of the generated session key. This will be 0 if no session key was requested.
Security	Audit Success	12544	2015-04-24 21:06:24	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-0-0 Account Name: - Account Domain: - Logon ID: 0x0 Logon Type: 3 Impersonation Level: %%1833 New Logon: Security ID: S-1-5-7 Account Name: ANONYMOUS LOGON Account Domain: NT AUTHORITY Logon ID: 0x188bf Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x0 Process Name: - Network Information: Workstation Name: Source Network Address: - Source Port: - Detailed Authentication Information: Logon Process: NtLmSsp Authentication Package: NTLM Transited Services: - Package Name (NTLM only): NTLM V1 Key Length: 0 This event is generated when a logon session is created. It is generated on the computer that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service such as the Server service, or a local process such as Winlogon.exe or Services.exe. The logon type field indicates the kind of logon that occurred. The most common types are 2 (interactive) and 3 (network). The New Logon fields indicate the account for whom the new logon was created, i.e. the account that was logged on. The network fields indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impersonation level field indicates the extent to which a process in the logon session can impersonate. The authentication information fields provide detailed information about this specific logon request. - Logon GUID is a unique identifier that can be used to correlate this event with a KDC event. - Transited services indicate which intermediate services have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indicates the length of the generated session key. This will be 0 if no session key was requested.
Security	Audit Success	12548	2015-04-24 21:06:24	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Logon ID: 0x3e7 Privileges: SeAssignPrimaryTokenPrivilege SeTcbPrivilege SeSecurityPrivilege SeTakeOwnershipPrivilege SeLoadDriverPrivilege SeBackupPrivilege SeRestorePrivilege SeDebugPrivilege SeAuditPrivilege SeSystemEnvironmentPrivilege SeImpersonatePrivilege
Security	Audit Success	12544	2015-04-24 21:06:25	Microsoft-Windows-Security-Auditing	4648: A logon was attempted using explicit credentials. Subject: Security ID: S-1-5-18 Account Name: LTRANPHD$ Account Domain: WORKGROUP Logon ID: 0x3e7 Logon GUID: {00000000-0000-0000-0000-000000000000} Account Whose Credentials Were Used: Account Name: Liem Account Domain: LTRANPHD Logon GUID: {00000000-0000-0000-0000-000000000000} Target Server: Target Server Name: localhost Additional Information: localhost Process Information: Process ID: 0x200 Process Name: C:\Windows\System32\winlogon.exe Network Information: Network Address: 127.0.0.1 Port: 0 This event is generated when a process attempts to log on an account by explicitly specifying that account's credentials. This most commonly occurs in batch-type configurations such as scheduled tasks, or when using the RUNAS command.
Security	Audit Success	12544	2015-04-24 21:06:25	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: LTRANPHD$ Account Domain: WORKGROUP Logon ID: 0x3e7 Logon Type: 2 Impersonation Level: %%1833 New Logon: Security ID: S-1-5-21-1888849264-3803429180-4108621888-1001 Account Name: Liem Account Domain: LTRANPHD Logon ID: 0x1a5fb Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x200 Process Name: C:\Windows\System32\winlogon.exe Network Information: Workstation Name: LTRANPHD Source Network Address: 127.0.0.1 Source Port: 0 Detailed Authentication Information: Logon Process: User32 Authentication Package: Negotiate Transited Services: - Package Name (NTLM only): - Key Length: 0 This event is generated when a logon session is created. It is generated on the computer that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service such as the Server service, or a local process such as Winlogon.exe or Services.exe. The logon type field indicates the kind of logon that occurred. The most common types are 2 (interactive) and 3 (network). The New Logon fields indicate the account for whom the new logon was created, i.e. the account that was logged on. The network fields indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impersonation level field indicates the extent to which a process in the logon session can impersonate. The authentication information fields provide detailed information about this specific logon request. - Logon GUID is a unique identifier that can be used to correlate this event with a KDC event. - Transited services indicate which intermediate services have participated in this

					logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indicates the length of the generated session key. This will be 0 if no session key was requested.
Security	Audit Success	12544	2015-04-24 21:06:25	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: LTRANPHD$ Account Domain: WORKGROUP Logon ID: 0x3e7 Logon Type: 2 Impersonation Level: %%1833 New Logon: Security ID: S-1-5-21-1888849264-3803429180-4108621888-1001 Account Name: Liem Account Domain: LTRANPHD Logon ID: 0x1a62a Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x200 Process Name: C:\Windows\System32\winlogon.exe Network Information: Workstation Name: LTRANPHD Source Network Address: 127.0.0.1 Source Port: 0 Detailed Authentication Information: Logon Process: User32 Authentication Package: Negotiate Transited Services: - Package Name (NTLM only): - Key Length: 0 This event is generated when a logon session is created. It is generated on the computer that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service such as the Server service, or a local process such as Winlogon.exe or Services.exe. The logon type field indicates the kind of logon that occurred. The most common types are 2 (interactive) and 3 (network). The New Logon fields indicate the account for whom the new logon was created, i.e. the account that was logged on. The network fields indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impersonation level field indicates the extent to which a process in the logon session can impersonate. The authentication information fields provide detailed information about this specific logon request. - Logon GUID is a unique identifier that can be used to correlate this event with a KDC event. - Transited services indicate which intermediate services have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indicates the length of the generated session key. This will be 0 if no session key was requested.
Security	Audit Success	12544	2015-04-24 21:06:25	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: LTRANPHD$ Account Domain: WORKGROUP Logon ID: 0x3e7 Logon Type: 5 Impersonation Level: %%1833 New Logon: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Logon ID: 0x3e7 Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x230 Process Name: C:\Windows\System32\services.exe Network Information: Workstation Name: Source Network Address: - Source Port: - Detailed Authentication Information: Logon Process: Advapi Authentication Package: Negotiate Transited Services: - Package Name (NTLM only): - Key Length: 0 This event is generated when a logon session is created. It is generated on the computer that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service such as the Server service, or a local process such as Winlogon.exe or Services.exe. The logon type field indicates the kind of logon that occurred. The most common types are 2 (interactive) and 3 (network). The New Logon fields indicate the account for whom the new logon was created, i.e. the account that was logged on. The network fields indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impersonation level field indicates the extent to which a process in the logon session can impersonate. The authentication information fields provide detailed information about this specific logon request. - Logon GUID is a unique identifier that can be used to correlate this event with a KDC event. - Transited services indicate which intermediate services have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indicates the length of the generated session key. This will be 0 if no session key was requested.
Security	Audit Success	12548	2015-04-24 21:06:25	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-21-1888849264-3803429180-4108621888-1001 Account Name: Liem Account Domain: LTRANPHD Logon ID: 0x1a5fb Privileges: SeSecurityPrivilege SeTakeOwnershipPrivilege SeLoadDriverPrivilege SeBackupPrivilege SeRestorePrivilege SeDebugPrivilege SeSystemEnvironmentPrivilege SeImpersonatePrivilege
Security	Audit Success	12548	2015-04-24 21:06:25	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Logon ID: 0x3e7 Privileges: SeAssignPrimaryTokenPrivilege SeTcbPrivilege SeSecurityPrivilege SeTakeOwnershipPrivilege SeLoadDriverPrivilege SeBackupPrivilege SeRestorePrivilege SeDebugPrivilege SeAuditPrivilege SeSystemEnvironmentPrivilege SeImpersonatePrivilege
Security	Audit Success	13824	2015-04-24 21:06:28	Microsoft-Windows-Security-Auditing	4797: An attempt was made to query the existence of a blank password for an account. Subject: Security ID: S-1-5-21-1888849264-3803429180-4108621888-1001 Account Name: Liem Account Domain: LTRANPHD Logon ID: 0x1a62a Additional Information: Caller Workstation: LTRANPHD Target Account Name: Administrator Target Account Domain: LTRANPHD
Security	Audit Success	13824	2015-04-24 21:06:28	Microsoft-Windows-Security-Auditing	4797: An attempt was made to query the existence of a blank password for an account. Subject: Security ID: S-1-5-21-1888849264-3803429180-4108621888-1001 Account Name: Liem Account Domain: LTRANPHD Logon ID: 0x1a62a Additional Information: Caller Workstation: LTRANPHD Target Account Name: Guest Target Account Domain: LTRANPHD
Security	Audit Success	13824	2015-04-24 21:06:28	Microsoft-Windows-Security-Auditing	4797: An attempt was made to query the existence of a blank password for an account. Subject: Security ID: S-1-5-21-1888849264-3803429180-4108621888-1001 Account Name: Liem Account Domain: LTRANPHD Logon ID: 0x1a62a Additional Information: Caller Workstation: LTRANPHD Target Account Name: Administrator Target Account Domain: LTRANPHD
Security	Audit Success	13824	2015-04-24 21:06:28	Microsoft-Windows-Security-Auditing	4797: An attempt was made to query the existence of a blank password for an account. Subject: Security ID: S-1-5-21-1888849264-3803429180-4108621888-1001 Account Name: Liem Account Domain: LTRANPHD Logon ID: 0x1a62a Additional Information: Caller Workstation: LTRANPHD Target Account Name: Guest Target Account Domain: LTRANPHD
					4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: LTRANPHD$

Security	Audit Success	12544	2015-04-24 21:06:31		Microsoft-Windows-Security-Auditing	Account Domain: WORKGROUP Logon ID: 0x3e7 Logon Type: 5 Impersonation Level: %%1833 New Logon: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Logon ID: 0x3e7 Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x230 Process Name: C:\Windows\System32\services.exe Network Information: Workstation Name: Source Network Address: - Source Port: - Detailed Authentication Information: Logon Process: Advapi Authentication Package: Negotiate Transited Services: - Package Name (NTLM only): - Key Length: 0 This event is generated when a logon session is created. It is generated on the computer that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service such as the Server service, or a local process such as Winlogon.exe or Services.exe. The logon type field indicates the kind of logon that occurred. The most common types are 2 (interactive) and 3 (network). The New Logon fields indicate the account for whom the new logon was created, i.e. the account that was logged on. The network fields indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impersonation level field indicates the extent to which a process in the logon session can impersonate. The authentication information fields provide detailed information about this specific logon request. - Logon GUID is a unique identifier that can be used to correlate this event with a KDC event. - Transited services indicate which intermediate services have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indicates the length of the generated session key. This will be 0 if no session key was requested.
Security	Audit Success	12548	2015-04-24 21:06:31		Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Logon ID: 0x3e7 Privileges: SeAssignPrimaryTokenPrivilege SeTcbPrivilege SeSecurityPrivilege SeTakeOwnershipPrivilege SeLoadDriverPrivilege SeBackupPrivilege SeRestorePrivilege SeDebugPrivilege SeAuditPrivilege SeSystemEnvironmentPrivilege SeImpersonatePrivilege
Security	Audit Success	13824	2015-04-24 21:06:32		Microsoft-Windows-Security-Auditing	4797: An attempt was made to query the existence of a blank password for an account. Subject: Security ID: S-1-5-19 Account Name: LOCAL SERVICE Account Domain: NT AUTHORITY Logon ID: 0x3e5 Additional Information: Caller Workstation: LTRANPHD Target Account Name: Administrator Target Account Domain: LTRANPHD
Security	Audit Success	13824	2015-04-24 21:06:32		Microsoft-Windows-Security-Auditing	4797: An attempt was made to query the existence of a blank password for an account. Subject: Security ID: S-1-5-19 Account Name: LOCAL SERVICE Account Domain: NT AUTHORITY Logon ID: 0x3e5 Additional Information: Caller Workstation: LTRANPHD Target Account Name: Administrator Target Account Domain: LTRANPHD
Security	Audit Success	13824	2015-04-24 21:06:32		Microsoft-Windows-Security-Auditing	4797: An attempt was made to query the existence of a blank password for an account. Subject: Security ID: S-1-5-19 Account Name: LOCAL SERVICE Account Domain: NT AUTHORITY Logon ID: 0x3e5 Additional Information: Caller Workstation: LTRANPHD Target Account Name: Guest Target Account Domain: LTRANPHD
Security	Audit Success	13824	2015-04-24 21:06:32		Microsoft-Windows-Security-Auditing	4797: An attempt was made to query the existence of a blank password for an account. Subject: Security ID: S-1-5-19 Account Name: LOCAL SERVICE Account Domain: NT AUTHORITY Logon ID: 0x3e5 Additional Information: Caller Workstation: LTRANPHD Target Account Name: Guest Target Account Domain: LTRANPHD
Security	Audit Success	13824	2015-04-24 21:06:32		Microsoft-Windows-Security-Auditing	4797: An attempt was made to query the existence of a blank password for an account. Subject: Security ID: S-1-5-19 Account Name: LOCAL SERVICE Account Domain: NT AUTHORITY Logon ID: 0x3e5 Additional Information: Caller Workstation: LTRANPHD Target Account Name: Liem Target Account Domain: LTRANPHD
Security	Audit Success	13824	2015-04-24 21:06:32		Microsoft-Windows-Security-Auditing	4797: An attempt was made to query the existence of a blank password for an account. Subject: Security ID: S-1-5-19 Account Name: LOCAL SERVICE Account Domain: NT AUTHORITY Logon ID: 0x3e5 Additional Information: Caller Workstation: LTRANPHD Target Account Name: Liem Target Account Domain: LTRANPHD
Security	Audit Success	13824	2015-04-24 21:06:32		Microsoft-Windows-Security-Auditing	4797: An attempt was made to query the existence of a blank password for an account. Subject: Security ID: S-1-5-19 Account Name: LOCAL SERVICE Account Domain: NT AUTHORITY Logon ID: 0x3e5 Additional Information: Caller Workstation: LTRANPHD Target Account Name: Liem Target Account Domain: LTRANPHD
Security	Audit Success	13824	2015-04-24 21:06:32		Microsoft-Windows-Security-Auditing	4797: An attempt was made to query the existence of a blank password for an account. Subject: Security ID: S-1-5-19 Account Name: LOCAL SERVICE Account Domain: NT AUTHORITY Logon ID: 0x3e5 Additional Information: Caller Workstation: LTRANPHD Target Account Name: Liem Target Account Domain: LTRANPHD
Security	Audit Success	12544	2015-04-24 21:06:34		Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: LTRANPHD$ Account Domain: WORKGROUP Logon ID: 0x3e7 Logon Type: 5 Impersonation Level: %%1833 New Logon: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Logon ID: 0x3e7 Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x230 Process Name: C:\Windows\System32\services.exe Network Information: Workstation Name: Source Network Address: - Source Port: - Detailed Authentication Information: Logon Process: Advapi Authentication Package: Negotiate Transited Services: - Package Name (NTLM only): - Key Length: 0 This event is generated when a logon session is created. It is generated on the computer that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service such as the Server service, or a local process such as Winlogon.exe or Services.exe. The logon type field indicates the kind of logon that occurred. The most common types are 2 (interactive) and 3 (network). The New Logon fields indicate the account for whom the new logon was created, i.e. the account that was logged on. The network fields indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impersonation level field indicates the extent to which a process in the logon session can impersonate. The authentication information fields provide detailed information about this specific logon request. - Logon GUID is a unique identifier that can be used to correlate this event with a KDC event. - Transited services indicate which intermediate services have participated in this logon request. - Package name indicates

					which sub-protocol was used among the NTLM protocols. - Key length indicates the length of the generated session key. This will be 0 if no session key was requested.
	Security	Audit Success	12548	2015-04-24 21:06:34	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Logon ID: 0x3e7 Privileges: SeAssignPrimaryTokenPrivilege SeTcbPrivilege SeSecurityPrivilege SeTakeOwnershipPrivilege SeLoadDriverPrivilege SeBackupPrivilege SeRestorePrivilege SeDebugPrivilege SeAuditPrivilege SeSystemEnvironmentPrivilege SeImpersonatePrivilege
	Security	Audit Success	12544	2015-04-24 21:17:09	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: LTRANPHD$ Account Domain: WORKGROUP Logon ID: 0x3e7 Logon Type: 5 Impersonation Level: %%1833 New Logon: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Logon ID: 0x3e7 Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x230 Process Name: C:\Windows\System32\services.exe Network Information: Workstation Name: Source Network Address: - Source Port: - Detailed Authentication Information: Logon Process: Advapi Authentication Package: Negotiate Transited Services: - Package Name (NTLM only): - Key Length: 0 This event is generated when a logon session is created. It is generated on the computer that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service such as the Server service, or a local process such as Winlogon.exe or Services.exe. The logon type field indicates the kind of logon that occurred. The most common types are 2 (interactive) and 3 (network). The New Logon fields indicate the account for whom the new logon was created, i.e. the account that was logged on. The network fields indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impersonation level field indicates the extent to which a process in the logon session can impersonate. The authentication information fields provide detailed information about this specific logon request. - Logon GUID is a unique identifier that can be used to correlate this event with a KDC event. - Transited services indicate which intermediate services have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indicates the length of the generated session key. This will be 0 if no session key was requested.
	Security	Audit Success	12548	2015-04-24 21:17:09	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Logon ID: 0x3e7 Privileges: SeAssignPrimaryTokenPrivilege SeTcbPrivilege SeSecurityPrivilege SeTakeOwnershipPrivilege SeLoadDriverPrivilege SeBackupPrivilege SeRestorePrivilege SeDebugPrivilege SeAuditPrivilege SeSystemEnvironmentPrivilege SeImpersonatePrivilege
	Security	Audit Success	12544	2015-04-24 21:23:01	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: LTRANPHD$ Account Domain: WORKGROUP Logon ID: 0x3e7 Logon Type: 5 Impersonation Level: %%1833 New Logon: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Logon ID: 0x3e7 Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x230 Process Name: C:\Windows\System32\services.exe Network Information: Workstation Name: Source Network Address: - Source Port: - Detailed Authentication Information: Logon Process: Advapi Authentication Package: Negotiate Transited Services: - Package Name (NTLM only): - Key Length: 0 This event is generated when a logon session is created. It is generated on the computer that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service such as the Server service, or a local process such as Winlogon.exe or Services.exe. The logon type field indicates the kind of logon that occurred. The most common types are 2 (interactive) and 3 (network). The New Logon fields indicate the account for whom the new logon was created, i.e. the account that was logged on. The network fields indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impersonation level field indicates the extent to which a process in the logon session can impersonate. The authentication information fields provide detailed information about this specific logon request. - Logon GUID is a unique identifier that can be used to correlate this event with a KDC event. - Transited services indicate which intermediate services have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indicates the length of the generated session key. This will be 0 if no session key was requested.
	Security	Audit Success	12548	2015-04-24 21:23:01	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Logon ID: 0x3e7 Privileges: SeAssignPrimaryTokenPrivilege SeTcbPrivilege SeSecurityPrivilege SeTakeOwnershipPrivilege SeLoadDriverPrivilege SeBackupPrivilege SeRestorePrivilege SeDebugPrivilege SeAuditPrivilege SeSystemEnvironmentPrivilege SeImpersonatePrivilege
	Security	Audit Success	12288	2015-04-24 21:36:33	Microsoft-Windows-Security-Auditing	4608: Windows is starting up. This event is logged when LSASS.EXE starts and the auditing subsystem is initialized.
	Security	Audit Success	12544	2015-04-24 21:36:33	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-0-0 Account Name: - Account Domain: - Logon ID: 0x0 Logon Type: 0 Impersonation Level: - New Logon: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Logon ID: 0x3e7 Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x4 Process Name: Network Information: Workstation Name: - Source Network Address: - Source Port: - Detailed Authentication Information: Logon Process: - Authentication Package: - Transited Services: - Package Name (NTLM only): - Key Length: 0 This event is generated when a logon session is created. It is generated on the computer that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service such as the Server service, or a local process such as Winlogon.exe or Services.exe. The logon type field indicates the kind of logon that occurred. The most common types are 2 (interactive) and 3 (network). The New Logon fields indicate the account for whom the new logon was created, i.e. the account that was logged

					on. The network fields indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impersonation level field indicates the extent to which a process in the logon session can impersonate. The authentication information fields provide detailed information about this specific logon request. - Logon GUID is a unique identifier that can be used to correlate this event with a KDC event. - Transited services indicate which intermediate services have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indicates the length of the generated session key. This will be 0 if no session key was requested.
Security	Audit Success	12544	2015-04-24 21:36:33	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: LTRANPHD$ Account Domain: WORKGROUP Logon ID: 0x3e7 Logon Type: 5 Impersonation Level: %%1833 New Logon: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Logon ID: 0x3e7 Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x22c Process Name: C:\Windows\System32\services.exe Network Information: Workstation Name: Source Network Address: - Source Port: - Detailed Authentication Information: Logon Process: Advapi Authentication Package: Negotiate Transited Services: - Package Name (NTLM only): - Key Length: 0 This event is generated when a logon session is created. It is generated on the computer that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service such as the Server service, or a local process such as Winlogon.exe or Services.exe. The logon type field indicates the kind of logon that occurred. The most common types are 2 (interactive) and 3 (network). The New Logon fields indicate the account for whom the new logon was created, i.e. the account that was logged on. The network fields indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impersonation level field indicates the extent to which a process in the logon session can impersonate. The authentication information fields provide detailed information about this specific logon request. - Logon GUID is a unique identifier that can be used to correlate this event with a KDC event. - Transited services indicate which intermediate services have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indicates the length of the generated session key. This will be 0 if no session key was requested.
Security	Audit Success	12544	2015-04-24 21:36:33	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: LTRANPHD$ Account Domain: WORKGROUP Logon ID: 0x3e7 Logon Type: 5 Impersonation Level: %%1833 New Logon: Security ID: S-1-5-20 Account Name: NETWORK SERVICE Account Domain: NT AUTHORITY Logon ID: 0x3e4 Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x22c Process Name: C:\Windows\System32\services.exe Network Information: Workstation Name: Source Network Address: - Source Port: - Detailed Authentication Information: Logon Process: Advapi Authentication Package: Negotiate Transited Services: - Package Name (NTLM only): - Key Length: 0 This event is generated when a logon session is created. It is generated on the computer that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service such as the Server service, or a local process such as Winlogon.exe or Services.exe. The logon type field indicates the kind of logon that occurred. The most common types are 2 (interactive) and 3 (network). The New Logon fields indicate the account for whom the new logon was created, i.e. the account that was logged on. The network fields indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impersonation level field indicates the extent to which a process in the logon session can impersonate. The authentication information fields provide detailed information about this specific logon request. - Logon GUID is a unique identifier that can be used to correlate this event with a KDC event. - Transited services indicate which intermediate services have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indicates the length of the generated session key. This will be 0 if no session key was requested.
Security	Audit Success	12548	2015-04-24 21:36:33	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Logon ID: 0x3e7 Privileges: SeAssignPrimaryTokenPrivilege SeTcbPrivilege SeSecurityPrivilege SeTakeOwnershipPrivilege SeLoadDriverPrivilege SeBackupPrivilege SeRestorePrivilege SeDebugPrivilege SeAuditPrivilege SeSystemEnvironmentPrivilege SeImpersonatePrivilege
Security	Audit Success	12548	2015-04-24 21:36:33	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-20 Account Name: NETWORK SERVICE Account Domain: NT AUTHORITY Logon ID: 0x3e4 Privileges: SeAssignPrimaryTokenPrivilege SeAuditPrivilege SeImpersonatePrivilege
Security	Audit Success	13568	2015-04-24 21:36:33	Microsoft-Windows-Security-Auditing	4902: The Per-user audit policy table was created. Number of Elements: 0 Policy ID: 0x9b70
Security	Audit Success	12544	2015-04-24 21:36:34	Microsoft-Windows-Security-Auditing	4648: A logon was attempted using explicit credentials. Subject: Security ID: S-1-5-18 Account Name: LTRANPHD$ Account Domain: WORKGROUP Logon ID: 0x3e7 Logon GUID: {00000000-0000-0000-0000-000000000000} Account Whose Credentials Were Used: Account Name: DWM-1 Account Domain: Window Manager Logon GUID: {00000000-0000-0000-0000-000000000000} Target Server: Target Server Name: localhost Additional Information: localhost Process Information: Process ID: 0x1fc Process Name: C:\Windows\System32\winlogon.exe Network Information: Network Address: - Port: - This event is generated when a process attempts to log on an account by explicitly specifying that account's credentials. This most commonly occurs in batch-type configurations such as scheduled tasks, or when using the RUNAS command.
					4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: LTRANPHD$ Account Domain: WORKGROUP Logon ID: 0x3e7 Logon Type: 2 Impersonation Level: %%1833 New Logon: Security ID: S-1-5-90-1 Account Name: DWM-1 Account Domain: Window Manager Logon ID: 0xea1f Logon

Security	Audit Success	12544	2015-04-24 21:36:34	Microsoft-Windows-Security-Auditing	GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x1fc Process Name: C:\Windows\System32\winlogon.exe Network Information: Workstation Name: Source Network Address: - Source Port: - Detailed Authentication Information: Logon Process: Advapi Authentication Package: Negotiate Transited Services: - Package Name (NTLM only): - Key Length: 0 This event is generated when a logon session is created. It is generated on the computer that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service such as the Server service, or a local process such as Winlogon.exe or Services.exe. The logon type field indicates the kind of logon that occurred. The most common types are 2 (interactive) and 3 (network). The New Logon fields indicate the account for whom the new logon was created, i.e. the account that was logged on. The network fields indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impersonation level field indicates the extent to which a process in the logon session can impersonate. The authentication information fields provide detailed information about this specific logon request. - Logon GUID is a unique identifier that can be used to correlate this event with a KDC event. - Transited services indicate which intermediate services have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indicates the length of the generated session key. This will be 0 if no session key was requested.
Security	Audit Success	12544	2015-04-24 21:36:34	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: LTRANPHD$ Account Domain: WORKGROUP Logon ID: 0x3e7 Logon Type: 2 Impersonation Level: %%1833 New Logon: Security ID: S-1-5-90-1 Account Name: DWM-1 Account Domain: Window Manager Logon ID: 0xea3c Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x1fc Process Name: C:\Windows\System32\winlogon.exe Network Information: Workstation Name: Source Network Address: - Source Port: - Detailed Authentication Information: Logon Process: Advapi Authentication Package: Negotiate Transited Services: - Package Name (NTLM only): - Key Length: 0 This event is generated when a logon session is created. It is generated on the computer that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service such as the Server service, or a local process such as Winlogon.exe or Services.exe. The logon type field indicates the kind of logon that occurred. The most common types are 2 (interactive) and 3 (network). The New Logon fields indicate the account for whom the new logon was created, i.e. the account that was logged on. The network fields indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impersonation level field indicates the extent to which a process in the logon session can impersonate. The authentication information fields provide detailed information about this specific logon request. - Logon GUID is a unique identifier that can be used to correlate this event with a KDC event. - Transited services indicate which intermediate services have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indicates the length of the generated session key. This will be 0 if no session key was requested.
Security	Audit Success	12544	2015-04-24 21:36:34	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: LTRANPHD$ Account Domain: WORKGROUP Logon ID: 0x3e7 Logon Type: 5 Impersonation Level: %%1833 New Logon: Security ID: S-1-5-19 Account Name: LOCAL SERVICE Account Domain: NT AUTHORITY Logon ID: 0x3e5 Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x22c Process Name: C:\Windows\System32\services.exe Network Information: Workstation Name: Source Network Address: - Source Port: - Detailed Authentication Information: Logon Process: Advapi Authentication Package: Negotiate Transited Services: - Package Name (NTLM only): - Key Length: 0 This event is generated when a logon session is created. It is generated on the computer that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service such as the Server service, or a local process such as Winlogon.exe or Services.exe. The logon type field indicates the kind of logon that occurred. The most common types are 2 (interactive) and 3 (network). The New Logon fields indicate the account for whom the new logon was created, i.e. the account that was logged on. The network fields indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impersonation level field indicates the extent to which a process in the logon session can impersonate. The authentication information fields provide detailed information about this specific logon request. - Logon GUID is a unique identifier that can be used to correlate this event with a KDC event. - Transited services indicate which intermediate services have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indicates the length of the generated session key. This will be 0 if no session key was requested.
Security	Audit Success	12544	2015-04-24 21:36:34	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: LTRANPHD$ Account Domain: WORKGROUP Logon ID: 0x3e7 Logon Type: 5 Impersonation Level: %%1833 New Logon: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Logon ID: 0x3e7 Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x22c Process Name: C:\Windows\System32\services.exe Network Information: Workstation Name: Source Network Address: - Source Port: - Detailed Authentication Information: Logon Process: Advapi Authentication Package: Negotiate Transited Services: - Package Name (NTLM only): - Key Length: 0 This event is generated when a logon session is created. It is generated on the computer that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service such as the Server service, or a local process such as Winlogon.exe or Services.exe. The logon type field indicates the kind of logon that occurred. The most common types are 2 (interactive) and 3 (network). The New Logon fields indicate the account for whom the new logon was created, i.e. the account that was logged on. The network fields indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some

					cases. The impersonation level field indicates the extent to which a process in the logon session can impersonate. The authentication information fields provide detailed information about this specific logon request. - Logon GUID is a unique identifier that can be used to correlate this event with a KDC event. - Transited services indicate which intermediate services have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indicates the length of the generated session key. This will be 0 if no session key was requested.
Security	Audit Success	12544	2015-04-24 21:36:34	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: LTRANPHD$ Account Domain: WORKGROUP Logon ID: 0x3e7 Logon Type: 5 Impersonation Level: %%1833 New Logon: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Logon ID: 0x3e7 Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x22c Process Name: C:\Windows\System32\services.exe Network Information: Workstation Name: Source Network Address: - Source Port: - Detailed Authentication Information: Logon Process: Advapi Authentication Package: Negotiate Transited Services: - Package Name (NTLM only): - Key Length: 0 This event is generated when a logon session is created. It is generated on the computer that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service such as the Server service, or a local process such as Winlogon.exe or Services.exe. The logon type field indicates the kind of logon that occurred. The most common types are 2 (interactive) and 3 (network). The New Logon fields indicate the account for whom the new logon was created, i.e. the account that was logged on. The network fields indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impersonation level field indicates the extent to which a process in the logon session can impersonate. The authentication information fields provide detailed information about this specific logon request. - Logon GUID is a unique identifier that can be used to correlate this event with a KDC event. - Transited services indicate which intermediate services have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indicates the length of the generated session key. This will be 0 if no session key was requested.
Security	Audit Success	12544	2015-04-24 21:36:34	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: LTRANPHD$ Account Domain: WORKGROUP Logon ID: 0x3e7 Logon Type: 5 Impersonation Level: %%1833 New Logon: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Logon ID: 0x3e7 Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x22c Process Name: C:\Windows\System32\services.exe Network Information: Workstation Name: Source Network Address: - Source Port: - Detailed Authentication Information: Logon Process: Advapi Authentication Package: Negotiate Transited Services: - Package Name (NTLM only): - Key Length: 0 This event is generated when a logon session is created. It is generated on the computer that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service such as the Server service, or a local process such as Winlogon.exe or Services.exe. The logon type field indicates the kind of logon that occurred. The most common types are 2 (interactive) and 3 (network). The New Logon fields indicate the account for whom the new logon was created, i.e. the account that was logged on. The network fields indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impersonation level field indicates the extent to which a process in the logon session can impersonate. The authentication information fields provide detailed information about this specific logon request. - Logon GUID is a unique identifier that can be used to correlate this event with a KDC event. - Transited services indicate which intermediate services have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indicates the length of the generated session key. This will be 0 if no session key was requested.
Security	Audit Success	12548	2015-04-24 21:36:34	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-90-1 Account Name: DWM-1 Account Domain: Window Manager Logon ID: 0xea1f Privileges: SeAssignPrimaryTokenPrivilege SeAuditPrivilege SeImpersonatePrivilege
Security	Audit Success	12548	2015-04-24 21:36:34	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-90-1 Account Name: DWM-1 Account Domain: Window Manager Logon ID: 0xea3c Privileges: SeAssignPrimaryTokenPrivilege SeAuditPrivilege
Security	Audit Success	12548	2015-04-24 21:36:34	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-19 Account Name: LOCAL SERVICE Account Domain: NT AUTHORITY Logon ID: 0x3e5 Privileges: SeAssignPrimaryTokenPrivilege SeAuditPrivilege SeImpersonatePrivilege
Security	Audit Success	12548	2015-04-24 21:36:34	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Logon ID: 0x3e7 Privileges: SeAssignPrimaryTokenPrivilege SeTcbPrivilege SeSecurityPrivilege SeTakeOwnershipPrivilege SeLoadDriverPrivilege SeBackupPrivilege SeRestorePrivilege SeDebugPrivilege SeAuditPrivilege SeSystemEnvironmentPrivilege SeImpersonatePrivilege
Security	Audit Success	12548	2015-04-24 21:36:34	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Logon ID: 0x3e7 Privileges: SeAssignPrimaryTokenPrivilege SeTcbPrivilege SeSecurityPrivilege SeTakeOwnershipPrivilege SeLoadDriverPrivilege SeBackupPrivilege SeRestorePrivilege SeDebugPrivilege SeAuditPrivilege SeSystemEnvironmentPrivilege SeImpersonatePrivilege
Security	Audit Success	12548	2015-04-24 21:36:34	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Logon ID: 0x3e7 Privileges: SeAssignPrimaryTokenPrivilege SeTcbPrivilege SeSecurityPrivilege SeTakeOwnershipPrivilege SeLoadDriverPrivilege SeBackupPrivilege SeRestorePrivilege SeDebugPrivilege SeAuditPrivilege SeSystemEnvironmentPrivilege SeImpersonatePrivilege

Security	Audit Success	12292	2015-04-24 21:36:35	Microsoft-Windows-Security-Auditing	5033: The Windows Firewall Driver started successfully.
Security	Audit Success	12292	2015-04-24 21:36:35	Microsoft-Windows-Security-Auditing	5024: The Windows Firewall service started successfully.
Security	Audit Success	12544	2015-04-24 21:36:35	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: LTRANPHD$ Account Domain: WORKGROUP Logon ID: 0x3e7 Logon Type: 5 Impersonation Level: %%1833 New Logon: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Logon ID: 0x3e7 Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x22c Process Name: C:\Windows\System32\services.exe Network Information: Workstation Name: Source Network Address: - Source Port: - Detailed Authentication Information: Logon Process: Advapi Authentication Package: Negotiate Transited Services: - Package Name (NTLM only): - Key Length: 0 This event is generated when a logon session is created. It is generated on the computer that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service such as the Server service, or a local process such as Winlogon.exe or Services.exe. The logon type field indicates the kind of logon that occurred. The most common types are 2 (interactive) and 3 (network). The New Logon fields indicate the account for whom the new logon was created, i.e. the account that was logged on. The network fields indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impersonation level field indicates the extent to which a process in the logon session can impersonate. The authentication information fields provide detailed information about this specific logon request. - Logon GUID is a unique identifier that can be used to correlate this event with a KDC event. - Transited services indicate which intermediate services have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indicates the length of the generated session key. This will be 0 if no session key was requested.
Security	Audit Success	12544	2015-04-24 21:36:35	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: LTRANPHD$ Account Domain: WORKGROUP Logon ID: 0x3e7 Logon Type: 5 Impersonation Level: %%1833 New Logon: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Logon ID: 0x3e7 Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x22c Process Name: C:\Windows\System32\services.exe Network Information: Workstation Name: Source Network Address: - Source Port: - Detailed Authentication Information: Logon Process: Advapi Authentication Package: Negotiate Transited Services: - Package Name (NTLM only): - Key Length: 0 This event is generated when a logon session is created. It is generated on the computer that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service such as the Server service, or a local process such as Winlogon.exe or Services.exe. The logon type field indicates the kind of logon that occurred. The most common types are 2 (interactive) and 3 (network). The New Logon fields indicate the account for whom the new logon was created, i.e. the account that was logged on. The network fields indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impersonation level field indicates the extent to which a process in the logon session can impersonate. The authentication information fields provide detailed information about this specific logon request. - Logon GUID is a unique identifier that can be used to correlate this event with a KDC event. - Transited services indicate which intermediate services have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indicates the length of the generated session key. This will be 0 if no session key was requested.
Security	Audit Success	12544	2015-04-24 21:36:35	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-0-0 Account Name: - Account Domain: - Logon ID: 0x0 Logon Type: 3 Impersonation Level: %%1833 New Logon: Security ID: S-1-5-7 Account Name: ANONYMOUS LOGON Account Domain: NT AUTHORITY Logon ID: 0x1a8c1 Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x0 Process Name: - Network Information: Workstation Name: Source Network Address: - Source Port: - Detailed Authentication Information: Logon Process: NtLmSsp Authentication Package: NTLM Transited Services: - Package Name (NTLM only): NTLM V1 Key Length: 0 This event is generated when a logon session is created. It is generated on the computer that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service such as the Server service, or a local process such as Winlogon.exe or Services.exe. The logon type field indicates the kind of logon that occurred. The most common types are 2 (interactive) and 3 (network). The New Logon fields indicate the account for whom the new logon was created, i.e. the account that was logged on. The network fields indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impersonation level field indicates the extent to which a process in the logon session can impersonate. The authentication information fields provide detailed information about this specific logon request. - Logon GUID is a unique identifier that can be used to correlate this event with a KDC event. - Transited services indicate which intermediate services have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indicates the length of the generated session key. This will be 0 if no session key was requested.
Security	Audit Success	12548	2015-04-24 21:36:35	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Logon ID: 0x3e7 Privileges: SeAssignPrimaryTokenPrivilege SeTcbPrivilege SeSecurityPrivilege SeTakeOwnershipPrivilege SeLoadDriverPrivilege SeBackupPrivilege SeRestorePrivilege SeDebugPrivilege SeAuditPrivilege SeSystemEnvironmentPrivilege SeImpersonatePrivilege

Security	Audit Success	12548	2015-04-24 21:36:35	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Logon ID: 0x3e7 Privileges: SeAssignPrimaryTokenPrivilege SeTcbPrivilege SeSecurityPrivilege SeTakeOwnershipPrivilege SeLoadDriverPrivilege SeBackupPrivilege SeRestorePrivilege SeDebugPrivilege SeAuditPrivilege SeSystemEnvironmentPrivilege SeImpersonatePrivilege
Security	Audit Success	12544	2015-04-24 21:36:37	Microsoft-Windows-Security-Auditing	4648: A logon was attempted using explicit credentials. Subject: Security ID: S-1-5-18 Account Name: LTRANPHD$ Account Domain: WORKGROUP Logon ID: 0x3e7 Logon GUID: {00000000-0000-0000-0000-000000000000} Account Whose Credentials Were Used: Account Name: Liem Account Domain: LTRANPHD Logon GUID: {00000000-0000-0000-0000-000000000000} Target Server: Target Server Name: localhost Additional Information: localhost Process Information: Process ID: 0x1fc Process Name: C:\Windows\System32\winlogon.exe Network Information: Network Address: 127.0.0.1 Port: 0 This event is generated when a process attempts to log on an account by explicitly specifying that account's credentials. This most commonly occurs in batch-type configurations such as scheduled tasks, or when using the RUNAS command.
Security	Audit Success	12544	2015-04-24 21:36:37	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: LTRANPHD$ Account Domain: WORKGROUP Logon ID: 0x3e7 Logon Type: 2 Impersonation Level: %%1833 New Logon: Security ID: S-1-5-21-1888849264-3803429180-4108621888-1001 Account Name: Liem Account Domain: LTRANPHD Logon ID: 0x1c136 Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x1fc Process Name: C:\Windows\System32\winlogon.exe Network Information: Workstation Name: LTRANPHD Source Network Address: 127.0.0.1 Source Port: 0 Detailed Authentication Information: Logon Process: User32 Authentication Package: Negotiate Transited Services: - Package Name (NTLM only): - Key Length: 0 This event is generated when a logon session is created. It is generated on the computer that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service such as the Server service, or a local process such as Winlogon.exe or Services.exe. The logon type field indicates the kind of logon that occurred. The most common types are 2 (interactive) and 3 (network). The New Logon fields indicate the account for whom the new logon was created, i.e. the account that was logged on. The network fields indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impersonation level field indicates the extent to which a process in the logon session can impersonate. The authentication information fields provide detailed information about this specific logon request. - Logon GUID is a unique identifier that can be used to correlate this event with a KDC event. - Transited services indicate which intermediate services have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indicates the length of the generated session key. This will be 0 if no session key was requested.
Security	Audit Success	12544	2015-04-24 21:36:37	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: LTRANPHD$ Account Domain: WORKGROUP Logon ID: 0x3e7 Logon Type: 2 Impersonation Level: %%1833 New Logon: Security ID: S-1-5-21-1888849264-3803429180-4108621888-1001 Account Name: Liem Account Domain: LTRANPHD Logon ID: 0x1c169 Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x1fc Process Name: C:\Windows\System32\winlogon.exe Network Information: Workstation Name: LTRANPHD Source Network Address: 127.0.0.1 Source Port: 0 Detailed Authentication Information: Logon Process: User32 Authentication Package: Negotiate Transited Services: - Package Name (NTLM only): - Key Length: 0 This event is generated when a logon session is created. It is generated on the computer that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service such as the Server service, or a local process such as Winlogon.exe or Services.exe. The logon type field indicates the kind of logon that occurred. The most common types are 2 (interactive) and 3 (network). The New Logon fields indicate the account for whom the new logon was created, i.e. the account that was logged on. The network fields indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impersonation level field indicates the extent to which a process in the logon session can impersonate. The authentication information fields provide detailed information about this specific logon request. - Logon GUID is a unique identifier that can be used to correlate this event with a KDC event. - Transited services indicate which intermediate services have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indicates the length of the generated session key. This will be 0 if no session key was requested.
Security	Audit Success	12548	2015-04-24 21:36:37	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-21-1888849264-3803429180-4108621888-1001 Account Name: Liem Account Domain: LTRANPHD Logon ID: 0x1c136 Privileges: SeSecurityPrivilege SeTakeOwnershipPrivilege SeLoadDriverPrivilege SeBackupPrivilege SeRestorePrivilege SeDebugPrivilege SeSystemEnvironmentPrivilege SeImpersonatePrivilege
Security	Audit Success	12544	2015-04-24 21:36:38	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: LTRANPHD$ Account Domain: WORKGROUP Logon ID: 0x3e7 Logon Type: 5 Impersonation Level: %%1833 New Logon: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Logon ID: 0x3e7 Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x22c Process Name: C:\Windows\System32\services.exe Network Information: Workstation Name: Source Network Address: - Source Port: - Detailed Authentication Information: Logon Process: Advapi Authentication Package: Negotiate Transited Services: - Package Name (NTLM only): - Key Length: 0 This event is generated when a logon session is created. It is generated on the computer that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service such as the Server service, or a local process such as Winlogon.exe or Services.exe. The logon type field indicates the kind of logon that occurred. The most common types are 2 (interactive) and 3 (network). The New Logon fields indicate the account for

						whom the new logon was created, i.e. the account that was logged on. The network fields indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impersonation level field indicates the extent to which a process in the logon session can impersonate. The authentication information fields provide detailed information about this specific logon request. - Logon GUID is a unique identifier that can be used to correlate this event with a KDC event. - Transited services indicate which intermediate services have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indicates the length of the generated session key. This will be 0 if no session key was requested.
Security	Audit Success	12548	2015-04-24 21:36:38		Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Logon ID: 0x3e7 Privileges: SeAssignPrimaryTokenPrivilege SeTcbPrivilege SeSecurityPrivilege SeTakeOwnershipPrivilege SeLoadDriverPrivilege SeBackupPrivilege SeRestorePrivilege SeDebugPrivilege SeAuditPrivilege SeSystemEnvironmentPrivilege SeImpersonatePrivilege
Security	Audit Success	13824	2015-04-24 21:36:40		Microsoft-Windows-Security-Auditing	4797: An attempt was made to query the existence of a blank password for an account. Subject: Security ID: S-1-5-21-1888849264-3803429180-4108621888-1001 Account Name: Liem Account Domain: LTRANPHD Logon ID: 0x1c169 Additional Information: Caller Workstation: LTRANPHD Target Account Name: Administrator Target Account Domain: LTRANPHD
Security	Audit Success	13824	2015-04-24 21:36:40		Microsoft-Windows-Security-Auditing	4797: An attempt was made to query the existence of a blank password for an account. Subject: Security ID: S-1-5-21-1888849264-3803429180-4108621888-1001 Account Name: Liem Account Domain: LTRANPHD Logon ID: 0x1c169 Additional Information: Caller Workstation: LTRANPHD Target Account Name: Guest Target Account Domain: LTRANPHD
Security	Audit Success	13824	2015-04-24 21:36:40		Microsoft-Windows-Security-Auditing	4797: An attempt was made to query the existence of a blank password for an account. Subject: Security ID: S-1-5-21-1888849264-3803429180-4108621888-1001 Account Name: Liem Account Domain: LTRANPHD Logon ID: 0x1c169 Additional Information: Caller Workstation: LTRANPHD Target Account Name: Administrator Target Account Domain: LTRANPHD
Security	Audit Success	13824	2015-04-24 21:36:40		Microsoft-Windows-Security-Auditing	4797: An attempt was made to query the existence of a blank password for an account. Subject: Security ID: S-1-5-21-1888849264-3803429180-4108621888-1001 Account Name: Liem Account Domain: LTRANPHD Logon ID: 0x1c169 Additional Information: Caller Workstation: LTRANPHD Target Account Name: Guest Target Account Domain: LTRANPHD
Security	Audit Success	13824	2015-04-24 21:36:42		Microsoft-Windows-Security-Auditing	4797: An attempt was made to query the existence of a blank password for an account. Subject: Security ID: S-1-5-19 Account Name: LOCAL SERVICE Account Domain: NT AUTHORITY Logon ID: 0x3e5 Additional Information: Caller Workstation: LTRANPHD Target Account Name: Administrator Target Account Domain: LTRANPHD
Security	Audit Success	13824	2015-04-24 21:36:42		Microsoft-Windows-Security-Auditing	4797: An attempt was made to query the existence of a blank password for an account. Subject: Security ID: S-1-5-19 Account Name: LOCAL SERVICE Account Domain: NT AUTHORITY Logon ID: 0x3e5 Additional Information: Caller Workstation: LTRANPHD Target Account Name: Administrator Target Account Domain: LTRANPHD
Security	Audit Success	13824	2015-04-24 21:36:42		Microsoft-Windows-Security-Auditing	4797: An attempt was made to query the existence of a blank password for an account. Subject: Security ID: S-1-5-19 Account Name: LOCAL SERVICE Account Domain: NT AUTHORITY Logon ID: 0x3e5 Additional Information: Caller Workstation: LTRANPHD Target Account Name: Guest Target Account Domain: LTRANPHD
Security	Audit Success	13824	2015-04-24 21:36:42		Microsoft-Windows-Security-Auditing	4797: An attempt was made to query the existence of a blank password for an account. Subject: Security ID: S-1-5-19 Account Name: LOCAL SERVICE Account Domain: NT AUTHORITY Logon ID: 0x3e5 Additional Information: Caller Workstation: LTRANPHD Target Account Name: Guest Target Account Domain: LTRANPHD
Security	Audit Success	13824	2015-04-24 21:36:42		Microsoft-Windows-Security-Auditing	4797: An attempt was made to query the existence of a blank password for an account. Subject: Security ID: S-1-5-19 Account Name: LOCAL SERVICE Account Domain: NT AUTHORITY Logon ID: 0x3e5 Additional Information: Caller Workstation: LTRANPHD Target Account Name: Liem Target Account Domain: LTRANPHD
Security	Audit Success	13824	2015-04-24 21:36:42		Microsoft-Windows-Security-Auditing	4797: An attempt was made to query the existence of a blank password for an account. Subject: Security ID: S-1-5-19 Account Name: LOCAL SERVICE Account Domain: NT AUTHORITY Logon ID: 0x3e5 Additional Information: Caller Workstation: LTRANPHD Target Account Name: Liem Target Account Domain: LTRANPHD
Security	Audit Success	13824	2015-04-24 21:36:42		Microsoft-Windows-Security-Auditing	4797: An attempt was made to query the existence of a blank password for an account. Subject: Security ID: S-1-5-19 Account Name: LOCAL SERVICE Account Domain: NT AUTHORITY Logon ID: 0x3e5 Additional Information: Caller Workstation: LTRANPHD Target Account Name: Liem Target Account Domain: LTRANPHD
Security	Audit Success	13824	2015-04-24 21:36:42		Microsoft-Windows-Security-Auditing	4797: An attempt was made to query the existence of a blank password for an account. Subject: Security ID: S-1-5-19 Account Name: LOCAL SERVICE Account Domain: NT AUTHORITY Logon ID: 0x3e5 Additional Information: Caller Workstation: LTRANPHD Target Account Name: Liem Target Account Domain: LTRANPHD
Security	Audit Success	12288	2015-04-24 22:06:41		Microsoft-Windows-Security-Auditing	4608: Windows is starting up. This event is logged when LSASS.EXE starts and the auditing subsystem is initialized.
						4624: An account was successfully logged on. Subject: Security ID: S-1-0-0 Account Name: - Account Domain: - Logon ID: 0x0 Logon Type: 0 Impersonation Level: - New Logon: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Logon ID: 0x3e7 Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x4 Process Name: Network Information: Workstation Name: - Source Network Address: - Source Port: - Detailed Authentication Information: Logon Process: - Authentication Package: - Transited Services: - Package Name (NTLM only): - Key Length: 0 This event is generated when a logon session is created. It is generated on the computer that was accessed. The subject

Security	Audit Success	12544	2015-04-24 22:06:41	Microsoft-Windows-Security-Auditing	fields indicate the account on the local system which requested the logon. This is most commonly a service such as the Server service, or a local process such as Winlogon.exe or Services.exe. The logon type field indicates the kind of logon that occurred. The most common types are 2 (interactive) and 3 (network). The New Logon fields indicate the account for whom the new logon was created, i.e. the account that was logged on. The network fields indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impersonation level field indicates the extent to which a process in the logon session can impersonate. The authentication information fields provide detailed information about this specific logon request. - Logon GUID is a unique identifier that can be used to correlate this event with a KDC event. - Transited services indicate which intermediate services have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indicates the length of the generated session key. This will be 0 if no session key was requested.
Security	Audit Success	12544	2015-04-24 22:06:41	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: LTRANPHD$ Account Domain: WORKGROUP Logon ID: 0x3e7 Logon Type: 5 Impersonation Level: %%1833 New Logon: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Logon ID: 0x3e7 Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x228 Process Name: C:\Windows\System32\services.exe Network Information: Workstation Name: Source Network Address: - Source Port: - Detailed Authentication Information: Logon Process: Advapi Authentication Package: Negotiate Transited Services: - Package Name (NTLM only): - Key Length: 0 This event is generated when a logon session is created. It is generated on the computer that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service such as the Server service, or a local process such as Winlogon.exe or Services.exe. The logon type field indicates the kind of logon that occurred. The most common types are 2 (interactive) and 3 (network). The New Logon fields indicate the account for whom the new logon was created, i.e. the account that was logged on. The network fields indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impersonation level field indicates the extent to which a process in the logon session can impersonate. The authentication information fields provide detailed information about this specific logon request. - Logon GUID is a unique identifier that can be used to correlate this event with a KDC event. - Transited services indicate which intermediate services have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indicates the length of the generated session key. This will be 0 if no session key was requested.
Security	Audit Success	12544	2015-04-24 22:06:41	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: LTRANPHD$ Account Domain: WORKGROUP Logon ID: 0x3e7 Logon Type: 5 Impersonation Level: %%1833 New Logon: Security ID: S-1-5-20 Account Name: NETWORK SERVICE Account Domain: NT AUTHORITY Logon ID: 0x3e4 Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x228 Process Name: C:\Windows\System32\services.exe Network Information: Workstation Name: Source Network Address: - Source Port: - Detailed Authentication Information: Logon Process: Advapi Authentication Package: Negotiate Transited Services: - Package Name (NTLM only): - Key Length: 0 This event is generated when a logon session is created. It is generated on the computer that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service such as the Server service, or a local process such as Winlogon.exe or Services.exe. The logon type field indicates the kind of logon that occurred. The most common types are 2 (interactive) and 3 (network). The New Logon fields indicate the account for whom the new logon was created, i.e. the account that was logged on. The network fields indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impersonation level field indicates the extent to which a process in the logon session can impersonate. The authentication information fields provide detailed information about this specific logon request. - Logon GUID is a unique identifier that can be used to correlate this event with a KDC event. - Transited services indicate which intermediate services have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indicates the length of the generated session key. This will be 0 if no session key was requested.
Security	Audit Success	12544	2015-04-24 22:06:41	Microsoft-Windows-Security-Auditing	4648: A logon was attempted using explicit credentials. Subject: Security ID: S-1-5-18 Account Name: LTRANPHD$ Account Domain: WORKGROUP Logon ID: 0x3e7 Logon GUID: {00000000-0000-0000-0000-000000000000} Account Whose Credentials Were Used: Account Name: DWM-1 Account Domain: Window Manager Logon GUID: {00000000-0000-0000-0000-000000000000} Target Server: Target Server Name: localhost Additional Information: localhost Process Information: Process ID: 0x200 Process Name: C:\Windows\System32\winlogon.exe Network Information: Network Address: - Port: - This event is generated when a process attempts to log on an account by explicitly specifying that account's credentials. This most commonly occurs in batch-type configurations such as scheduled tasks, or when using the RUNAS command.
Security	Audit	12544	2015-04-24	Microsoft-Windows-Security-	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: LTRANPHD$ Account Domain: WORKGROUP Logon ID: 0x3e7 Logon Type: 2 Impersonation Level: %%1833 New Logon: Security ID: S-1-5-90-1 Account Name: DWM-1 Account Domain: Window Manager Logon ID: 0xdb5b Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x200 Process Name: C:\Windows\System32\winlogon.exe Network Information: Workstation Name: Source Network Address: - Source Port: - Detailed Authentication Information: Logon Process: Advapi Authentication Package: Negotiate Transited Services: - Package Name (NTLM only): - Key Length: 0 This event is generated when a logon session is created. It is generated on the computer that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service such as the Server service, or a local process such as Winlogon.exe or Services.exe. The logon type field indicates the kind of logon that occurred.

	Success		22:06:41	Auditing	The most common types are 2 (interactive) and 3 (network). The New Logon fields indicate the account for whom the new logon was created, i.e. the account that was logged on. The network fields indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impersonation level field indicates the extent to which a process in the logon session can impersonate. The authentication information fields provide detailed information about this specific logon request. - Logon GUID is a unique identifier that can be used to correlate this event with a KDC event. - Transited services indicate which intermediate services have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indicates the length of the generated session key. This will be 0 if no session key was requested.
Security	Audit Success	12544	2015-04-24 22:06:41	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: LTRANPHD$ Account Domain: WORKGROUP Logon ID: 0x3e7 Logon Type: 2 Impersonation Level: %%1833 New Logon: Security ID: S-1-5-90-1 Account Name: DWM-1 Account Domain: Window Manager Logon ID: 0xdb79 Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x200 Process Name: C:\Windows\System32\winlogon.exe Network Information: Workstation Name: Source Network Address: - Source Port: - Detailed Authentication Information: Logon Process: Advapi Authentication Package: Negotiate Transited Services: - Package Name (NTLM only): - Key Length: 0 This event is generated when a logon session is created. It is generated on the computer that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service such as the Server service, or a local process such as Winlogon.exe or Services.exe. The logon type field indicates the kind of logon that occurred. The most common types are 2 (interactive) and 3 (network). The New Logon fields indicate the account for whom the new logon was created, i.e. the account that was logged on. The network fields indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impersonation level field indicates the extent to which a process in the logon session can impersonate. The authentication information fields provide detailed information about this specific logon request. - Logon GUID is a unique identifier that can be used to correlate this event with a KDC event. - Transited services indicate which intermediate services have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indicates the length of the generated session key. This will be 0 if no session key was requested.
Security	Audit Success	12544	2015-04-24 22:06:41	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: LTRANPHD$ Account Domain: WORKGROUP Logon ID: 0x3e7 Logon Type: 5 Impersonation Level: %%1833 New Logon: Security ID: S-1-5-19 Account Name: LOCAL SERVICE Account Domain: NT AUTHORITY Logon ID: 0x3e5 Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x228 Process Name: C:\Windows\System32\services.exe Network Information: Workstation Name: Source Network Address: - Source Port: - Detailed Authentication Information: Logon Process: Advapi Authentication Package: Negotiate Transited Services: - Package Name (NTLM only): - Key Length: 0 This event is generated when a logon session is created. It is generated on the computer that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service such as the Server service, or a local process such as Winlogon.exe or Services.exe. The logon type field indicates the kind of logon that occurred. The most common types are 2 (interactive) and 3 (network). The New Logon fields indicate the account for whom the new logon was created, i.e. the account that was logged on. The network fields indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impersonation level field indicates the extent to which a process in the logon session can impersonate. The authentication information fields provide detailed information about this specific logon request. - Logon GUID is a unique identifier that can be used to correlate this event with a KDC event. - Transited services indicate which intermediate services have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indicates the length of the generated session key. This will be 0 if no session key was requested.
Security	Audit Success	12544	2015-04-24 22:06:41	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: LTRANPHD$ Account Domain: WORKGROUP Logon ID: 0x3e7 Logon Type: 5 Impersonation Level: %%1833 New Logon: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Logon ID: 0x3e7 Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x228 Process Name: C:\Windows\System32\services.exe Network Information: Workstation Name: Source Network Address: - Source Port: - Detailed Authentication Information: Logon Process: Advapi Authentication Package: Negotiate Transited Services: - Package Name (NTLM only): - Key Length: 0 This event is generated when a logon session is created. It is generated on the computer that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service such as the Server service, or a local process such as Winlogon.exe or Services.exe. The logon type field indicates the kind of logon that occurred. The most common types are 2 (interactive) and 3 (network). The New Logon fields indicate the account for whom the new logon was created, i.e. the account that was logged on. The network fields indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impersonation level field indicates the extent to which a process in the logon session can impersonate. The authentication information fields provide detailed information about this specific logon request. - Logon GUID is a unique identifier that can be used to correlate this event with a KDC event. - Transited services indicate which intermediate services have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indicates the length of the generated session key. This will be 0 if no session key was requested.

Security	Audit Success	12544	2015-04-24 22:06:41	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: LTRANPHD$ Account Domain: WORKGROUP Logon ID: 0x3e7 Logon Type: 5 Impersonation Level: %%1833 New Logon: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Logon ID: 0x3e7 Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x228 Process Name: C:\Windows\System32\services.exe Network Information: Workstation Name: Source Network Address: - Source Port: - Detailed Authentication Information: Logon Process: Advapi Authentication Package: Negotiate Transited Services: - Package Name (NTLM only): - Key Length: 0 This event is generated when a logon session is created. It is generated on the computer that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service such as the Server service, or a local process such as Winlogon.exe or Services.exe. The logon type field indicates the kind of logon that occurred. The most common types are 2 (interactive) and 3 (network). The New Logon fields indicate the account for whom the new logon was created, i.e. the account that was logged on. The network fields indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impersonation level field indicates the extent to which a process in the logon session can impersonate. The authentication information fields provide detailed information about this specific logon request. - Logon GUID is a unique identifier that can be used to correlate this event with a KDC event. - Transited services indicate which intermediate services have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indicates the length of the generated session key. This will be 0 if no session key was requested.
Security	Audit Success	12548	2015-04-24 22:06:41	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Logon ID: 0x3e7 Privileges: SeAssignPrimaryTokenPrivilege SeTcbPrivilege SeSecurityPrivilege SeTakeOwnershipPrivilege SeLoadDriverPrivilege SeBackupPrivilege SeRestorePrivilege SeDebugPrivilege SeAuditPrivilege SeSystemEnvironmentPrivilege SeImpersonatePrivilege
Security	Audit Success	12548	2015-04-24 22:06:41	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-20 Account Name: NETWORK SERVICE Account Domain: NT AUTHORITY Logon ID: 0x3e4 Privileges: SeAssignPrimaryTokenPrivilege SeAuditPrivilege SeImpersonatePrivilege
Security	Audit Success	12548	2015-04-24 22:06:41	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-90-1 Account Name: DWM-1 Account Domain: Window Manager Logon ID: 0xdb5b Privileges: SeAssignPrimaryTokenPrivilege SeAuditPrivilege SeImpersonatePrivilege
Security	Audit Success	12548	2015-04-24 22:06:41	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-90-1 Account Name: DWM-1 Account Domain: Window Manager Logon ID: 0xdb79 Privileges: SeAssignPrimaryTokenPrivilege SeAuditPrivilege
Security	Audit Success	12548	2015-04-24 22:06:41	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-19 Account Name: LOCAL SERVICE Account Domain: NT AUTHORITY Logon ID: 0x3e5 Privileges: SeAssignPrimaryTokenPrivilege SeAuditPrivilege SeImpersonatePrivilege
Security	Audit Success	12548	2015-04-24 22:06:41	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Logon ID: 0x3e7 Privileges: SeAssignPrimaryTokenPrivilege SeTcbPrivilege SeSecurityPrivilege SeTakeOwnershipPrivilege SeLoadDriverPrivilege SeBackupPrivilege SeRestorePrivilege SeDebugPrivilege SeAuditPrivilege SeSystemEnvironmentPrivilege SeImpersonatePrivilege
Security	Audit Success	12548	2015-04-24 22:06:41	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Logon ID: 0x3e7 Privileges: SeAssignPrimaryTokenPrivilege SeTcbPrivilege SeSecurityPrivilege SeTakeOwnershipPrivilege SeLoadDriverPrivilege SeBackupPrivilege SeRestorePrivilege SeDebugPrivilege SeAuditPrivilege SeSystemEnvironmentPrivilege SeImpersonatePrivilege
Security	Audit Success	13568	2015-04-24 22:06:41	Microsoft-Windows-Security-Auditing	4902: The Per-user audit policy table was created. Number of Elements: 0 Policy ID: 0x8af1
Security	Audit Success	12292	2015-04-24 22:06:42	Microsoft-Windows-Security-Auditing	5033: The Windows Firewall Driver started successfully.
Security	Audit Success	12292	2015-04-24 22:06:42	Microsoft-Windows-Security-Auditing	5024: The Windows Firewall service started successfully.
Security	Audit Success	12544	2015-04-24 22:06:42	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: LTRANPHD$ Account Domain: WORKGROUP Logon ID: 0x3e7 Logon Type: 5 Impersonation Level: %%1833 New Logon: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Logon ID: 0x3e7 Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x228 Process Name: C:\Windows\System32\services.exe Network Information: Workstation Name: Source Network Address: - Source Port: - Detailed Authentication Information: Logon Process: Advapi Authentication Package: Negotiate Transited Services: - Package Name (NTLM only): - Key Length: 0 This event is generated when a logon session is created. It is generated on the computer that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service such as the Server service, or a local process such as Winlogon.exe or Services.exe. The logon type field indicates the kind of logon that occurred. The most common types are 2 (interactive) and 3 (network). The New Logon fields indicate the account for whom the new logon was created, i.e. the account that was logged on. The network fields indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some

						cases. The impersonation level field indicates the extent to which a process in the logon session can impersonate. The authentication information fields provide detailed information about this specific logon request. - Logon GUID is a unique identifier that can be used to correlate this event with a KDC event. - Transited services indicate which intermediate services have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indicates the length of the generated session key. This will be 0 if no session key was requested.
Security	Audit Success	12544	2015-04-24 22:06:42		Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: LTRANPHD$ Account Domain: WORKGROUP Logon ID: 0x3e7 Logon Type: 5 Impersonation Level: %%1833 New Logon: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Logon ID: 0x3e7 Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x228 Process Name: C:\Windows\System32\services.exe Network Information: Workstation Name: Source Network Address: - Source Port: - Detailed Authentication Information: Logon Process: Advapi Authentication Package: Negotiate Transited Services: - Package Name (NTLM only): - Key Length: 0 This event is generated when a logon session is created. It is generated on the computer that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service such as the Server service, or a local process such as Winlogon.exe or Services.exe. The logon type field indicates the kind of logon that occurred. The most common types are 2 (interactive) and 3 (network). The New Logon fields indicate the account for whom the new logon was created, i.e. the account that was logged on. The network fields indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impersonation level field indicates the extent to which a process in the logon session can impersonate. The authentication information fields provide detailed information about this specific logon request. - Logon GUID is a unique identifier that can be used to correlate this event with a KDC event. - Transited services indicate which intermediate services have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indicates the length of the generated session key. This will be 0 if no session key was requested.
Security	Audit Success	12544	2015-04-24 22:06:42		Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: LTRANPHD$ Account Domain: WORKGROUP Logon ID: 0x3e7 Logon Type: 5 Impersonation Level: %%1833 New Logon: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Logon ID: 0x3e7 Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x228 Process Name: C:\Windows\System32\services.exe Network Information: Workstation Name: Source Network Address: - Source Port: - Detailed Authentication Information: Logon Process: Advapi Authentication Package: Negotiate Transited Services: - Package Name (NTLM only): - Key Length: 0 This event is generated when a logon session is created. It is generated on the computer that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service such as the Server service, or a local process such as Winlogon.exe or Services.exe. The logon type field indicates the kind of logon that occurred. The most common types are 2 (interactive) and 3 (network). The New Logon fields indicate the account for whom the new logon was created, i.e. the account that was logged on. The network fields indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impersonation level field indicates the extent to which a process in the logon session can impersonate. The authentication information fields provide detailed information about this specific logon request. - Logon GUID is a unique identifier that can be used to correlate this event with a KDC event. - Transited services indicate which intermediate services have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indicates the length of the generated session key. This will be 0 if no session key was requested.
Security	Audit Success	12548	2015-04-24 22:06:42		Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Logon ID: 0x3e7 Privileges: SeAssignPrimaryTokenPrivilege SeTcbPrivilege SeSecurityPrivilege SeTakeOwnershipPrivilege SeLoadDriverPrivilege SeBackupPrivilege SeRestorePrivilege SeDebugPrivilege SeAuditPrivilege SeSystemEnvironmentPrivilege SeImpersonatePrivilege
Security	Audit Success	12548	2015-04-24 22:06:42		Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Logon ID: 0x3e7 Privileges: SeAssignPrimaryTokenPrivilege SeTcbPrivilege SeSecurityPrivilege SeTakeOwnershipPrivilege SeLoadDriverPrivilege SeBackupPrivilege SeRestorePrivilege SeDebugPrivilege SeAuditPrivilege SeSystemEnvironmentPrivilege SeImpersonatePrivilege
Security	Audit Success	12548	2015-04-24 22:06:42		Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Logon ID: 0x3e7 Privileges: SeAssignPrimaryTokenPrivilege SeTcbPrivilege SeSecurityPrivilege SeTakeOwnershipPrivilege SeLoadDriverPrivilege SeBackupPrivilege SeRestorePrivilege SeDebugPrivilege SeAuditPrivilege SeSystemEnvironmentPrivilege SeImpersonatePrivilege
Security	Audit Success	12544	2015-04-24 22:06:43		Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-0-0 Account Name: - Account Domain: - Logon ID: 0x0 Logon Type: 3 Impersonation Level: %%1833 New Logon: Security ID: S-1-5-7 Account Name: ANONYMOUS LOGON Account Domain: NT AUTHORITY Logon ID: 0x198f5 Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x0 Process Name: - Network Information: Workstation Name: Source Network Address: - Source Port: - Detailed Authentication Information: Logon Process: NtLmSsp Authentication Package: NTLM Transited Services: - Package Name (NTLM only): NTLM V1 Key Length: 0 This event is generated when a logon session is created. It is generated on the computer that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service such as the Server service, or a local process such as Winlogon.exe or Services.exe. The logon type field indicates the kind of logon that occurred. The most common types are 2 (interactive) and 3

					(network). The New Logon fields indicate the account for whom the new logon was created, i.e. the account that was logged on. The network fields indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impersonation level field indicates the extent to which a process in the logon session can impersonate. The authentication information fields provide detailed information about this specific logon request. - Logon GUID is a unique identifier that can be used to correlate this event with a KDC event. - Transited services indicate which intermediate services have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indicates the length of the generated session key. This will be 0 if no session key was requested.
Security	Audit Success	12544	2015-04-24 22:06:45	Microsoft-Windows-Security-Auditing	4648: A logon was attempted using explicit credentials. Subject: Security ID: S-1-5-18 Account Name: LTRANPHD$ Account Domain: WORKGROUP Logon ID: 0x3e7 Logon GUID: {00000000-0000-0000-0000-000000000000} Account Whose Credentials Were Used: Account Name: Liem Account Domain: LTRANPHD Logon GUID: {00000000-0000-0000-0000-000000000000} Target Server: Target Server Name: localhost Additional Information: localhost Process Information: Process ID: 0x200 Process Name: C:\Windows\System32\winlogon.exe Network Information: Network Address: 127.0.0.1 Port: 0 This event is generated when a process attempts to log on an account by explicitly specifying that account's credentials. This most commonly occurs in batch-type configurations such as scheduled tasks, or when using the RUNAS command.
Security	Audit Success	12544	2015-04-24 22:06:45	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: LTRANPHD$ Account Domain: WORKGROUP Logon ID: 0x3e7 Logon Type: 2 Impersonation Level: %%1833 New Logon: Security ID: S-1-5-21-1888849264-3803429180-4108621888-1001 Account Name: Liem Account Domain: LTRANPHD Logon ID: 0x1bde7 Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x200 Process Name: C:\Windows\System32\winlogon.exe Network Information: Workstation Name: LTRANPHD Source Network Address: 127.0.0.1 Source Port: 0 Detailed Authentication Information: Logon Process: User32 Authentication Package: Negotiate Transited Services: - Package Name (NTLM only): - Key Length: 0 This event is generated when a logon session is created. It is generated on the computer that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service such as the Server service, or a local process such as Winlogon.exe or Services.exe. The logon type field indicates the kind of logon that occurred. The most common types are 2 (interactive) and 3 (network). The New Logon fields indicate the account for whom the new logon was created, i.e. the account that was logged on. The network fields indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impersonation level field indicates the extent to which a process in the logon session can impersonate. The authentication information fields provide detailed information about this specific logon request. - Logon GUID is a unique identifier that can be used to correlate this event with a KDC event. - Transited services indicate which intermediate services have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indicates the length of the generated session key. This will be 0 if no session key was requested.
Security	Audit Success	12544	2015-04-24 22:06:45	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: LTRANPHD$ Account Domain: WORKGROUP Logon ID: 0x3e7 Logon Type: 2 Impersonation Level: %%1833 New Logon: Security ID: S-1-5-21-1888849264-3803429180-4108621888-1001 Account Name: Liem Account Domain: LTRANPHD Logon ID: 0x1be1a Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x200 Process Name: C:\Windows\System32\winlogon.exe Network Information: Workstation Name: LTRANPHD Source Network Address: 127.0.0.1 Source Port: 0 Detailed Authentication Information: Logon Process: User32 Authentication Package: Negotiate Transited Services: - Package Name (NTLM only): - Key Length: 0 This event is generated when a logon session is created. It is generated on the computer that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service such as the Server service, or a local process such as Winlogon.exe or Services.exe. The logon type field indicates the kind of logon that occurred. The most common types are 2 (interactive) and 3 (network). The New Logon fields indicate the account for whom the new logon was created, i.e. the account that was logged on. The network fields indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impersonation level field indicates the extent to which a process in the logon session can impersonate. The authentication information fields provide detailed information about this specific logon request. - Logon GUID is a unique identifier that can be used to correlate this event with a KDC event. - Transited services indicate which intermediate services have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indicates the length of the generated session key. This will be 0 if no session key was requested.
Security	Audit Success	12548	2015-04-24 22:06:45	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-21-1888849264-3803429180-4108621888-1001 Account Name: Liem Account Domain: LTRANPHD Logon ID: 0x1bde7 Privileges: SeSecurityPrivilege SeTakeOwnershipPrivilege SeLoadDriverPrivilege SeBackupPrivilege SeRestorePrivilege SeDebugPrivilege SeSystemEnvironmentPrivilege SeImpersonatePrivilege
					4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: LTRANPHD$ Account Domain: WORKGROUP Logon ID: 0x3e7 Logon Type: 5 Impersonation Level: %%1833 New Logon: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Logon ID: 0x3e7 Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x228 Process Name: C:\Windows\System32\services.exe Network Information: Workstation Name: Source Network Address: - Source Port: - Detailed Authentication Information: Logon Process: Advapi Authentication Package: Negotiate Transited Services: - Package Name (NTLM only): - Key Length: 0 This event is generated when a logon session is

Security	Audit Success	12544	2015-04-24 22:06:46	Microsoft-Windows-Security-Auditing	created. It is generated on the computer that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service such as the Server service, or a local process such as Winlogon.exe or Services.exe. The logon type field indicates the kind of logon that occurred. The most common types are 2 (interactive) and 3 (network). The New Logon fields indicate the account for whom the new logon was created, i.e. the account that was logged on. The network fields indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impersonation level field indicates the extent to which a process in the logon session can impersonate. The authentication information fields provide detailed information about this specific logon request. - Logon GUID is a unique identifier that can be used to correlate this event with a KDC event. - Transited services indicate which intermediate services have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indicates the length of the generated session key. This will be 0 if no session key was requested.
Security	Audit Success	12548	2015-04-24 22:06:46	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Logon ID: 0x3e7 Privileges: SeAssignPrimaryTokenPrivilege SeTcbPrivilege SeSecurityPrivilege SeTakeOwnershipPrivilege SeLoadDriverPrivilege SeBackupPrivilege SeRestorePrivilege SeDebugPrivilege SeAuditPrivilege SeSystemEnvironmentPrivilege SeImpersonatePrivilege
Security	Audit Success	13824	2015-04-24 22:06:47	Microsoft-Windows-Security-Auditing	4797: An attempt was made to query the existence of a blank password for an account. Subject: Security ID: S-1-5-19 Account Name: LOCAL SERVICE Account Domain: NT AUTHORITY Logon ID: 0x3e5 Additional Information: Caller Workstation: LTRANPHD Target Account Name: Administrator Target Account Domain: LTRANPHD
Security	Audit Success	13824	2015-04-24 22:06:47	Microsoft-Windows-Security-Auditing	4797: An attempt was made to query the existence of a blank password for an account. Subject: Security ID: S-1-5-19 Account Name: LOCAL SERVICE Account Domain: NT AUTHORITY Logon ID: 0x3e5 Additional Information: Caller Workstation: LTRANPHD Target Account Name: Guest Target Account Domain: LTRANPHD
Security	Audit Success	13824	2015-04-24 22:06:47	Microsoft-Windows-Security-Auditing	4797: An attempt was made to query the existence of a blank password for an account. Subject: Security ID: S-1-5-19 Account Name: LOCAL SERVICE Account Domain: NT AUTHORITY Logon ID: 0x3e5 Additional Information: Caller Workstation: LTRANPHD Target Account Name: Liem Target Account Domain: LTRANPHD
Security	Audit Success	13824	2015-04-24 22:06:47	Microsoft-Windows-Security-Auditing	4797: An attempt was made to query the existence of a blank password for an account. Subject: Security ID: S-1-5-19 Account Name: LOCAL SERVICE Account Domain: NT AUTHORITY Logon ID: 0x3e5 Additional Information: Caller Workstation: LTRANPHD Target Account Name: Liem Target Account Domain: LTRANPHD
Security	Audit Success	13824	2015-04-24 22:06:47	Microsoft-Windows-Security-Auditing	4797: An attempt was made to query the existence of a blank password for an account. Subject: Security ID: S-1-5-19 Account Name: LOCAL SERVICE Account Domain: NT AUTHORITY Logon ID: 0x3e5 Additional Information: Caller Workstation: LTRANPHD Target Account Name: Administrator Target Account Domain: LTRANPHD
Security	Audit Success	13824	2015-04-24 22:06:47	Microsoft-Windows-Security-Auditing	4797: An attempt was made to query the existence of a blank password for an account. Subject: Security ID: S-1-5-19 Account Name: LOCAL SERVICE Account Domain: NT AUTHORITY Logon ID: 0x3e5 Additional Information: Caller Workstation: LTRANPHD Target Account Name: Guest Target Account Domain: LTRANPHD
Security	Audit Success	13824	2015-04-24 22:06:47	Microsoft-Windows-Security-Auditing	4797: An attempt was made to query the existence of a blank password for an account. Subject: Security ID: S-1-5-19 Account Name: LOCAL SERVICE Account Domain: NT AUTHORITY Logon ID: 0x3e5 Additional Information: Caller Workstation: LTRANPHD Target Account Name: Liem Target Account Domain: LTRANPHD
Security	Audit Success	13824	2015-04-24 22:06:47	Microsoft-Windows-Security-Auditing	4797: An attempt was made to query the existence of a blank password for an account. Subject: Security ID: S-1-5-19 Account Name: LOCAL SERVICE Account Domain: NT AUTHORITY Logon ID: 0x3e5 Additional Information: Caller Workstation: LTRANPHD Target Account Name: Administrator Target Account Domain: LTRANPHD
Security	Audit Success	13824	2015-04-24 22:06:47	Microsoft-Windows-Security-Auditing	4797: An attempt was made to query the existence of a blank password for an account. Subject: Security ID: S-1-5-19 Account Name: LOCAL SERVICE Account Domain: NT AUTHORITY Logon ID: 0x3e5 Additional Information: Caller Workstation: LTRANPHD Target Account Name: Liem Target Account Domain: LTRANPHD
Security	Audit Success	13824	2015-04-24 22:06:47	Microsoft-Windows-Security-Auditing	4797: An attempt was made to query the existence of a blank password for an account. Subject: Security ID: S-1-5-19 Account Name: LOCAL SERVICE Account Domain: NT AUTHORITY Logon ID: 0x3e5 Additional Information: Caller Workstation: LTRANPHD Target Account Name: Administrator Target Account Domain: LTRANPHD
Security	Audit Success	13824	2015-04-24 22:06:47	Microsoft-Windows-Security-Auditing	4797: An attempt was made to query the existence of a blank password for an account. Subject: Security ID: S-1-5-19 Account Name: LOCAL SERVICE Account Domain: NT AUTHORITY Logon ID: 0x3e5 Additional Information: Caller Workstation: LTRANPHD Target Account Name: Guest Target Account Domain: LTRANPHD
Security	Audit Success	13824	2015-04-24 22:06:47	Microsoft-Windows-Security-Auditing	4797: An attempt was made to query the existence of a blank password for an account. Subject: Security ID: S-1-5-19 Account Name: LOCAL SERVICE Account Domain: NT AUTHORITY Logon ID: 0x3e5 Additional Information: Caller Workstation: LTRANPHD Target Account Name: Liem Target Account Domain: LTRANPHD
Security	Audit Success	13824	2015-04-24 22:06:47	Microsoft-Windows-Security-Auditing	4797: An attempt was made to query the existence of a blank password for an account. Subject: Security ID: S-1-5-19 Account Name: LOCAL SERVICE Account Domain: NT AUTHORITY Logon ID: 0x3e5 Additional Information: Caller Workstation: LTRANPHD Target Account Name: Administrator Target Account Domain: LTRANPHD
Security	Audit Success	13824	2015-04-24 22:06:47	Microsoft-Windows-Security-Auditing	4797: An attempt was made to query the existence of a blank password for an account. Subject: Security ID: S-1-5-19 Account Name: LOCAL SERVICE Account Domain: NT AUTHORITY Logon ID: 0x3e5 Additional Information: Caller Workstation: LTRANPHD Target Account Name: Guest Target Account Domain: LTRANPHD
Security	Audit Success	13824	2015-04-24 22:06:47	Microsoft-Windows-Security-Auditing	4797: An attempt was made to query the existence of a blank password for an account. Subject: Security ID: S-1-5-19 Account Name: LOCAL SERVICE Account Domain: NT AUTHORITY Logon ID: 0x3e5 Additional Information: Caller Workstation: LTRANPHD Target Account Name: Liem Target Account Domain: LTRANPHD
Security	Audit Success	13824	2015-04-24 22:06:47	Microsoft-Windows-Security-Auditing	4797: An attempt was made to query the existence of a blank password for an account. Subject: Security ID: S-1-5-19 Account Name: LOCAL SERVICE Account Domain: NT AUTHORITY Logon ID: 0x3e5 Additional Information: Caller Workstation: LTRANPHD Target Account Name: Administrator Target Account Domain: LTRANPHD
Security	Audit Success	13824	2015-04-	Microsoft-Windows-Security-	4797: An attempt was made to query the existence of a blank password for an account. Subject: Security ID:

Security	Audit Success	13824	24 22:06:47	Microsoft-Windows-Security-Auditing	S-1-5-19 Account Name: LOCAL SERVICE Account Domain: NT AUTHORITY Logon ID: 0x3e5 Additional Information: Caller Workstation: LTRANPHD Target Account Name: Guest Target Account Domain: LTRANPHD
Security	Audit Success	13824	2015-04-24 22:06:47	Microsoft-Windows-Security-Auditing	4797: An attempt was made to query the existence of a blank password for an account. Subject: Security ID: S-1-5-19 Account Name: LOCAL SERVICE Account Domain: NT AUTHORITY Logon ID: 0x3e5 Additional Information: Caller Workstation: LTRANPHD Target Account Name: Liem Target Account Domain: LTRANPHD
Security	Audit Success	13824	2015-04-24 22:06:47	Microsoft-Windows-Security-Auditing	4797: An attempt was made to query the existence of a blank password for an account. Subject: Security ID: S-1-5-19 Account Name: LOCAL SERVICE Account Domain: NT AUTHORITY Logon ID: 0x3e5 Additional Information: Caller Workstation: LTRANPHD Target Account Name: Liem Target Account Domain: LTRANPHD
Security	Audit Success	13824	2015-04-24 22:06:48	Microsoft-Windows-Security-Auditing	4797: An attempt was made to query the existence of a blank password for an account. Subject: Security ID: S-1-5-21-1888849264-3803429180-4108621888-1001 Account Name: Liem Account Domain: LTRANPHD Logon ID: 0x1be1a Additional Information: Caller Workstation: LTRANPHD Target Account Name: Administrator Target Account Domain: LTRANPHD
Security	Audit Success	13824	2015-04-24 22:06:48	Microsoft-Windows-Security-Auditing	4797: An attempt was made to query the existence of a blank password for an account. Subject: Security ID: S-1-5-21-1888849264-3803429180-4108621888-1001 Account Name: Liem Account Domain: LTRANPHD Logon ID: 0x1be1a Additional Information: Caller Workstation: LTRANPHD Target Account Name: Guest Target Account Domain: LTRANPHD
Security	Audit Success	13824	2015-04-24 22:06:48	Microsoft-Windows-Security-Auditing	4797: An attempt was made to query the existence of a blank password for an account. Subject: Security ID: S-1-5-21-1888849264-3803429180-4108621888-1001 Account Name: Liem Account Domain: LTRANPHD Logon ID: 0x1be1a Additional Information: Caller Workstation: LTRANPHD Target Account Name: Administrator Target Account Domain: LTRANPHD
Security	Audit Success	13824	2015-04-24 22:06:48	Microsoft-Windows-Security-Auditing	4797: An attempt was made to query the existence of a blank password for an account. Subject: Security ID: S-1-5-21-1888849264-3803429180-4108621888-1001 Account Name: Liem Account Domain: LTRANPHD Logon ID: 0x1be1a Additional Information: Caller Workstation: LTRANPHD Target Account Name: Guest Target Account Domain: LTRANPHD
Security	Audit Success	103	2015-04-24 22:16:42	Microsoft-Windows-Eventlog	1100: The event logging service has shut down.
Security	Audit Success	12545	2015-04-24 22:16:42	Microsoft-Windows-Security-Auditing	4647: User initiated logoff: Subject: Security ID: S-1-5-21-1888849264-3803429180-4108621888-1001 Account Name: Liem Account Domain: LTRANPHD Logon ID: 0x1be1a This event is generated when a logoff is initiated. No further user-initiated activity can occur. This event can be interpreted as a logoff event.
Security	Audit Success	12288	2015-04-24 22:16:54	Microsoft-Windows-Security-Auditing	4608: Windows is starting up. This event is logged when LSASS.EXE starts and the auditing subsystem is initialized.
Security	Audit Success	12292	2015-04-24 22:16:54	Microsoft-Windows-Security-Auditing	5033: The Windows Firewall Driver started successfully.
Security	Audit Success	12544	2015-04-24 22:16:54	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-0-0 Account Name: - Account Domain: - Logon ID: 0x0 Logon Type: 0 Impersonation Level: - New Logon: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Logon ID: 0x3e7 Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x4 Process Name: Network Information: Workstation Name: - Source Network Address: - Source Port: - Detailed Authentication Information: Logon Process: - Authentication Package: - Transited Services: - Package Name (NTLM only): - Key Length: 0 This event is generated when a logon session is created. It is generated on the computer that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service such as the Server service, or a local process such as Winlogon.exe or Services.exe. The logon type field indicates the kind of logon that occurred. The most common types are 2 (interactive) and 3 (network). The New Logon fields indicate the account for whom the new logon was created, i.e. the account that was logged on. The network fields indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impersonation level field indicates the extent to which a process in the logon session can impersonate. The authentication information fields provide detailed information about this specific logon request. - Logon GUID is a unique identifier that can be used to correlate this event with a KDC event. - Transited services indicate which intermediate services have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indicates the length of the generated session key. This will be 0 if no session key was requested.
Security	Audit Success	12544	2015-04-24	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: LTRANPHD$ Account Domain: WORKGROUP Logon ID: 0x3e7 Logon Type: 5 Impersonation Level: %%1833 New Logon: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Logon ID: 0x3e7 Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x230 Process Name: C:\Windows\System32\services.exe Network Information: Workstation Name: Source Network Address: - Source Port: - Detailed Authentication Information: Logon Process: Advapi Authentication Package: Negotiate Transited Services: - Package Name (NTLM only): - Key Length: 0 This event is generated when a logon session is created. It is generated on the computer that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service such as the Server service, or a local process such as Winlogon.exe or Services.exe. The logon type field indicates the kind of logon that occurred.

			22:16:54		The most common types are 2 (interactive) and 3 (network). The New Logon fields indicate the account for whom the new logon was created, i.e. the account that was logged on. The network fields indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impersonation level field indicates the extent to which a process in the logon session can impersonate. The authentication information fields provide detailed information about this specific logon request. - Logon GUID is a unique identifier that can be used to correlate this event with a KDC event. - Transited services indicate which intermediate services have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indicates the length of the generated session key. This will be 0 if no session key was requested.
Security	Audit Success	12544	2015-04-24 22:16:54	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: LTRANPHD$ Account Domain: WORKGROUP Logon ID: 0x3e7 Logon Type: 5 Impersonation Level: %%1833 New Logon: Security ID: S-1-5-20 Account Name: NETWORK SERVICE Account Domain: NT AUTHORITY Logon ID: 0x3e4 Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x230 Process Name: C:\Windows\System32\services.exe Network Information: Workstation Name: Source Network Address: - Source Port: - Detailed Authentication Information: Logon Process: Advapi Authentication Package: Negotiate Transited Services: - Package Name (NTLM only): - Key Length: 0 This event is generated when a logon session is created. It is generated on the computer that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service such as the Server service, or a local process such as Winlogon.exe or Services.exe. The logon type field indicates the kind of logon that occurred. The most common types are 2 (interactive) and 3 (network). The New Logon fields indicate the account for whom the new logon was created, i.e. the account that was logged on. The network fields indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impersonation level field indicates the extent to which a process in the logon session can impersonate. The authentication information fields provide detailed information about this specific logon request. - Logon GUID is a unique identifier that can be used to correlate this event with a KDC event. - Transited services indicate which intermediate services have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indicates the length of the generated session key. This will be 0 if no session key was requested.
Security	Audit Success	12544	2015-04-24 22:16:54	Microsoft-Windows-Security-Auditing	4648: A logon was attempted using explicit credentials. Subject: Security ID: S-1-5-18 Account Name: LTRANPHD$ Account Domain: WORKGROUP Logon ID: 0x3e7 Logon GUID: {00000000-0000-0000-0000-000000000000} Account Whose Credentials Were Used: Account Name: DWM-1 Account Domain: Window Manager Logon GUID: {00000000-0000-0000-0000-000000000000} Target Server: Target Server Name: localhost Additional Information: localhost Process Information: Process ID: 0x200 Process Name: C:\Windows\System32\winlogon.exe Network Information: Network Address: - Port: - This event is generated when a process attempts to log on an account by explicitly specifying that account's credentials. This most commonly occurs in batch-type configurations such as scheduled tasks, or when using the RUNAS command.
Security	Audit Success	12544	2015-04-24 22:16:54	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: LTRANPHD$ Account Domain: WORKGROUP Logon ID: 0x3e7 Logon Type: 2 Impersonation Level: %%1833 New Logon: Security ID: S-1-5-90-1 Account Name: DWM-1 Account Domain: Window Manager Logon ID: 0xc7a2 Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x200 Process Name: C:\Windows\System32\winlogon.exe Network Information: Workstation Name: Source Network Address: - Source Port: - Detailed Authentication Information: Logon Process: Advapi Authentication Package: Negotiate Transited Services: - Package Name (NTLM only): - Key Length: 0 This event is generated when a logon session is created. It is generated on the computer that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service such as the Server service, or a local process such as Winlogon.exe or Services.exe. The logon type field indicates the kind of logon that occurred. The most common types are 2 (interactive) and 3 (network). The New Logon fields indicate the account for whom the new logon was created, i.e. the account that was logged on. The network fields indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impersonation level field indicates the extent to which a process in the logon session can impersonate. The authentication information fields provide detailed information about this specific logon request. - Logon GUID is a unique identifier that can be used to correlate this event with a KDC event. - Transited services indicate which intermediate services have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indicates the length of the generated session key. This will be 0 if no session key was requested.
Security	Audit Success	12544	2015-04-24 22:16:54	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: LTRANPHD$ Account Domain: WORKGROUP Logon ID: 0x3e7 Logon Type: 2 Impersonation Level: %%1833 New Logon: Security ID: S-1-5-90-1 Account Name: DWM-1 Account Domain: Window Manager Logon ID: 0xc7bf Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x200 Process Name: C:\Windows\System32\winlogon.exe Network Information: Workstation Name: Source Network Address: - Source Port: - Detailed Authentication Information: Logon Process: Advapi Authentication Package: Negotiate Transited Services: - Package Name (NTLM only): - Key Length: 0 This event is generated when a logon session is created. It is generated on the computer that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service such as the Server service, or a local process such as Winlogon.exe or Services.exe. The logon type field indicates the kind of logon that occurred. The most common types are 2 (interactive) and 3 (network). The New Logon fields indicate the account for whom the new logon was created, i.e. the account that was logged on. The network fields indicate where a

					remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impersonation level field indicates the extent to which a process in the logon session can impersonate. The authentication information fields provide detailed information about this specific logon request. - Logon GUID is a unique identifier that can be used to correlate this event with a KDC event. - Transited services indicate which intermediate services have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indicates the length of the generated session key. This will be 0 if no session key was requested.
Security	Audit Success	12544	2015-04-24 22:16:54	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: LTRANPHD$ Account Domain: WORKGROUP Logon ID: 0x3e7 Logon Type: 5 Impersonation Level: %%1833 New Logon: Security ID: S-1-5-19 Account Name: LOCAL SERVICE Account Domain: NT AUTHORITY Logon ID: 0x3e5 Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x230 Process Name: C:\Windows\System32\services.exe Network Information: Workstation Name: Source Network Address: - Source Port: - Detailed Authentication Information: Logon Process: Advapi Authentication Package: Negotiate Transited Services: - Package Name (NTLM only): - Key Length: 0 This event is generated when a logon session is created. It is generated on the computer that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service such as the Server service, or a local process such as Winlogon.exe or Services.exe. The logon type field indicates the kind of logon that occurred. The most common types are 2 (interactive) and 3 (network). The New Logon fields indicate the account for whom the new logon was created, i.e. the account that was logged on. The network fields indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impersonation level field indicates the extent to which a process in the logon session can impersonate. The authentication information fields provide detailed information about this specific logon request. - Logon GUID is a unique identifier that can be used to correlate this event with a KDC event. - Transited services indicate which intermediate services have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indicates the length of the generated session key. This will be 0 if no session key was requested.
Security	Audit Success	12544	2015-04-24 22:16:54	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: LTRANPHD$ Account Domain: WORKGROUP Logon ID: 0x3e7 Logon Type: 5 Impersonation Level: %%1833 New Logon: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Logon ID: 0x3e7 Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x230 Process Name: C:\Windows\System32\services.exe Network Information: Workstation Name: Source Network Address: - Source Port: - Detailed Authentication Information: Logon Process: Advapi Authentication Package: Negotiate Transited Services: - Package Name (NTLM only): - Key Length: 0 This event is generated when a logon session is created. It is generated on the computer that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service such as the Server service, or a local process such as Winlogon.exe or Services.exe. The logon type field indicates the kind of logon that occurred. The most common types are 2 (interactive) and 3 (network). The New Logon fields indicate the account for whom the new logon was created, i.e. the account that was logged on. The network fields indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impersonation level field indicates the extent to which a process in the logon session can impersonate. The authentication information fields provide detailed information about this specific logon request. - Logon GUID is a unique identifier that can be used to correlate this event with a KDC event. - Transited services indicate which intermediate services have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indicates the length of the generated session key. This will be 0 if no session key was requested.
Security	Audit Success	12544	2015-04-24 22:16:54	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: LTRANPHD$ Account Domain: WORKGROUP Logon ID: 0x3e7 Logon Type: 5 Impersonation Level: %%1833 New Logon: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Logon ID: 0x3e7 Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x230 Process Name: C:\Windows\System32\services.exe Network Information: Workstation Name: Source Network Address: - Source Port: - Detailed Authentication Information: Logon Process: Advapi Authentication Package: Negotiate Transited Services: - Package Name (NTLM only): - Key Length: 0 This event is generated when a logon session is created. It is generated on the computer that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service such as the Server service, or a local process such as Winlogon.exe or Services.exe. The logon type field indicates the kind of logon that occurred. The most common types are 2 (interactive) and 3 (network). The New Logon fields indicate the account for whom the new logon was created, i.e. the account that was logged on. The network fields indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impersonation level field indicates the extent to which a process in the logon session can impersonate. The authentication information fields provide detailed information about this specific logon request. - Logon GUID is a unique identifier that can be used to correlate this event with a KDC event. - Transited services indicate which intermediate services have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indicates the length of the generated session key. This will be 0 if no session key was requested.
					4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: LTRANPHD$ Account Domain: WORKGROUP Logon ID: 0x3e7 Logon Type: 5 Impersonation Level: %%1833 New Logon: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Logon ID: 0x3e7 Logon GUID:

Security	Audit Success	12544	2015-04-24 22:16:54	Microsoft-Windows-Security-Auditing	{00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x230 Process Name: C:\Windows\System32\services.exe Network Information: Workstation Name: Source Network Address: - Source Port: - Detailed Authentication Information: Logon Process: Advapi Authentication Package: Negotiate Transited Services: - Package Name (NTLM only): - Key Length: 0 This event is generated when a logon session is created. It is generated on the computer that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service such as the Server service, or a local process such as Winlogon.exe or Services.exe. The logon type field indicates the kind of logon that occurred. The most common types are 2 (interactive) and 3 (network). The New Logon fields indicate the account for whom the new logon was created, i.e. the account that was logged on. The network fields indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impersonation level field indicates the extent to which a process in the logon session can impersonate. The authentication information fields provide detailed information about this specific logon request. - Logon GUID is a unique identifier that can be used to correlate this event with a KDC event. - Transited services indicate which intermediate services have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indicates the length of the generated session key. This will be 0 if no session key was requested.
Security	Audit Success	12544	2015-04-24 22:16:54	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: LTRANPHD$ Account Domain: WORKGROUP Logon ID: 0x3e7 Logon Type: 5 Impersonation Level: %%1833 New Logon: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Logon ID: 0x3e7 Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x230 Process Name: C:\Windows\System32\services.exe Network Information: Workstation Name: Source Network Address: - Source Port: - Detailed Authentication Information: Logon Process: Advapi Authentication Package: Negotiate Transited Services: - Package Name (NTLM only): - Key Length: 0 This event is generated when a logon session is created. It is generated on the computer that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service such as the Server service, or a local process such as Winlogon.exe or Services.exe. The logon type field indicates the kind of logon that occurred. The most common types are 2 (interactive) and 3 (network). The New Logon fields indicate the account for whom the new logon was created, i.e. the account that was logged on. The network fields indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impersonation level field indicates the extent to which a process in the logon session can impersonate. The authentication information fields provide detailed information about this specific logon request. - Logon GUID is a unique identifier that can be used to correlate this event with a KDC event. - Transited services indicate which intermediate services have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indicates the length of the generated session key. This will be 0 if no session key was requested.
Security	Audit Success	12548	2015-04-24 22:16:54	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Logon ID: 0x3e7 Privileges: SeAssignPrimaryTokenPrivilege SeTcbPrivilege SeSecurityPrivilege SeTakeOwnershipPrivilege SeLoadDriverPrivilege SeBackupPrivilege SeRestorePrivilege SeDebugPrivilege SeAuditPrivilege SeSystemEnvironmentPrivilege SeImpersonatePrivilege
Security	Audit Success	12548	2015-04-24 22:16:54	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-20 Account Name: NETWORK SERVICE Account Domain: NT AUTHORITY Logon ID: 0x3e4 Privileges: SeAssignPrimaryTokenPrivilege SeAuditPrivilege SeImpersonatePrivilege
Security	Audit Success	12548	2015-04-24 22:16:54	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-90-1 Account Name: DWM-1 Account Domain: Window Manager Logon ID: 0xc7a2 Privileges: SeAssignPrimaryTokenPrivilege SeAuditPrivilege SeImpersonatePrivilege
Security	Audit Success	12548	2015-04-24 22:16:54	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-90-1 Account Name: DWM-1 Account Domain: Window Manager Logon ID: 0xc7bf Privileges: SeAssignPrimaryTokenPrivilege SeAuditPrivilege
Security	Audit Success	12548	2015-04-24 22:16:54	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-19 Account Name: LOCAL SERVICE Account Domain: NT AUTHORITY Logon ID: 0x3e5 Privileges: SeAssignPrimaryTokenPrivilege SeAuditPrivilege SeImpersonatePrivilege
Security	Audit Success	12548	2015-04-24 22:16:54	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Logon ID: 0x3e7 Privileges: SeAssignPrimaryTokenPrivilege SeTcbPrivilege SeSecurityPrivilege SeTakeOwnershipPrivilege SeLoadDriverPrivilege SeBackupPrivilege SeRestorePrivilege SeDebugPrivilege SeAuditPrivilege SeSystemEnvironmentPrivilege SeImpersonatePrivilege
Security	Audit Success	12548	2015-04-24 22:16:54	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Logon ID: 0x3e7 Privileges: SeAssignPrimaryTokenPrivilege SeTcbPrivilege SeSecurityPrivilege SeTakeOwnershipPrivilege SeLoadDriverPrivilege SeBackupPrivilege SeRestorePrivilege SeDebugPrivilege SeAuditPrivilege SeSystemEnvironmentPrivilege SeImpersonatePrivilege
Security	Audit Success	12548	2015-04-24 22:16:54	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Logon ID: 0x3e7 Privileges: SeAssignPrimaryTokenPrivilege SeTcbPrivilege SeSecurityPrivilege SeTakeOwnershipPrivilege SeLoadDriverPrivilege SeBackupPrivilege SeRestorePrivilege SeDebugPrivilege SeAuditPrivilege SeSystemEnvironmentPrivilege SeImpersonatePrivilege
Security	Audit	12548	2015-04-24	Microsoft-Windows-Security-	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Logon ID: 0x3e7 Privileges: SeAssignPrimaryTokenPrivilege SeTcbPrivilege

	Success		22:16:54	Auditing	SeSecurityPrivilege SeTakeOwnershipPrivilege SeLoadDriverPrivilege SeBackupPrivilege SeRestorePrivilege SeDebugPrivilege SeAuditPrivilege SeSystemEnvironmentPrivilege SeImpersonatePrivilege
Security	Audit Success	13568	2015-04-24 22:16:54	Microsoft-Windows-Security-Auditing	4902: The Per-user audit policy table was created. Number of Elements: 0 Policy ID: 0x785e
Security	Audit Success	12292	2015-04-24 22:16:55	Microsoft-Windows-Security-Auditing	5024: The Windows Firewall service started successfully.
Security	Audit Success	12544	2015-04-24 22:16:55	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: LTRANPHD$ Account Domain: WORKGROUP Logon ID: 0x3e7 Logon Type: 5 Impersonation Level: %%1833 New Logon: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Logon ID: 0x3e7 Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x230 Process Name: C:\Windows\System32\services.exe Network Information: Workstation Name: Source Network Address: - Source Port: - Detailed Authentication Information: Logon Process: Advapi Authentication Package: Negotiate Transited Services: - Package Name (NTLM only): - Key Length: 0 This event is generated when a logon session is created. It is generated on the computer that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service such as the Server service, or a local process such as Winlogon.exe or Services.exe. The logon type field indicates the kind of logon that occurred. The most common types are 2 (interactive) and 3 (network). The New Logon fields indicate the account for whom the new logon was created, i.e. the account that was logged on. The network fields indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impersonation level field indicates the extent to which a process in the logon session can impersonate. The authentication information fields provide detailed information about this specific logon request. - Logon GUID is a unique identifier that can be used to correlate this event with a KDC event. - Transited services indicate which intermediate services have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indicates the length of the generated session key. This will be 0 if no session key was requested.
Security	Audit Success	12544	2015-04-24 22:16:55	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-0-0 Account Name: - Account Domain: - Logon ID: 0x0 Logon Type: 3 Impersonation Level: %%1833 New Logon: Security ID: S-1-5-7 Account Name: ANONYMOUS LOGON Account Domain: NT AUTHORITY Logon ID: 0x180b3 Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x0 Process Name: - Network Information: Workstation Name: Source Network Address: - Source Port: - Detailed Authentication Information: Logon Process: NtLmSsp Authentication Package: NTLM Transited Services: - Package Name (NTLM only): NTLM V1 Key Length: 0 This event is generated when a logon session is created. It is generated on the computer that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service such as the Server service, or a local process such as Winlogon.exe or Services.exe. The logon type field indicates the kind of logon that occurred. The most common types are 2 (interactive) and 3 (network). The New Logon fields indicate the account for whom the new logon was created, i.e. the account that was logged on. The network fields indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impersonation level field indicates the extent to which a process in the logon session can impersonate. The authentication information fields provide detailed information about this specific logon request. - Logon GUID is a unique identifier that can be used to correlate this event with a KDC event. - Transited services indicate which intermediate services have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indicates the length of the generated session key. This will be 0 if no session key was requested.
Security	Audit Success	12548	2015-04-24 22:16:55	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Logon ID: 0x3e7 Privileges: SeAssignPrimaryTokenPrivilege SeTcbPrivilege SeSecurityPrivilege SeTakeOwnershipPrivilege SeLoadDriverPrivilege SeBackupPrivilege SeRestorePrivilege SeDebugPrivilege SeAuditPrivilege SeSystemEnvironmentPrivilege SeImpersonatePrivilege
Security	Audit Success	12544	2015-04-24 22:16:56	Microsoft-Windows-Security-Auditing	4648: A logon was attempted using explicit credentials. Subject: Security ID: S-1-5-18 Account Name: LTRANPHD$ Account Domain: WORKGROUP Logon ID: 0x3e7 Logon GUID: {00000000-0000-0000-0000-000000000000} Account Whose Credentials Were Used: Account Name: Liem Account Domain: LTRANPHD Logon GUID: {00000000-0000-0000-0000-000000000000} Target Server: Target Server Name: localhost Additional Information: localhost Process Information: Process ID: 0x200 Process Name: C:\Windows\System32\winlogon.exe Network Information: Network Address: 127.0.0.1 Port: 0 This event is generated when a process attempts to log on an account by explicitly specifying that account's credentials. This most commonly occurs in batch-type configurations such as scheduled tasks, or when using the RUNAS command.
					4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: LTRANPHD$ Account Domain: WORKGROUP Logon ID: 0x3e7 Logon Type: 2 Impersonation Level: %%1833 New Logon: Security ID: S-1-5-21-1888849264-3803429180-4108621888-1001 Account Name: Liem Account Domain: LTRANPHD Logon ID: 0x19963 Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x200 Process Name: C:\Windows\System32\winlogon.exe Network Information: Workstation Name: LTRANPHD Source Network Address: 127.0.0.1 Source Port: 0 Detailed Authentication Information: Logon Process: User32 Authentication Package: Negotiate Transited Services: - Package Name (NTLM only): - Key Length: 0 This event is generated when a logon session is created. It is generated on the computer that

Security	Audit Success	12544	2015-04-24 22:16:56	Microsoft-Windows-Security-Auditing	was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service such as the Server service, or a local process such as Winlogon.exe or Services.exe. The logon type field indicates the kind of logon that occurred. The most common types are 2 (interactive) and 3 (network). The New Logon fields indicate the account for whom the new logon was created, i.e. the account that was logged on. The network fields indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impersonation level field indicates the extent to which a process in the logon session can impersonate. The authentication information fields provide detailed information about this specific logon request. - Logon GUID is a unique identifier that can be used to correlate this event with a KDC event. - Transited services indicate which intermediate services have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indicates the length of the generated session key. This will be 0 if no session key was requested.
Security	Audit Success	12544	2015-04-24 22:16:56	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: LTRANPHD$ Account Domain: WORKGROUP Logon ID: 0x3e7 Logon Type: 2 Impersonation Level: %%1833 New Logon: Security ID: S-1-5-21-1888849264-3803429180-4108621888-1001 Account Name: Liem Account Domain: LTRANPHD Logon ID: 0x19999 Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x200 Process Name: C:\Windows\System32\winlogon.exe Network Information: Workstation Name: LTRANPHD Source Network Address: 127.0.0.1 Source Port: 0 Detailed Authentication Information: Logon Process: User32 Authentication Package: Negotiate Transited Services: - Package Name (NTLM only): - Key Length: 0 This event is generated when a logon session is created. It is generated on the computer that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service such as the Server service, or a local process such as Winlogon.exe or Services.exe. The logon type field indicates the kind of logon that occurred. The most common types are 2 (interactive) and 3 (network). The New Logon fields indicate the account for whom the new logon was created, i.e. the account that was logged on. The network fields indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impersonation level field indicates the extent to which a process in the logon session can impersonate. The authentication information fields provide detailed information about this specific logon request. - Logon GUID is a unique identifier that can be used to correlate this event with a KDC event. - Transited services indicate which intermediate services have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indicates the length of the generated session key. This will be 0 if no session key was requested.
Security	Audit Success	12544	2015-04-24 22:16:56	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: LTRANPHD$ Account Domain: WORKGROUP Logon ID: 0x3e7 Logon Type: 5 Impersonation Level: %%1833 New Logon: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Logon ID: 0x3e7 Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x230 Process Name: C:\Windows\System32\services.exe Network Information: Workstation Name: Source Network Address: - Source Port: - Detailed Authentication Information: Logon Process: Advapi Authentication Package: Negotiate Transited Services: - Package Name (NTLM only): - Key Length: 0 This event is generated when a logon session is created. It is generated on the computer that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service such as the Server service, or a local process such as Winlogon.exe or Services.exe. The logon type field indicates the kind of logon that occurred. The most common types are 2 (interactive) and 3 (network). The New Logon fields indicate the account for whom the new logon was created, i.e. the account that was logged on. The network fields indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impersonation level field indicates the extent to which a process in the logon session can impersonate. The authentication information fields provide detailed information about this specific logon request. - Logon GUID is a unique identifier that can be used to correlate this event with a KDC event. - Transited services indicate which intermediate services have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indicates the length of the generated session key. This will be 0 if no session key was requested.
Security	Audit Success	12548	2015-04-24 22:16:56	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-21-1888849264-3803429180-4108621888-1001 Account Name: Liem Account Domain: LTRANPHD Logon ID: 0x19963 Privileges: SeSecurityPrivilege SeTakeOwnershipPrivilege SeLoadDriverPrivilege SeBackupPrivilege SeRestorePrivilege SeDebugPrivilege SeSystemEnvironmentPrivilege SeImpersonatePrivilege
Security	Audit Success	12548	2015-04-24 22:16:56	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Logon ID: 0x3e7 Privileges: SeAssignPrimaryTokenPrivilege SeTcbPrivilege SeSecurityPrivilege SeTakeOwnershipPrivilege SeLoadDriverPrivilege SeBackupPrivilege SeRestorePrivilege SeDebugPrivilege SeAuditPrivilege SeSystemEnvironmentPrivilege SeImpersonatePrivilege
Security	Audit Success	13824	2015-04-24 22:16:58	Microsoft-Windows-Security-Auditing	4797: An attempt was made to query the existence of a blank password for an account. Subject: Security ID: S-1-5-21-1888849264-3803429180-4108621888-1001 Account Name: Liem Account Domain: LTRANPHD Logon ID: 0x19999 Additional Information: Caller Workstation: LTRANPHD Target Account Name: Administrator Target Account Domain: LTRANPHD
Security	Audit Success	13824	2015-04-24 22:16:58	Microsoft-Windows-Security-Auditing	4797: An attempt was made to query the existence of a blank password for an account. Subject: Security ID: S-1-5-21-1888849264-3803429180-4108621888-1001 Account Name: Liem Account Domain: LTRANPHD Logon ID: 0x19999 Additional Information: Caller Workstation: LTRANPHD Target Account Name: Guest Target Account Domain: LTRANPHD
					4797: An attempt was made to query the existence of a blank password for an account. Subject: Security ID:

Security	Audit Success	13824	2015-04-24 22:16:58	Microsoft-Windows-Security-Auditing	S-1-5-21-1888849264-3803429180-4108621888-1001 Account Name: Liem Account Domain: LTRANPHD Logon ID: 0x19999 Additional Information: Caller Workstation: LTRANPHD Target Account Name: Administrator Target Account Domain: LTRANPHD
Security	Audit Success	13824	2015-04-24 22:16:58	Microsoft-Windows-Security-Auditing	4797: An attempt was made to query the existence of a blank password for an account. Subject: Security ID: S-1-5-21-1888849264-3803429180-4108621888-1001 Account Name: Liem Account Domain: LTRANPHD Logon ID: 0x19999 Additional Information: Caller Workstation: LTRANPHD Target Account Name: Guest Target Account Domain: LTRANPHD
Security	Audit Success	13824	2015-04-24 22:17:04	Microsoft-Windows-Security-Auditing	4797: An attempt was made to query the existence of a blank password for an account. Subject: Security ID: S-1-5-19 Account Name: LOCAL SERVICE Account Domain: NT AUTHORITY Logon ID: 0x3e5 Additional Information: Caller Workstation: LTRANPHD Target Account Name: Administrator Target Account Domain: LTRANPHD
Security	Audit Success	13824	2015-04-24 22:17:04	Microsoft-Windows-Security-Auditing	4797: An attempt was made to query the existence of a blank password for an account. Subject: Security ID: S-1-5-19 Account Name: LOCAL SERVICE Account Domain: NT AUTHORITY Logon ID: 0x3e5 Additional Information: Caller Workstation: LTRANPHD Target Account Name: Guest Target Account Domain: LTRANPHD
Security	Audit Success	13824	2015-04-24 22:17:04	Microsoft-Windows-Security-Auditing	4797: An attempt was made to query the existence of a blank password for an account. Subject: Security ID: S-1-5-19 Account Name: LOCAL SERVICE Account Domain: NT AUTHORITY Logon ID: 0x3e5 Additional Information: Caller Workstation: LTRANPHD Target Account Name: Liem Target Account Domain: LTRANPHD
Security	Audit Success	13824	2015-04-24 22:17:04	Microsoft-Windows-Security-Auditing	4797: An attempt was made to query the existence of a blank password for an account. Subject: Security ID: S-1-5-19 Account Name: LOCAL SERVICE Account Domain: NT AUTHORITY Logon ID: 0x3e5 Additional Information: Caller Workstation: LTRANPHD Target Account Name: Liem Target Account Domain: LTRANPHD
Security	Audit Success	12544	2015-04-24 22:33:05	Microsoft-Windows-Security-Auditing	4648: A logon was attempted using explicit credentials. Subject: Security ID: S-1-5-18 Account Name: LTRANPHD$ Account Domain: WORKGROUP Logon ID: 0x3e7 Logon GUID: {00000000-0000-0000-0000-000000000000} Account Whose Credentials Were Used: Account Name: DWM-2 Account Domain: Window Manager Logon GUID: {00000000-0000-0000-0000-000000000000} Target Server: Target Server Name: localhost Additional Information: localhost Process Information: Process ID: 0xb34 Process Name: C:\Windows\System32\winlogon.exe Network Information: Network Address: - Port: - This event is generated when a process attempts to log on an account by explicitly specifying that account's credentials. This most commonly occurs in batch-type configurations such as scheduled tasks, or when using the RUNAS command.
Security	Audit Success	12544	2015-04-24 22:33:05	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: LTRANPHD$ Account Domain: WORKGROUP Logon ID: 0x3e7 Logon Type: 2 Impersonation Level: %%1833 New Logon: Security ID: S-1-5-90-2 Account Name: DWM-2 Account Domain: Window Manager Logon ID: 0x1f7a43 Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0xb34 Process Name: C:\Windows\System32\winlogon.exe Network Information: Workstation Name: Source Network Address: - Source Port: - Detailed Authentication Information: Logon Process: Advapi Authentication Package: Negotiate Transited Services: - Package Name (NTLM only): - Key Length: 0 This event is generated when a logon session is created. It is generated on the computer that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service such as the Server service, or a local process such as Winlogon.exe or Services.exe. The logon type field indicates the kind of logon that occurred. The most common types are 2 (interactive) and 3 (network). The New Logon fields indicate the account for whom the new logon was created, i.e. the account that was logged on. The network fields indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impersonation level field indicates the extent to which a process in the logon session can impersonate. The authentication information fields provide detailed information about this specific logon request. - Logon GUID is a unique identifier that can be used to correlate this event with a KDC event. - Transited services indicate which intermediate services have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indicates the length of the generated session key. This will be 0 if no session key was requested.
Security	Audit Success	12544	2015-04-24 22:33:05	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: LTRANPHD$ Account Domain: WORKGROUP Logon ID: 0x3e7 Logon Type: 2 Impersonation Level: %%1833 New Logon: Security ID: S-1-5-90-2 Account Name: DWM-2 Account Domain: Window Manager Logon ID: 0x1f7a6e Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0xb34 Process Name: C:\Windows\System32\winlogon.exe Network Information: Workstation Name: Source Network Address: - Source Port: - Detailed Authentication Information: Logon Process: Advapi Authentication Package: Negotiate Transited Services: - Package Name (NTLM only): - Key Length: 0 This event is generated when a logon session is created. It is generated on the computer that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service such as the Server service, or a local process such as Winlogon.exe or Services.exe. The logon type field indicates the kind of logon that occurred. The most common types are 2 (interactive) and 3 (network). The New Logon fields indicate the account for whom the new logon was created, i.e. the account that was logged on. The network fields indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impersonation level field indicates the extent to which a process in the logon session can impersonate. The authentication information fields provide detailed information about this specific logon request. - Logon GUID is a unique identifier that can be used to correlate this event with a KDC event. - Transited services indicate which intermediate services have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indicates the length of the generated

					session key. This will be 0 if no session key was requested.
Security	Audit Success	12548	2015-04-24 22:33:05	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-90-2 Account Name: DWM-2 Account Domain: Window Manager Logon ID: 0x1f7a43 Privileges: SeAssignPrimaryTokenPrivilege SeAuditPrivilege SeImpersonatePrivilege
Security	Audit Success	12548	2015-04-24 22:33:05	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-90-2 Account Name: DWM-2 Account Domain: Window Manager Logon ID: 0x1f7a6e Privileges: SeAssignPrimaryTokenPrivilege SeAuditPrivilege
Security	Audit Success	12545	2015-04-24 22:33:08	Microsoft-Windows-Security-Auditing	4647: User initiated logoff: Subject: Security ID: S-1-5-21-1888849264-3803429180-4108621888-1001 Account Name: Liem Account Domain: LTRANPHD Logon ID: 0x19999 This event is generated when a logoff is initiated. No further user-initiated activity can occur. This event can be interpreted as a logoff event.
Security	Audit Success	12545	2015-04-24 22:33:09	Microsoft-Windows-Security-Auditing	4634: An account was logged off. Subject: Security ID: S-1-5-90-1 Account Name: DWM-1 Account Domain: Window Manager Logon ID: 0xc7bf Logon Type: 2 This event is generated when a logon session is destroyed. It may be positively correlated with a logon event using the Logon ID value. Logon IDs are only unique between reboots on the same computer.
Security	Audit Success	12545	2015-04-24 22:33:09	Microsoft-Windows-Security-Auditing	4634: An account was logged off. Subject: Security ID: S-1-5-90-1 Account Name: DWM-1 Account Domain: Window Manager Logon ID: 0xc7a2 Logon Type: 2 This event is generated when a logon session is destroyed. It may be positively correlated with a logon event using the Logon ID value. Logon IDs are only unique between reboots on the same computer.
Security	Audit Success	12544	2015-04-24 22:33:48	Microsoft-Windows-Security-Auditing	4648: A logon was attempted using explicit credentials. Subject: Security ID: S-1-5-18 Account Name: LTRANPHD$ Account Domain: WORKGROUP Logon ID: 0x3e7 Logon GUID: {00000000-0000-0000-0000-000000000000} Account Whose Credentials Were Used: Account Name: Liem Account Domain: LTRANPHD Logon GUID: {00000000-0000-0000-0000-000000000000} Target Server: Target Server Name: localhost Additional Information: localhost Process Information: Process ID: 0xb34 Process Name: C:\Windows\System32\winlogon.exe Network Information: Network Address: 127.0.0.1 Port: 0 This event is generated when a process attempts to log on an account by explicitly specifying that account's credentials. This most commonly occurs in batch-type configurations such as scheduled tasks, or when using the RUNAS command.
Security	Audit Success	12544	2015-04-24 22:33:48	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: LTRANPHD$ Account Domain: WORKGROUP Logon ID: 0x3e7 Logon Type: 2 Impersonation Level: %%1833 New Logon: Security ID: S-1-5-21-1888849264-3803429180-4108621888-1001 Account Name: Liem Account Domain: LTRANPHD Logon ID: 0x2030fe Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0xb34 Process Name: C:\Windows\System32\winlogon.exe Network Information: Workstation Name: LTRANPHD Source Network Address: 127.0.0.1 Source Port: 0 Detailed Authentication Information: Logon Process: User32 Authentication Package: Negotiate Transited Services: - Package Name (NTLM only): - Key Length: 0 This event is generated when a logon session is created. It is generated on the computer that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service such as the Server service, or a local process such as Winlogon.exe or Services.exe. The logon type field indicates the kind of logon that occurred. The most common types are 2 (interactive) and 3 (network). The New Logon fields indicate the account for whom the new logon was created, i.e. the account that was logged on. The network fields indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impersonation level field indicates the extent to which a process in the logon session can impersonate. The authentication information fields provide detailed information about this specific logon request. - Logon GUID is a unique identifier that can be used to correlate this event with a KDC event. - Transited services indicate which intermediate services have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indicates the length of the generated session key. This will be 0 if no session key was requested.
Security	Audit Success	12544	2015-04-24 22:33:48	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: LTRANPHD$ Account Domain: WORKGROUP Logon ID: 0x3e7 Logon Type: 2 Impersonation Level: %%1833 New Logon: Security ID: S-1-5-21-1888849264-3803429180-4108621888-1001 Account Name: Liem Account Domain: LTRANPHD Logon ID: 0x20311e Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0xb34 Process Name: C:\Windows\System32\winlogon.exe Network Information: Workstation Name: LTRANPHD Source Network Address: 127.0.0.1 Source Port: 0 Detailed Authentication Information: Logon Process: User32 Authentication Package: Negotiate Transited Services: - Package Name (NTLM only): - Key Length: 0 This event is generated when a logon session is created. It is generated on the computer that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service such as the Server service, or a local process such as Winlogon.exe or Services.exe. The logon type field indicates the kind of logon that occurred. The most common types are 2 (interactive) and 3 (network). The New Logon fields indicate the account for whom the new logon was created, i.e. the account that was logged on. The network fields indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impersonation level field indicates the extent to which a process in the logon session can impersonate. The authentication information fields provide detailed information about this specific logon request. - Logon GUID is a unique identifier that can be used to correlate this event with a KDC event. - Transited services indicate which intermediate services have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indicates the length of the generated session key. This will be 0 if no session key was

					requested.
Security	Audit Success	12548	2015-04-24 22:33:48	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-21-1888849264-3803429180-4108621888-1001 Account Name: Liem Account Domain: LTRANPHD Logon ID: 0x2030fe Privileges: SeSecurityPrivilege SeTakeOwnershipPrivilege SeLoadDriverPrivilege SeBackupPrivilege SeRestorePrivilege SeDebugPrivilege SeSystemEnvironmentPrivilege SeImpersonatePrivilege
Security	Audit Success	13824	2015-04-24 22:33:49	Microsoft-Windows-Security-Auditing	4797: An attempt was made to query the existence of a blank password for an account. Subject: Security ID: S-1-5-19 Account Name: LOCAL SERVICE Account Domain: NT AUTHORITY Logon ID: 0x3e5 Additional Information: Caller Workstation: LTRANPHD Target Account Name: Administrator Target Account Domain: LTRANPHD
Security	Audit Success	13824	2015-04-24 22:33:49	Microsoft-Windows-Security-Auditing	4797: An attempt was made to query the existence of a blank password for an account. Subject: Security ID: S-1-5-19 Account Name: LOCAL SERVICE Account Domain: NT AUTHORITY Logon ID: 0x3e5 Additional Information: Caller Workstation: LTRANPHD Target Account Name: Guest Target Account Domain: LTRANPHD
Security	Audit Success	13824	2015-04-24 22:33:49	Microsoft-Windows-Security-Auditing	4797: An attempt was made to query the existence of a blank password for an account. Subject: Security ID: S-1-5-19 Account Name: LOCAL SERVICE Account Domain: NT AUTHORITY Logon ID: 0x3e5 Additional Information: Caller Workstation: LTRANPHD Target Account Name: Liem Target Account Domain: LTRANPHD
Security	Audit Success	13824	2015-04-24 22:33:49	Microsoft-Windows-Security-Auditing	4797: An attempt was made to query the existence of a blank password for an account. Subject: Security ID: S-1-5-19 Account Name: LOCAL SERVICE Account Domain: NT AUTHORITY Logon ID: 0x3e5 Additional Information: Caller Workstation: LTRANPHD Target Account Name: Liem Target Account Domain: LTRANPHD
Security	Audit Success	13824	2015-04-24 22:33:49	Microsoft-Windows-Security-Auditing	4797: An attempt was made to query the existence of a blank password for an account. Subject: Security ID: S-1-5-19 Account Name: LOCAL SERVICE Account Domain: NT AUTHORITY Logon ID: 0x3e5 Additional Information: Caller Workstation: LTRANPHD Target Account Name: Administrator Target Account Domain: LTRANPHD
Security	Audit Success	13824	2015-04-24 22:33:49	Microsoft-Windows-Security-Auditing	4797: An attempt was made to query the existence of a blank password for an account. Subject: Security ID: S-1-5-19 Account Name: LOCAL SERVICE Account Domain: NT AUTHORITY Logon ID: 0x3e5 Additional Information: Caller Workstation: LTRANPHD Target Account Name: Guest Target Account Domain: LTRANPHD
Security	Audit Success	13824	2015-04-24 22:33:49	Microsoft-Windows-Security-Auditing	4797: An attempt was made to query the existence of a blank password for an account. Subject: Security ID: S-1-5-19 Account Name: LOCAL SERVICE Account Domain: NT AUTHORITY Logon ID: 0x3e5 Additional Information: Caller Workstation: LTRANPHD Target Account Name: Liem Target Account Domain: LTRANPHD
Security	Audit Success	13824	2015-04-24 22:33:49	Microsoft-Windows-Security-Auditing	4797: An attempt was made to query the existence of a blank password for an account. Subject: Security ID: S-1-5-19 Account Name: LOCAL SERVICE Account Domain: NT AUTHORITY Logon ID: 0x3e5 Additional Information: Caller Workstation: LTRANPHD Target Account Name: Administrator Target Account Domain: LTRANPHD
Security	Audit Success	13824	2015-04-24 22:33:49	Microsoft-Windows-Security-Auditing	4797: An attempt was made to query the existence of a blank password for an account. Subject: Security ID: S-1-5-19 Account Name: LOCAL SERVICE Account Domain: NT AUTHORITY Logon ID: 0x3e5 Additional Information: Caller Workstation: LTRANPHD Target Account Name: Liem Target Account Domain: LTRANPHD
Security	Audit Success	13824	2015-04-24 22:33:49	Microsoft-Windows-Security-Auditing	4797: An attempt was made to query the existence of a blank password for an account. Subject: Security ID: S-1-5-19 Account Name: LOCAL SERVICE Account Domain: NT AUTHORITY Logon ID: 0x3e5 Additional Information: Caller Workstation: LTRANPHD Target Account Name: Administrator Target Account Domain: LTRANPHD
Security	Audit Success	13824	2015-04-24 22:33:49	Microsoft-Windows-Security-Auditing	4797: An attempt was made to query the existence of a blank password for an account. Subject: Security ID: S-1-5-19 Account Name: LOCAL SERVICE Account Domain: NT AUTHORITY Logon ID: 0x3e5 Additional Information: Caller Workstation: LTRANPHD Target Account Name: Guest Target Account Domain: LTRANPHD
Security	Audit Success	13824	2015-04-24 22:33:49	Microsoft-Windows-Security-Auditing	4797: An attempt was made to query the existence of a blank password for an account. Subject: Security ID: S-1-5-19 Account Name: LOCAL SERVICE Account Domain: NT AUTHORITY Logon ID: 0x3e5 Additional Information: Caller Workstation: LTRANPHD Target Account Name: Liem Target Account Domain: LTRANPHD
Security	Audit Success	13824	2015-04-24 22:33:49	Microsoft-Windows-Security-Auditing	4797: An attempt was made to query the existence of a blank password for an account. Subject: Security ID: S-1-5-19 Account Name: LOCAL SERVICE Account Domain: NT AUTHORITY Logon ID: 0x3e5 Additional Information: Caller Workstation: LTRANPHD Target Account Name: Liem Target Account Domain: LTRANPHD
Security	Audit Success	13824	2015-04-24 22:33:49	Microsoft-Windows-Security-Auditing	4797: An attempt was made to query the existence of a blank password for an account. Subject: Security ID: S-1-5-19 Account Name: LOCAL SERVICE Account Domain: NT AUTHORITY Logon ID: 0x3e5 Additional Information: Caller Workstation: LTRANPHD Target Account Name: Administrator Target Account Domain: LTRANPHD
Security	Audit Success	13824	2015-04-24 22:33:49	Microsoft-Windows-Security-Auditing	4797: An attempt was made to query the existence of a blank password for an account. Subject: Security ID: S-1-5-19 Account Name: LOCAL SERVICE Account Domain: NT AUTHORITY Logon ID: 0x3e5 Additional Information: Caller Workstation: LTRANPHD Target Account Name: Guest Target Account Domain: LTRANPHD
Security	Audit Success	13824	2015-04-24 22:33:49	Microsoft-Windows-Security-Auditing	4797: An attempt was made to query the existence of a blank password for an account. Subject: Security ID: S-1-5-19 Account Name: LOCAL SERVICE Account Domain: NT AUTHORITY Logon ID: 0x3e5 Additional Information: Caller Workstation: LTRANPHD Target Account Name: Liem Target Account Domain: LTRANPHD
Security	Audit Success	13824	2015-04-24 22:33:49	Microsoft-Windows-Security-Auditing	4797: An attempt was made to query the existence of a blank password for an account. Subject: Security ID: S-1-5-19 Account Name: LOCAL SERVICE Account Domain: NT AUTHORITY Logon ID: 0x3e5 Additional Information: Caller Workstation: LTRANPHD Target Account Name: Liem Target Account Domain: LTRANPHD
	Audit		2015-04-	Microsoft-Windows-Security-	4797: An attempt was made to query the existence of a blank password for an account. Subject: Security ID: S-1-5-21-1888849264-3803429180-4108621888-1001 Account Name: Liem Account Domain: LTRANPHD Logon

Security	Success	13824	24 22:33:50	Auditing	ID: 0x20311e Additional Information: Caller Workstation: LTRANPHD Target Account Name: Administrator Target Account Domain: LTRANPHD
Security	Audit Success	13824	2015-04-24 22:33:50	Microsoft-Windows-Security-Auditing	4797: An attempt was made to query the existence of a blank password for an account. Subject: Security ID: S-1-5-21-1888849264-3803429180-4108621888-1001 Account Name: Liem Account Domain: LTRANPHD Logon ID: 0x20311e Additional Information: Caller Workstation: LTRANPHD Target Account Name: Guest Target Account Domain: LTRANPHD
Security	Audit Success	13824	2015-04-24 22:33:50	Microsoft-Windows-Security-Auditing	4797: An attempt was made to query the existence of a blank password for an account. Subject: Security ID: S-1-5-21-1888849264-3803429180-4108621888-1001 Account Name: Liem Account Domain: LTRANPHD Logon ID: 0x20311e Additional Information: Caller Workstation: LTRANPHD Target Account Name: Administrator Target Account Domain: LTRANPHD
Security	Audit Success	13824	2015-04-24 22:33:50	Microsoft-Windows-Security-Auditing	4797: An attempt was made to query the existence of a blank password for an account. Subject: Security ID: S-1-5-21-1888849264-3803429180-4108621888-1001 Account Name: Liem Account Domain: LTRANPHD Logon ID: 0x20311e Additional Information: Caller Workstation: LTRANPHD Target Account Name: Guest Target Account Domain: LTRANPHD
Security	Audit Success	12545	2015-04-24 22:38:01	Microsoft-Windows-Security-Auditing	4647: User initiated logoff: Subject: Security ID: S-1-5-21-1888849264-3803429180-4108621888-1001 Account Name: Liem Account Domain: LTRANPHD Logon ID: 0x20311e This event is generated when a logoff is initiated. No further user-initiated activity can occur. This event can be interpreted as a logoff event.
Security	Audit Success	103	2015-04-24 22:38:02	Microsoft-Windows-Eventlog	1100: The event logging service has shut down.
Security	Audit Success	12288	2015-04-25 07:22:37	Microsoft-Windows-Security-Auditing	4608: Windows is starting up. This event is logged when LSASS.EXE starts and the auditing subsystem is initialized.
Security	Audit Success	12544	2015-04-25 07:22:37	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-0-0 Account Name: - Account Domain: - Logon ID: 0x0 Logon Type: 0 Impersonation Level: - New Logon: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Logon ID: 0x3e7 Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x4 Process Name: Network Information: Workstation Name: - Source Network Address: - Source Port: - Detailed Authentication Information: Logon Process: - Authentication Package: - Transited Services: - Package Name (NTLM only): - Key Length: 0 This event is generated when a logon session is created. It is generated on the computer that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service such as the Server service, or a local process such as Winlogon.exe or Services.exe. The logon type field indicates the kind of logon that occurred. The most common types are 2 (interactive) and 3 (network). The New Logon fields indicate the account for whom the new logon was created, i.e. the account that was logged on. The network fields indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impersonation level field indicates the extent to which a process in the logon session can impersonate. The authentication information fields provide detailed information about this specific logon request. - Logon GUID is a unique identifier that can be used to correlate this event with a KDC event. - Transited services indicate which intermediate services have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indicates the length of the generated session key. This will be 0 if no session key was requested.
Security	Audit Success	12544	2015-04-25 07:22:37	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: LTRANPHD$ Account Domain: WORKGROUP Logon ID: 0x3e7 Logon Type: 5 Impersonation Level: %%1833 New Logon: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Logon ID: 0x3e7 Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x234 Process Name: C:\Windows\System32\services.exe Network Information: Workstation Name: Source Network Address: - Source Port: - Detailed Authentication Information: Logon Process: Advapi Authentication Package: Negotiate Transited Services: - Package Name (NTLM only): - Key Length: 0 This event is generated when a logon session is created. It is generated on the computer that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service such as the Server service, or a local process such as Winlogon.exe or Services.exe. The logon type field indicates the kind of logon that occurred. The most common types are 2 (interactive) and 3 (network). The New Logon fields indicate the account for whom the new logon was created, i.e. the account that was logged on. The network fields indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impersonation level field indicates the extent to which a process in the logon session can impersonate. The authentication information fields provide detailed information about this specific logon request. - Logon GUID is a unique identifier that can be used to correlate this event with a KDC event. - Transited services indicate which intermediate services have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indicates the length of the generated session key. This will be 0 if no session key was requested.
					4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: LTRANPHD$ Account Domain: WORKGROUP Logon ID: 0x3e7 Logon Type: 5 Impersonation Level: %%1833 New Logon: Security ID: S-1-5-20 Account Name: NETWORK SERVICE Account Domain: NT AUTHORITY Logon ID: 0x3e4 Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x234 Process Name: C:\Windows\System32\services.exe Network Information: Workstation Name: Source Network Address: -

Security	Audit Success	12544	2015-04-25 07:22:37	Microsoft-Windows-Security-Auditing	Source Port: - Detailed Authentication Information: Logon Process: Advapi Authentication Package: Negotiate Transited Services: - Package Name (NTLM only): - Key Length: 0 This event is generated when a logon session is created. It is generated on the computer that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service such as the Server service, or a local process such as Winlogon.exe or Services.exe. The logon type field indicates the kind of logon that occurred. The most common types are 2 (interactive) and 3 (network). The New Logon fields indicate the account for whom the new logon was created, i.e. the account that was logged on. The network fields indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impersonation level field indicates the extent to which a process in the logon session can impersonate. The authentication information fields provide detailed information about this specific logon request. - Logon GUID is a unique identifier that can be used to correlate this event with a KDC event. - Transited services indicate which intermediate services have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indicates the length of the generated session key. This will be 0 if no session key was requested.
Security	Audit Success	12544	2015-04-25 07:22:37	Microsoft-Windows-Security-Auditing	4648: A logon was attempted using explicit credentials. Subject: Security ID: S-1-5-18 Account Name: LTRANPHD$ Account Domain: WORKGROUP Logon ID: 0x3e7 Logon GUID: {00000000-0000-0000-0000-000000000000} Account Whose Credentials Were Used: Account Name: DWM-1 Account Domain: Window Manager Logon GUID: {00000000-0000-0000-0000-000000000000} Target Server: Target Server Name: localhost Additional Information: localhost Process Information: Process ID: 0x204 Process Name: C:\Windows\System32\winlogon.exe Network Information: Network Address: - Port: - This event is generated when a process attempts to log on an account by explicitly specifying that account's credentials. This most commonly occurs in batch-type configurations such as scheduled tasks, or when using the RUNAS command.
Security	Audit Success	12544	2015-04-25 07:22:37	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: LTRANPHD$ Account Domain: WORKGROUP Logon ID: 0x3e7 Logon Type: 2 Impersonation Level: %%1833 New Logon: Security ID: S-1-5-90-1 Account Name: DWM-1 Account Domain: Window Manager Logon ID: 0xc7cc Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x204 Process Name: C:\Windows\System32\winlogon.exe Network Information: Workstation Name: Source Network Address: - Source Port: - Detailed Authentication Information: Logon Process: Advapi Authentication Package: Negotiate Transited Services: - Package Name (NTLM only): - Key Length: 0 This event is generated when a logon session is created. It is generated on the computer that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service such as the Server service, or a local process such as Winlogon.exe or Services.exe. The logon type field indicates the kind of logon that occurred. The most common types are 2 (interactive) and 3 (network). The New Logon fields indicate the account for whom the new logon was created, i.e. the account that was logged on. The network fields indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impersonation level field indicates the extent to which a process in the logon session can impersonate. The authentication information fields provide detailed information about this specific logon request. - Logon GUID is a unique identifier that can be used to correlate this event with a KDC event. - Transited services indicate which intermediate services have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indicates the length of the generated session key. This will be 0 if no session key was requested.
Security	Audit Success	12544	2015-04-25 07:22:37	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: LTRANPHD$ Account Domain: WORKGROUP Logon ID: 0x3e7 Logon Type: 2 Impersonation Level: %%1833 New Logon: Security ID: S-1-5-90-1 Account Name: DWM-1 Account Domain: Window Manager Logon ID: 0xc7e4 Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x204 Process Name: C:\Windows\System32\winlogon.exe Network Information: Workstation Name: Source Network Address: - Source Port: - Detailed Authentication Information: Logon Process: Advapi Authentication Package: Negotiate Transited Services: - Package Name (NTLM only): - Key Length: 0 This event is generated when a logon session is created. It is generated on the computer that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service such as the Server service, or a local process such as Winlogon.exe or Services.exe. The logon type field indicates the kind of logon that occurred. The most common types are 2 (interactive) and 3 (network). The New Logon fields indicate the account for whom the new logon was created, i.e. the account that was logged on. The network fields indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impersonation level field indicates the extent to which a process in the logon session can impersonate. The authentication information fields provide detailed information about this specific logon request. - Logon GUID is a unique identifier that can be used to correlate this event with a KDC event. - Transited services indicate which intermediate services have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indicates the length of the generated session key. This will be 0 if no session key was requested.
					4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: LTRANPHD$ Account Domain: WORKGROUP Logon ID: 0x3e7 Logon Type: 5 Impersonation Level: %%1833 New Logon: Security ID: S-1-5-19 Account Name: LOCAL SERVICE Account Domain: NT AUTHORITY Logon ID: 0x3e5 Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x234 Process Name: C:\Windows\System32\services.exe Network Information: Workstation Name: Source Network Address: - Source Port: - Detailed Authentication Information: Logon Process: Advapi Authentication Package: Negotiate Transited Services: - Package Name (NTLM only): - Key Length: 0 This event is generated when a logon session is

Security	Audit Success	12544	2015-04-25 07:22:37		Microsoft-Windows-Security-Auditing	created. It is generated on the computer that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service such as the Server service, or a local process such as Winlogon.exe or Services.exe. The logon type field indicates the kind of logon that occurred. The most common types are 2 (interactive) and 3 (network). The New Logon fields indicate the account for whom the new logon was created, i.e. the account that was logged on. The network fields indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impersonation level field indicates the extent to which a process in the logon session can impersonate. The authentication information fields provide detailed information about this specific logon request. - Logon GUID is a unique identifier that can be used to correlate this event with a KDC event. - Transited services indicate which intermediate services have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indicates the length of the generated session key. This will be 0 if no session key was requested.
Security	Audit Success	12544	2015-04-25 07:22:37		Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: LTRANPHD$ Account Domain: WORKGROUP Logon ID: 0x3e7 Logon Type: 5 Impersonation Level: %%1833 New Logon: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Logon ID: 0x3e7 Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x234 Process Name: C:\Windows\System32\services.exe Network Information: Workstation Name: Source Network Address: - Source Port: - Detailed Authentication Information: Logon Process: Advapi Authentication Package: Negotiate Transited Services: - Package Name (NTLM only): - Key Length: 0 This event is generated when a logon session is created. It is generated on the computer that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service such as the Server service, or a local process such as Winlogon.exe or Services.exe. The logon type field indicates the kind of logon that occurred. The most common types are 2 (interactive) and 3 (network). The New Logon fields indicate the account for whom the new logon was created, i.e. the account that was logged on. The network fields indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impersonation level field indicates the extent to which a process in the logon session can impersonate. The authentication information fields provide detailed information about this specific logon request. - Logon GUID is a unique identifier that can be used to correlate this event with a KDC event. - Transited services indicate which intermediate services have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indicates the length of the generated session key. This will be 0 if no session key was requested.
Security	Audit Success	12544	2015-04-25 07:22:37		Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: LTRANPHD$ Account Domain: WORKGROUP Logon ID: 0x3e7 Logon Type: 5 Impersonation Level: %%1833 New Logon: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Logon ID: 0x3e7 Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x234 Process Name: C:\Windows\System32\services.exe Network Information: Workstation Name: Source Network Address: - Source Port: - Detailed Authentication Information: Logon Process: Advapi Authentication Package: Negotiate Transited Services: - Package Name (NTLM only): - Key Length: 0 This event is generated when a logon session is created. It is generated on the computer that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service such as the Server service, or a local process such as Winlogon.exe or Services.exe. The logon type field indicates the kind of logon that occurred. The most common types are 2 (interactive) and 3 (network). The New Logon fields indicate the account for whom the new logon was created, i.e. the account that was logged on. The network fields indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impersonation level field indicates the extent to which a process in the logon session can impersonate. The authentication information fields provide detailed information about this specific logon request. - Logon GUID is a unique identifier that can be used to correlate this event with a KDC event. - Transited services indicate which intermediate services have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indicates the length of the generated session key. This will be 0 if no session key was requested.
Security	Audit Success	12544	2015-04-25 07:22:37		Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: LTRANPHD$ Account Domain: WORKGROUP Logon ID: 0x3e7 Logon Type: 5 Impersonation Level: %%1833 New Logon: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Logon ID: 0x3e7 Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x234 Process Name: C:\Windows\System32\services.exe Network Information: Workstation Name: Source Network Address: - Source Port: - Detailed Authentication Information: Logon Process: Advapi Authentication Package: Negotiate Transited Services: - Package Name (NTLM only): - Key Length: 0 This event is generated when a logon session is created. It is generated on the computer that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service such as the Server service, or a local process such as Winlogon.exe or Services.exe. The logon type field indicates the kind of logon that occurred. The most common types are 2 (interactive) and 3 (network). The New Logon fields indicate the account for whom the new logon was created, i.e. the account that was logged on. The network fields indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impersonation level field indicates the extent to which a process in the logon session can impersonate. The authentication information fields provide detailed information about this specific logon request. - Logon GUID is a unique identifier that can be used to correlate this event with a KDC event. - Transited services indicate which intermediate services have participated in this logon request. - Package name indicates

						which sub-protocol was used among the NTLM protocols. - Key length indicates the length of the generated session key. This will be 0 if no session key was requested.
Security	Audit Success	12548	2015-04-25 07:22:37		Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Logon ID: 0x3e7 Privileges: SeAssignPrimaryTokenPrivilege SeTcbPrivilege SeSecurityPrivilege SeTakeOwnershipPrivilege SeLoadDriverPrivilege SeBackupPrivilege SeRestorePrivilege SeDebugPrivilege SeAuditPrivilege SeSystemEnvironmentPrivilege SeImpersonatePrivilege
Security	Audit Success	12548	2015-04-25 07:22:37		Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-20 Account Name: NETWORK SERVICE Account Domain: NT AUTHORITY Logon ID: 0x3e4 Privileges: SeAssignPrimaryTokenPrivilege SeAuditPrivilege SeImpersonatePrivilege
Security	Audit Success	12548	2015-04-25 07:22:37		Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-90-1 Account Name: DWM-1 Account Domain: Window Manager Logon ID: 0xc7cc Privileges: SeAssignPrimaryTokenPrivilege SeAuditPrivilege SeImpersonatePrivilege
Security	Audit Success	12548	2015-04-25 07:22:37		Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-90-1 Account Name: DWM-1 Account Domain: Window Manager Logon ID: 0xc7e4 Privileges: SeAssignPrimaryTokenPrivilege SeAuditPrivilege
Security	Audit Success	12548	2015-04-25 07:22:37		Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-19 Account Name: LOCAL SERVICE Account Domain: NT AUTHORITY Logon ID: 0x3e5 Privileges: SeAssignPrimaryTokenPrivilege SeAuditPrivilege SeImpersonatePrivilege
Security	Audit Success	12548	2015-04-25 07:22:37		Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Logon ID: 0x3e7 Privileges: SeAssignPrimaryTokenPrivilege SeTcbPrivilege SeSecurityPrivilege SeTakeOwnershipPrivilege SeLoadDriverPrivilege SeBackupPrivilege SeRestorePrivilege SeDebugPrivilege SeAuditPrivilege SeSystemEnvironmentPrivilege SeImpersonatePrivilege
Security	Audit Success	12548	2015-04-25 07:22:37		Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Logon ID: 0x3e7 Privileges: SeAssignPrimaryTokenPrivilege SeTcbPrivilege SeSecurityPrivilege SeTakeOwnershipPrivilege SeLoadDriverPrivilege SeBackupPrivilege SeRestorePrivilege SeDebugPrivilege SeAuditPrivilege SeSystemEnvironmentPrivilege SeImpersonatePrivilege
Security	Audit Success	12548	2015-04-25 07:22:37		Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Logon ID: 0x3e7 Privileges: SeAssignPrimaryTokenPrivilege SeTcbPrivilege SeSecurityPrivilege SeTakeOwnershipPrivilege SeLoadDriverPrivilege SeBackupPrivilege SeRestorePrivilege SeDebugPrivilege SeAuditPrivilege SeSystemEnvironmentPrivilege SeImpersonatePrivilege
Security	Audit Success	13568	2015-04-25 07:22:37		Microsoft-Windows-Security-Auditing	4902: The Per-user audit policy table was created. Number of Elements: 0 Policy ID: 0x7879
Security	Audit Success	12292	2015-04-25 07:22:38		Microsoft-Windows-Security-Auditing	5033: The Windows Firewall Driver started successfully.
Security	Audit Success	12292	2015-04-25 07:22:38		Microsoft-Windows-Security-Auditing	5024: The Windows Firewall service started successfully.
Security	Audit Success	12544	2015-04-25 07:22:38		Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: LTRANPHD$ Account Domain: WORKGROUP Logon ID: 0x3e7 Logon Type: 5 Impersonation Level: %%1833 New Logon: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Logon ID: 0x3e7 Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x234 Process Name: C:\Windows\System32\services.exe Network Information: Workstation Name: Source Network Address: - Source Port: - Detailed Authentication Information: Logon Process: Advapi Authentication Package: Negotiate Transited Services: - Package Name (NTLM only): - Key Length: 0 This event is generated when a logon session is created. It is generated on the computer that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service such as the Server service, or a local process such as Winlogon.exe or Services.exe. The logon type field indicates the kind of logon that occurred. The most common types are 2 (interactive) and 3 (network). The New Logon fields indicate the account for whom the new logon was created, i.e. the account that was logged on. The network fields indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impersonation level field indicates the extent to which a process in the logon session can impersonate. The authentication information fields provide detailed information about this specific logon request. - Logon GUID is a unique identifier that can be used to correlate this event with a KDC event. - Transited services indicate which intermediate services have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indicates the length of the generated session key. This will be 0 if no session key was requested.
						4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: LTRANPHD$ Account Domain: WORKGROUP Logon ID: 0x3e7 Logon Type: 5 Impersonation Level: %%1833 New Logon: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Logon ID: 0x3e7 Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x234 Process Name: C:\Windows\System32\services.exe Network Information: Workstation Name: Source Network Address: - Source Port: - Detailed Authentication Information: Logon Process: Advapi Authentication Package: Negotiate Transited

Security	Audit Success	12544	2015-04-25 07:22:38	Microsoft-Windows-Security-Auditing	Services: - Package Name (NTLM only): - Key Length: 0 This event is generated when a logon session is created. It is generated on the computer that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service such as the Server service, or a local process such as Winlogon.exe or Services.exe. The logon type field indicates the kind of logon that occurred. The most common types are 2 (interactive) and 3 (network). The New Logon fields indicate the account for whom the new logon was created, i.e. the account that was logged on. The network fields indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impersonation level field indicates the extent to which a process in the logon session can impersonate. The authentication information fields provide detailed information about this specific logon request. - Logon GUID is a unique identifier that can be used to correlate this event with a KDC event. - Transited services indicate which intermediate services have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indicates the length of the generated session key. This will be 0 if no session key was requested.
Security	Audit Success	12544	2015-04-25 07:22:38	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-0-0 Account Name: - Account Domain: - Logon ID: 0x0 Logon Type: 3 Impersonation Level: %%1833 New Logon: Security ID: S-1-5-7 Account Name: ANONYMOUS LOGON Account Domain: NT AUTHORITY Logon ID: 0x17616 Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x0 Process Name: - Network Information: Workstation Name: Source Network Address: - Source Port: - Detailed Authentication Information: Logon Process: NtLmSsp Authentication Package: NTLM Transited Services: - Package Name (NTLM only): NTLM V1 Key Length: 0 This event is generated when a logon session is created. It is generated on the computer that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service such as the Server service, or a local process such as Winlogon.exe or Services.exe. The logon type field indicates the kind of logon that occurred. The most common types are 2 (interactive) and 3 (network). The New Logon fields indicate the account for whom the new logon was created, i.e. the account that was logged on. The network fields indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impersonation level field indicates the extent to which a process in the logon session can impersonate. The authentication information fields provide detailed information about this specific logon request. - Logon GUID is a unique identifier that can be used to correlate this event with a KDC event. - Transited services indicate which intermediate services have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indicates the length of the generated session key. This will be 0 if no session key was requested.
Security	Audit Success	12548	2015-04-25 07:22:38	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Logon ID: 0x3e7 Privileges: SeAssignPrimaryTokenPrivilege SeTcbPrivilege SeSecurityPrivilege SeTakeOwnershipPrivilege SeLoadDriverPrivilege SeBackupPrivilege SeRestorePrivilege SeDebugPrivilege SeAuditPrivilege SeSystemEnvironmentPrivilege SeImpersonatePrivilege
Security	Audit Success	12548	2015-04-25 07:22:38	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Logon ID: 0x3e7 Privileges: SeAssignPrimaryTokenPrivilege SeTcbPrivilege SeSecurityPrivilege SeTakeOwnershipPrivilege SeLoadDriverPrivilege SeBackupPrivilege SeRestorePrivilege SeDebugPrivilege SeAuditPrivilege SeSystemEnvironmentPrivilege SeImpersonatePrivilege
Security	Audit Success	12544	2015-04-25 07:22:40	Microsoft-Windows-Security-Auditing	4648: A logon was attempted using explicit credentials. Subject: Security ID: S-1-5-18 Account Name: LTRANPHD$ Account Domain: WORKGROUP Logon ID: 0x3e7 Logon GUID: {00000000-0000-0000-0000-000000000000} Account Whose Credentials Were Used: Account Name: Liem Account Domain: LTRANPHD Logon GUID: {00000000-0000-0000-0000-000000000000} Target Server: Target Server Name: localhost Additional Information: localhost Process Information: Process ID: 0x204 Process Name: C:\Windows\System32\winlogon.exe Network Information: Network Address: 127.0.0.1 Port: 0 This event is generated when a process attempts to log on an account by explicitly specifying that account's credentials. This most commonly occurs in batch-type configurations such as scheduled tasks, or when using the RUNAS command.
Security	Audit Success	12544	2015-04-25 07:22:40	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: LTRANPHD$ Account Domain: WORKGROUP Logon ID: 0x3e7 Logon Type: 2 Impersonation Level: %%1833 New Logon: Security ID: S-1-5-21-1888849264-3803429180-4108621888-1001 Account Name: Liem Account Domain: LTRANPHD Logon ID: 0x1a85a Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x204 Process Name: C:\Windows\System32\winlogon.exe Network Information: Workstation Name: LTRANPHD Source Network Address: 127.0.0.1 Source Port: 0 Detailed Authentication Information: Logon Process: User32 Authentication Package: Negotiate Transited Services: - Package Name (NTLM only): - Key Length: 0 This event is generated when a logon session is created. It is generated on the computer that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service such as the Server service, or a local process such as Winlogon.exe or Services.exe. The logon type field indicates the kind of logon that occurred. The most common types are 2 (interactive) and 3 (network). The New Logon fields indicate the account for whom the new logon was created, i.e. the account that was logged on. The network fields indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impersonation level field indicates the extent to which a process in the logon session can impersonate. The authentication information fields provide detailed information about this specific logon request. - Logon GUID is a unique identifier that can be used to correlate this event with a KDC event. - Transited services indicate which intermediate services have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length

					indicates the length of the generated session key. This will be 0 if no session key was requested.
Security	Audit Success	12544	2015-04-25 07:22:40	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: LTRANPHD$ Account Domain: WORKGROUP Logon ID: 0x3e7 Logon Type: 2 Impersonation Level: %%1833 New Logon: Security ID: S-1-5-21-1888849264-3803429180-4108621888-1001 Account Name: Liem Account Domain: LTRANPHD Logon ID: 0x1a88d Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x204 Process Name: C:\Windows\System32\winlogon.exe Network Information: Workstation Name: LTRANPHD Source Network Address: 127.0.0.1 Source Port: 0 Detailed Authentication Information: Logon Process: User32 Authentication Package: Negotiate Transited Services: - Package Name (NTLM only): - Key Length: 0 This event is generated when a logon session is created. It is generated on the computer that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service such as the Server service, or a local process such as Winlogon.exe or Services.exe. The logon type field indicates the kind of logon that occurred. The most common types are 2 (interactive) and 3 (network). The New Logon fields indicate the account for whom the new logon was created, i.e. the account that was logged on. The network fields indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impersonation level field indicates the extent to which a process in the logon session can impersonate. The authentication information fields provide detailed information about this specific logon request. - Logon GUID is a unique identifier that can be used to correlate this event with a KDC event. - Transited services indicate which intermediate services have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indicates the length of the generated session key. This will be 0 if no session key was requested.
Security	Audit Success	12544	2015-04-25 07:22:40	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: LTRANPHD$ Account Domain: WORKGROUP Logon ID: 0x3e7 Logon Type: 5 Impersonation Level: %%1833 New Logon: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Logon ID: 0x3e7 Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x234 Process Name: C:\Windows\System32\services.exe Network Information: Workstation Name: Source Network Address: - Source Port: - Detailed Authentication Information: Logon Process: Advapi Authentication Package: Negotiate Transited Services: - Package Name (NTLM only): - Key Length: 0 This event is generated when a logon session is created. It is generated on the computer that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service such as the Server service, or a local process such as Winlogon.exe or Services.exe. The logon type field indicates the kind of logon that occurred. The most common types are 2 (interactive) and 3 (network). The New Logon fields indicate the account for whom the new logon was created, i.e. the account that was logged on. The network fields indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impersonation level field indicates the extent to which a process in the logon session can impersonate. The authentication information fields provide detailed information about this specific logon request. - Logon GUID is a unique identifier that can be used to correlate this event with a KDC event. - Transited services indicate which intermediate services have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indicates the length of the generated session key. This will be 0 if no session key was requested.
Security	Audit Success	12548	2015-04-25 07:22:40	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-21-1888849264-3803429180-4108621888-1001 Account Name: Liem Account Domain: LTRANPHD Logon ID: 0x1a85a Privileges: SeSecurityPrivilege SeTakeOwnershipPrivilege SeLoadDriverPrivilege SeBackupPrivilege SeRestorePrivilege SeDebugPrivilege SeSystemEnvironmentPrivilege SeImpersonatePrivilege
Security	Audit Success	12548	2015-04-25 07:22:40	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Logon ID: 0x3e7 Privileges: SeAssignPrimaryTokenPrivilege SeTcbPrivilege SeSecurityPrivilege SeTakeOwnershipPrivilege SeLoadDriverPrivilege SeBackupPrivilege SeRestorePrivilege SeDebugPrivilege SeAuditPrivilege SeSystemEnvironmentPrivilege SeImpersonatePrivilege
Security	Audit Success	13824	2015-04-25 07:22:42	Microsoft-Windows-Security-Auditing	4797: An attempt was made to query the existence of a blank password for an account. Subject: Security ID: S-1-5-21-1888849264-3803429180-4108621888-1001 Account Name: Liem Account Domain: LTRANPHD Logon ID: 0x1a88d Additional Information: Caller Workstation: LTRANPHD Target Account Name: Administrator Target Account Domain: LTRANPHD
Security	Audit Success	13824	2015-04-25 07:22:42	Microsoft-Windows-Security-Auditing	4797: An attempt was made to query the existence of a blank password for an account. Subject: Security ID: S-1-5-21-1888849264-3803429180-4108621888-1001 Account Name: Liem Account Domain: LTRANPHD Logon ID: 0x1a88d Additional Information: Caller Workstation: LTRANPHD Target Account Name: Guest Target Account Domain: LTRANPHD
Security	Audit Success	13824	2015-04-25 07:22:42	Microsoft-Windows-Security-Auditing	4797: An attempt was made to query the existence of a blank password for an account. Subject: Security ID: S-1-5-21-1888849264-3803429180-4108621888-1001 Account Name: Liem Account Domain: LTRANPHD Logon ID: 0x1a88d Additional Information: Caller Workstation: LTRANPHD Target Account Name: Administrator Target Account Domain: LTRANPHD
Security	Audit Success	13824	2015-04-25 07:22:42	Microsoft-Windows-Security-Auditing	4797: An attempt was made to query the existence of a blank password for an account. Subject: Security ID: S-1-5-21-1888849264-3803429180-4108621888-1001 Account Name: Liem Account Domain: LTRANPHD Logon ID: 0x1a88d Additional Information: Caller Workstation: LTRANPHD Target Account Name: Guest Target Account Domain: LTRANPHD
Security	Audit	13824	2015-04-25	Microsoft-Windows-Security-	4797: An attempt was made to query the existence of a blank password for an account. Subject: Security ID: S-1-5-19 Account Name: LOCAL SERVICE Account Domain: NT AUTHORITY Logon ID: 0x3e5 Additional

	Success		07:22:51	Auditing	Information: Caller Workstation: LTRANPHD Target Account Name: Administrator Target Account Domain: LTRANPHD
Security	Audit Success	13824	2015-04-25 07:22:51	Microsoft-Windows-Security-Auditing	4797: An attempt was made to query the existence of a blank password for an account. Subject: Security ID: S-1-5-19 Account Name: LOCAL SERVICE Account Domain: NT AUTHORITY Logon ID: 0x3e5 Additional Information: Caller Workstation: LTRANPHD Target Account Name: Administrator Target Account Domain: LTRANPHD
Security	Audit Success	13824	2015-04-25 07:22:51	Microsoft-Windows-Security-Auditing	4797: An attempt was made to query the existence of a blank password for an account. Subject: Security ID: S-1-5-19 Account Name: LOCAL SERVICE Account Domain: NT AUTHORITY Logon ID: 0x3e5 Additional Information: Caller Workstation: LTRANPHD Target Account Name: Guest Target Account Domain: LTRANPHD
Security	Audit Success	13824	2015-04-25 07:22:51	Microsoft-Windows-Security-Auditing	4797: An attempt was made to query the existence of a blank password for an account. Subject: Security ID: S-1-5-19 Account Name: LOCAL SERVICE Account Domain: NT AUTHORITY Logon ID: 0x3e5 Additional Information: Caller Workstation: LTRANPHD Target Account Name: Guest Target Account Domain: LTRANPHD
Security	Audit Success	13824	2015-04-25 07:22:51	Microsoft-Windows-Security-Auditing	4797: An attempt was made to query the existence of a blank password for an account. Subject: Security ID: S-1-5-19 Account Name: LOCAL SERVICE Account Domain: NT AUTHORITY Logon ID: 0x3e5 Additional Information: Caller Workstation: LTRANPHD Target Account Name: Liem Target Account Domain: LTRANPHD
Security	Audit Success	13824	2015-04-25 07:22:51	Microsoft-Windows-Security-Auditing	4797: An attempt was made to query the existence of a blank password for an account. Subject: Security ID: S-1-5-19 Account Name: LOCAL SERVICE Account Domain: NT AUTHORITY Logon ID: 0x3e5 Additional Information: Caller Workstation: LTRANPHD Target Account Name: Liem Target Account Domain: LTRANPHD
Security	Audit Success	13824	2015-04-25 07:22:51	Microsoft-Windows-Security-Auditing	4797: An attempt was made to query the existence of a blank password for an account. Subject: Security ID: S-1-5-19 Account Name: LOCAL SERVICE Account Domain: NT AUTHORITY Logon ID: 0x3e5 Additional Information: Caller Workstation: LTRANPHD Target Account Name: Liem Target Account Domain: LTRANPHD
Security	Audit Success	13824	2015-04-25 07:22:51	Microsoft-Windows-Security-Auditing	4797: An attempt was made to query the existence of a blank password for an account. Subject: Security ID: S-1-5-19 Account Name: LOCAL SERVICE Account Domain: NT AUTHORITY Logon ID: 0x3e5 Additional Information: Caller Workstation: LTRANPHD Target Account Name: Liem Target Account Domain: LTRANPHD
Security	Audit Success	12544	2015-04-25 07:27:39	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: LTRANPHD$ Account Domain: WORKGROUP Logon ID: 0x3e7 Logon Type: 5 Impersonation Level: %%1833 New Logon: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Logon ID: 0x3e7 Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x234 Process Name: C:\Windows\System32\services.exe Network Information: Workstation Name: Source Network Address: - Source Port: - Detailed Authentication Information: Logon Process: Advapi Authentication Package: Negotiate Transited Services: - Package Name (NTLM only): - Key Length: 0 This event is generated when a logon session is created. It is generated on the computer that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service such as the Server service, or a local process such as Winlogon.exe or Services.exe. The logon type field indicates the kind of logon that occurred. The most common types are 2 (interactive) and 3 (network). The New Logon fields indicate the account for whom the new logon was created, i.e. the account that was logged on. The network fields indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impersonation level field indicates the extent to which a process in the logon session can impersonate. The authentication information fields provide detailed information about this specific logon request. - Logon GUID is a unique identifier that can be used to correlate this event with a KDC event. - Transited services indicate which intermediate services have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indicates the length of the generated session key. This will be 0 if no session key was requested.
Security	Audit Success	12548	2015-04-25 07:27:39	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Logon ID: 0x3e7 Privileges: SeAssignPrimaryTokenPrivilege SeTcbPrivilege SeSecurityPrivilege SeTakeOwnershipPrivilege SeLoadDriverPrivilege SeBackupPrivilege SeRestorePrivilege SeDebugPrivilege SeAuditPrivilege SeSystemEnvironmentPrivilege SeImpersonatePrivilege
Security	Audit Success	12544	2015-04-25 07:27:40	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: LTRANPHD$ Account Domain: WORKGROUP Logon ID: 0x3e7 Logon Type: 5 Impersonation Level: %%1833 New Logon: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Logon ID: 0x3e7 Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x234 Process Name: C:\Windows\System32\services.exe Network Information: Workstation Name: Source Network Address: - Source Port: - Detailed Authentication Information: Logon Process: Advapi Authentication Package: Negotiate Transited Services: - Package Name (NTLM only): - Key Length: 0 This event is generated when a logon session is created. It is generated on the computer that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service such as the Server service, or a local process such as Winlogon.exe or Services.exe. The logon type field indicates the kind of logon that occurred. The most common types are 2 (interactive) and 3 (network). The New Logon fields indicate the account for whom the new logon was created, i.e. the account that was logged on. The network fields indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impersonation level field indicates the extent to which a process in the logon session can impersonate. The authentication information fields provide detailed information about this specific logon request. - Logon GUID is a unique identifier that can be used to correlate this event with a KDC event. - Transited services indicate which intermediate services have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indicates the length of the generated

					session key. This will be 0 if no session key was requested.
Security	Audit Success	12548	2015-04-25 07:27:40	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Logon ID: 0x3e7 Privileges: SeAssignPrimaryTokenPrivilege SeTcbPrivilege SeSecurityPrivilege SeTakeOwnershipPrivilege SeLoadDriverPrivilege SeBackupPrivilege SeRestorePrivilege SeDebugPrivilege SeAuditPrivilege SeSystemEnvironmentPrivilege SeImpersonatePrivilege
Security	Audit Success	12288	2015-04-25 07:52:52	Microsoft-Windows-Security-Auditing	4608: Windows is starting up. This event is logged when LSASS.EXE starts and the auditing subsystem is initialized.
Security	Audit Success	12544	2015-04-25 07:52:52	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-0-0 Account Name: - Account Domain: - Logon ID: 0x0 Logon Type: 0 Impersonation Level: - New Logon: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Logon ID: 0x3e7 Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x4 Process Name: Network Information: Workstation Name: - Source Network Address: - Source Port: - Detailed Authentication Information: Logon Process: - Authentication Package: - Transited Services: - Package Name (NTLM only): - Key Length: 0 This event is generated when a logon session is created. It is generated on the computer that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service such as the Server service, or a local process such as Winlogon.exe or Services.exe. The logon type field indicates the kind of logon that occurred. The most common types are 2 (interactive) and 3 (network). The New Logon fields indicate the account for whom the new logon was created, i.e. the account that was logged on. The network fields indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impersonation level field indicates the extent to which a process in the logon session can impersonate. The authentication information fields provide detailed information about this specific logon request. - Logon GUID is a unique identifier that can be used to correlate this event with a KDC event. - Transited services indicate which intermediate services have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indicates the length of the generated session key. This will be 0 if no session key was requested.
Security	Audit Success	12544	2015-04-25 07:52:52	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: LTRANPHD$ Account Domain: WORKGROUP Logon ID: 0x3e7 Logon Type: 5 Impersonation Level: %%1833 New Logon: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Logon ID: 0x3e7 Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x228 Process Name: C:\Windows\System32\services.exe Network Information: Workstation Name: Source Network Address: - Source Port: - Detailed Authentication Information: Logon Process: Advapi Authentication Package: Negotiate Transited Services: - Package Name (NTLM only): - Key Length: 0 This event is generated when a logon session is created. It is generated on the computer that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service such as the Server service, or a local process such as Winlogon.exe or Services.exe. The logon type field indicates the kind of logon that occurred. The most common types are 2 (interactive) and 3 (network). The New Logon fields indicate the account for whom the new logon was created, i.e. the account that was logged on. The network fields indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impersonation level field indicates the extent to which a process in the logon session can impersonate. The authentication information fields provide detailed information about this specific logon request. - Logon GUID is a unique identifier that can be used to correlate this event with a KDC event. - Transited services indicate which intermediate services have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indicates the length of the generated session key. This will be 0 if no session key was requested.
Security	Audit Success	12544	2015-04-25 07:52:52	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: LTRANPHD$ Account Domain: WORKGROUP Logon ID: 0x3e7 Logon Type: 5 Impersonation Level: %%1833 New Logon: Security ID: S-1-5-20 Account Name: NETWORK SERVICE Account Domain: NT AUTHORITY Logon ID: 0x3e4 Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x228 Process Name: C:\Windows\System32\services.exe Network Information: Workstation Name: Source Network Address: - Source Port: - Detailed Authentication Information: Logon Process: Advapi Authentication Package: Negotiate Transited Services: - Package Name (NTLM only): - Key Length: 0 This event is generated when a logon session is created. It is generated on the computer that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service such as the Server service, or a local process such as Winlogon.exe or Services.exe. The logon type field indicates the kind of logon that occurred. The most common types are 2 (interactive) and 3 (network). The New Logon fields indicate the account for whom the new logon was created, i.e. the account that was logged on. The network fields indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impersonation level field indicates the extent to which a process in the logon session can impersonate. The authentication information fields provide detailed information about this specific logon request. - Logon GUID is a unique identifier that can be used to correlate this event with a KDC event. - Transited services indicate which intermediate services have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indicates the length of the generated session key. This will be 0 if no session key was requested.
					4648: A logon was attempted using explicit credentials. Subject: Security ID: S-1-5-18 Account Name: LTRANPHD$ Account Domain: WORKGROUP Logon ID: 0x3e7 Logon GUID: {00000000-0000-0000-0000-

Security	Audit Success	12544	2015-04-25 07:52:52	Microsoft-Windows-Security-Auditing	000000000000} Account Whose Credentials Were Used: Account Name: DWM-1 Account Domain: Window Manager Logon GUID: {00000000-0000-0000-0000-000000000000} Target Server: Target Server Name: localhost Additional Information: localhost Process Information: Process ID: 0x20c Process Name: C:\Windows\System32\winlogon.exe Network Information: Network Address: - Port: - This event is generated when a process attempts to log on an account by explicitly specifying that account's credentials. This most commonly occurs in batch-type configurations such as scheduled tasks, or when using the RUNAS command.
Security	Audit Success	12544	2015-04-25 07:52:52	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: LTRANPHD$ Account Domain: WORKGROUP Logon ID: 0x3e7 Logon Type: 2 Impersonation Level: %%1833 New Logon: Security ID: S-1-5-90-1 Account Name: DWM-1 Account Domain: Window Manager Logon ID: 0xd6eb Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x20c Process Name: C:\Windows\System32\winlogon.exe Network Information: Workstation Name: Source Network Address: - Source Port: - Detailed Authentication Information: Logon Process: Advapi Authentication Package: Negotiate Transited Services: - Package Name (NTLM only): - Key Length: 0 This event is generated when a logon session is created. It is generated on the computer that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service such as the Server service, or a local process such as Winlogon.exe or Services.exe. The logon type field indicates the kind of logon that occurred. The most common types are 2 (interactive) and 3 (network). The New Logon fields indicate the account for whom the new logon was created, i.e. the account that was logged on. The network fields indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impersonation level field indicates the extent to which a process in the logon session can impersonate. The authentication information fields provide detailed information about this specific logon request. - Logon GUID is a unique identifier that can be used to correlate this event with a KDC event. - Transited services indicate which intermediate services have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indicates the length of the generated session key. This will be 0 if no session key was requested.
Security	Audit Success	12544	2015-04-25 07:52:52	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: LTRANPHD$ Account Domain: WORKGROUP Logon ID: 0x3e7 Logon Type: 2 Impersonation Level: %%1833 New Logon: Security ID: S-1-5-90-1 Account Name: DWM-1 Account Domain: Window Manager Logon ID: 0xd708 Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x20c Process Name: C:\Windows\System32\winlogon.exe Network Information: Workstation Name: Source Network Address: - Source Port: - Detailed Authentication Information: Logon Process: Advapi Authentication Package: Negotiate Transited Services: - Package Name (NTLM only): - Key Length: 0 This event is generated when a logon session is created. It is generated on the computer that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service such as the Server service, or a local process such as Winlogon.exe or Services.exe. The logon type field indicates the kind of logon that occurred. The most common types are 2 (interactive) and 3 (network). The New Logon fields indicate the account for whom the new logon was created, i.e. the account that was logged on. The network fields indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impersonation level field indicates the extent to which a process in the logon session can impersonate. The authentication information fields provide detailed information about this specific logon request. - Logon GUID is a unique identifier that can be used to correlate this event with a KDC event. - Transited services indicate which intermediate services have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indicates the length of the generated session key. This will be 0 if no session key was requested.
Security	Audit Success	12544	2015-04-25 07:52:52	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: LTRANPHD$ Account Domain: WORKGROUP Logon ID: 0x3e7 Logon Type: 5 Impersonation Level: %%1833 New Logon: Security ID: S-1-5-19 Account Name: LOCAL SERVICE Account Domain: NT AUTHORITY Logon ID: 0x3e5 Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x228 Process Name: C:\Windows\System32\services.exe Network Information: Workstation Name: Source Network Address: - Source Port: - Detailed Authentication Information: Logon Process: Advapi Authentication Package: Negotiate Transited Services: - Package Name (NTLM only): - Key Length: 0 This event is generated when a logon session is created. It is generated on the computer that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service such as the Server service, or a local process such as Winlogon.exe or Services.exe. The logon type field indicates the kind of logon that occurred. The most common types are 2 (interactive) and 3 (network). The New Logon fields indicate the account for whom the new logon was created, i.e. the account that was logged on. The network fields indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impersonation level field indicates the extent to which a process in the logon session can impersonate. The authentication information fields provide detailed information about this specific logon request. - Logon GUID is a unique identifier that can be used to correlate this event with a KDC event. - Transited services indicate which intermediate services have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indicates the length of the generated session key. This will be 0 if no session key was requested.
					4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: LTRANPHD$ Account Domain: WORKGROUP Logon ID: 0x3e7 Logon Type: 5 Impersonation Level: %%1833 New Logon: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Logon ID: 0x3e7 Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x228 Process Name:

Security	Audit Success	12544	2015-04-25 07:52:52	Microsoft-Windows-Security-Auditing	C:\Windows\System32\services.exe Network Information: Workstation Name: Source Network Address: - Source Port: - Detailed Authentication Information: Logon Process: Advapi Authentication Package: Negotiate Transited Services: - Package Name (NTLM only): - Key Length: 0 This event is generated when a logon session is created. It is generated on the computer that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service such as the Server service, or a local process such as Winlogon.exe or Services.exe. The logon type field indicates the kind of logon that occurred. The most common types are 2 (interactive) and 3 (network). The New Logon fields indicate the account for whom the new logon was created, i.e. the account that was logged on. The network fields indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impersonation level field indicates the extent to which a process in the logon session can impersonate. The authentication information fields provide detailed information about this specific logon request. - Logon GUID is a unique identifier that can be used to correlate this event with a KDC event. - Transited services indicate which intermediate services have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indicates the length of the generated session key. This will be 0 if no session key was requested.
Security	Audit Success	12544	2015-04-25 07:52:52	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: LTRANPHD$ Account Domain: WORKGROUP Logon ID: 0x3e7 Logon Type: 5 Impersonation Level: %%1833 New Logon: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Logon ID: 0x3e7 Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x228 Process Name: C:\Windows\System32\services.exe Network Information: Workstation Name: Source Network Address: - Source Port: - Detailed Authentication Information: Logon Process: Advapi Authentication Package: Negotiate Transited Services: - Package Name (NTLM only): - Key Length: 0 This event is generated when a logon session is created. It is generated on the computer that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service such as the Server service, or a local process such as Winlogon.exe or Services.exe. The logon type field indicates the kind of logon that occurred. The most common types are 2 (interactive) and 3 (network). The New Logon fields indicate the account for whom the new logon was created, i.e. the account that was logged on. The network fields indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impersonation level field indicates the extent to which a process in the logon session can impersonate. The authentication information fields provide detailed information about this specific logon request. - Logon GUID is a unique identifier that can be used to correlate this event with a KDC event. - Transited services indicate which intermediate services have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indicates the length of the generated session key. This will be 0 if no session key was requested.
Security	Audit Success	12548	2015-04-25 07:52:52	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Logon ID: 0x3e7 Privileges: SeAssignPrimaryTokenPrivilege SeTcbPrivilege SeSecurityPrivilege SeTakeOwnershipPrivilege SeLoadDriverPrivilege SeBackupPrivilege SeRestorePrivilege SeDebugPrivilege SeAuditPrivilege SeSystemEnvironmentPrivilege SeImpersonatePrivilege
Security	Audit Success	12548	2015-04-25 07:52:52	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-20 Account Name: NETWORK SERVICE Account Domain: NT AUTHORITY Logon ID: 0x3e4 Privileges: SeAssignPrimaryTokenPrivilege SeAuditPrivilege SeImpersonatePrivilege
Security	Audit Success	12548	2015-04-25 07:52:52	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-90-1 Account Name: DWM-1 Account Domain: Window Manager Logon ID: 0xd6eb Privileges: SeAssignPrimaryTokenPrivilege SeAuditPrivilege SeImpersonatePrivilege
Security	Audit Success	12548	2015-04-25 07:52:52	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-90-1 Account Name: DWM-1 Account Domain: Window Manager Logon ID: 0xd708 Privileges: SeAssignPrimaryTokenPrivilege SeAuditPrivilege
Security	Audit Success	12548	2015-04-25 07:52:52	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-19 Account Name: LOCAL SERVICE Account Domain: NT AUTHORITY Logon ID: 0x3e5 Privileges: SeAssignPrimaryTokenPrivilege SeAuditPrivilege SeImpersonatePrivilege
Security	Audit Success	12548	2015-04-25 07:52:52	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Logon ID: 0x3e7 Privileges: SeAssignPrimaryTokenPrivilege SeTcbPrivilege SeSecurityPrivilege SeTakeOwnershipPrivilege SeLoadDriverPrivilege SeBackupPrivilege SeRestorePrivilege SeDebugPrivilege SeAuditPrivilege SeSystemEnvironmentPrivilege SeImpersonatePrivilege
Security	Audit Success	12548	2015-04-25 07:52:52	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Logon ID: 0x3e7 Privileges: SeAssignPrimaryTokenPrivilege SeTcbPrivilege SeSecurityPrivilege SeTakeOwnershipPrivilege SeLoadDriverPrivilege SeBackupPrivilege SeRestorePrivilege SeDebugPrivilege SeAuditPrivilege SeSystemEnvironmentPrivilege SeImpersonatePrivilege
Security	Audit Success	13568	2015-04-25 07:52:52	Microsoft-Windows-Security-Auditing	4902: The Per-user audit policy table was created. Number of Elements: 0 Policy ID: 0x9e3c
Security	Audit Success	12292	2015-04-25 07:52:53	Microsoft-Windows-Security-Auditing	5033: The Windows Firewall Driver started successfully.
			2015-04-		

Security	Audit Success	12292	25 07:52:53	Microsoft-Windows-Security-Auditing	5024: The Windows Firewall service started successfully.
Security	Audit Success	12544	2015-04-25 07:52:53	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: LTRANPHD$ Account Domain: WORKGROUP Logon ID: 0x3e7 Logon Type: 5 Impersonation Level: %%1833 New Logon: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Logon ID: 0x3e7 Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x228 Process Name: C:\Windows\System32\services.exe Network Information: Workstation Name: Source Network Address: - Source Port: - Detailed Authentication Information: Logon Process: Advapi Authentication Package: Negotiate Transited Services: - Package Name (NTLM only): - Key Length: 0 This event is generated when a logon session is created. It is generated on the computer that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service such as the Server service, or a local process such as Winlogon.exe or Services.exe. The logon type field indicates the kind of logon that occurred. The most common types are 2 (interactive) and 3 (network). The New Logon fields indicate the account for whom the new logon was created, i.e. the account that was logged on. The network fields indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impersonation level field indicates the extent to which a process in the logon session can impersonate. The authentication information fields provide detailed information about this specific logon request. - Logon GUID is a unique identifier that can be used to correlate this event with a KDC event. - Transited services indicate which intermediate services have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indicates the length of the generated session key. This will be 0 if no session key was requested.
Security	Audit Success	12544	2015-04-25 07:52:53	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: LTRANPHD$ Account Domain: WORKGROUP Logon ID: 0x3e7 Logon Type: 5 Impersonation Level: %%1833 New Logon: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Logon ID: 0x3e7 Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x228 Process Name: C:\Windows\System32\services.exe Network Information: Workstation Name: Source Network Address: - Source Port: - Detailed Authentication Information: Logon Process: Advapi Authentication Package: Negotiate Transited Services: - Package Name (NTLM only): - Key Length: 0 This event is generated when a logon session is created. It is generated on the computer that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service such as the Server service, or a local process such as Winlogon.exe or Services.exe. The logon type field indicates the kind of logon that occurred. The most common types are 2 (interactive) and 3 (network). The New Logon fields indicate the account for whom the new logon was created, i.e. the account that was logged on. The network fields indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impersonation level field indicates the extent to which a process in the logon session can impersonate. The authentication information fields provide detailed information about this specific logon request. - Logon GUID is a unique identifier that can be used to correlate this event with a KDC event. - Transited services indicate which intermediate services have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indicates the length of the generated session key. This will be 0 if no session key was requested.
Security	Audit Success	12548	2015-04-25 07:52:53	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Logon ID: 0x3e7 Privileges: SeAssignPrimaryTokenPrivilege SeTcbPrivilege SeSecurityPrivilege SeTakeOwnershipPrivilege SeLoadDriverPrivilege SeBackupPrivilege SeRestorePrivilege SeDebugPrivilege SeAuditPrivilege SeSystemEnvironmentPrivilege SeImpersonatePrivilege
Security	Audit Success	12548	2015-04-25 07:52:53	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Logon ID: 0x3e7 Privileges: SeAssignPrimaryTokenPrivilege SeTcbPrivilege SeSecurityPrivilege SeTakeOwnershipPrivilege SeLoadDriverPrivilege SeBackupPrivilege SeRestorePrivilege SeDebugPrivilege SeAuditPrivilege SeSystemEnvironmentPrivilege SeImpersonatePrivilege
Security	Audit Success	12544	2015-04-25 07:52:54	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: LTRANPHD$ Account Domain: WORKGROUP Logon ID: 0x3e7 Logon Type: 5 Impersonation Level: %%1833 New Logon: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Logon ID: 0x3e7 Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x228 Process Name: C:\Windows\System32\services.exe Network Information: Workstation Name: Source Network Address: - Source Port: - Detailed Authentication Information: Logon Process: Advapi Authentication Package: Negotiate Transited Services: - Package Name (NTLM only): - Key Length: 0 This event is generated when a logon session is created. It is generated on the computer that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service such as the Server service, or a local process such as Winlogon.exe or Services.exe. The logon type field indicates the kind of logon that occurred. The most common types are 2 (interactive) and 3 (network). The New Logon fields indicate the account for whom the new logon was created, i.e. the account that was logged on. The network fields indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impersonation level field indicates the extent to which a process in the logon session can impersonate. The authentication information fields provide detailed information about this specific logon request. - Logon GUID is a unique identifier that can be used to correlate this event with a KDC event. - Transited services indicate which intermediate services have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indicates the length of the generated

					session key. This will be 0 if no session key was requested.
Security	Audit Success	12544	2015-04-25 07:52:54	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-0-0 Account Name: - Account Domain: - Logon ID: 0x0 Logon Type: 3 Impersonation Level: %%1833 New Logon: Security ID: S-1-5-7 Account Name: ANONYMOUS LOGON Account Domain: NT AUTHORITY Logon ID: 0x194ce Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x0 Process Name: - Network Information: Workstation Name: Source Network Address: - Source Port: - Detailed Authentication Information: Logon Process: NtLmSsp Authentication Package: NTLM Transited Services: - Package Name (NTLM only): NTLM V1 Key Length: 0 This event is generated when a logon session is created. It is generated on the computer that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service such as the Server service, or a local process such as Winlogon.exe or Services.exe. The logon type field indicates the kind of logon that occurred. The most common types are 2 (interactive) and 3 (network). The New Logon fields indicate the account for whom the new logon was created, i.e. the account that was logged on. The network fields indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impersonation level field indicates the extent to which a process in the logon session can impersonate. The authentication information fields provide detailed information about this specific logon request. - Logon GUID is a unique identifier that can be used to correlate this event with a KDC event. - Transited services indicate which intermediate services have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indicates the length of the generated session key. This will be 0 if no session key was requested.
Security	Audit Success	12548	2015-04-25 07:52:54	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Logon ID: 0x3e7 Privileges: SeAssignPrimaryTokenPrivilege SeTcbPrivilege SeSecurityPrivilege SeTakeOwnershipPrivilege SeLoadDriverPrivilege SeBackupPrivilege SeRestorePrivilege SeDebugPrivilege SeAuditPrivilege SeSystemEnvironmentPrivilege SeImpersonatePrivilege
Security	Audit Success	12544	2015-04-25 07:52:59	Microsoft-Windows-Security-Auditing	4648: A logon was attempted using explicit credentials. Subject: Security ID: S-1-5-18 Account Name: LTRANPHD$ Account Domain: WORKGROUP Logon ID: 0x3e7 Logon GUID: {00000000-0000-0000-0000-000000000000} Account Whose Credentials Were Used: Account Name: Liem Account Domain: LTRANPHD Logon GUID: {00000000-0000-0000-0000-000000000000} Target Server: Target Server Name: localhost Additional Information: localhost Process Information: Process ID: 0x20c Process Name: C:\Windows\System32\winlogon.exe Network Information: Network Address: 127.0.0.1 Port: 0 This event is generated when a process attempts to log on an account by explicitly specifying that account's credentials. This most commonly occurs in batch-type configurations such as scheduled tasks, or when using the RUNAS command.
Security	Audit Success	12544	2015-04-25 07:52:59	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: LTRANPHD$ Account Domain: WORKGROUP Logon ID: 0x3e7 Logon Type: 2 Impersonation Level: %%1833 New Logon: Security ID: S-1-5-21-1888849264-3803429180-4108621888-1001 Account Name: Liem Account Domain: LTRANPHD Logon ID: 0x1e830 Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x20c Process Name: C:\Windows\System32\winlogon.exe Network Information: Workstation Name: LTRANPHD Source Network Address: 127.0.0.1 Source Port: 0 Detailed Authentication Information: Logon Process: User32 Authentication Package: Negotiate Transited Services: - Package Name (NTLM only): - Key Length: 0 This event is generated when a logon session is created. It is generated on the computer that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service such as the Server service, or a local process such as Winlogon.exe or Services.exe. The logon type field indicates the kind of logon that occurred. The most common types are 2 (interactive) and 3 (network). The New Logon fields indicate the account for whom the new logon was created, i.e. the account that was logged on. The network fields indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impersonation level field indicates the extent to which a process in the logon session can impersonate. The authentication information fields provide detailed information about this specific logon request. - Logon GUID is a unique identifier that can be used to correlate this event with a KDC event. - Transited services indicate which intermediate services have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indicates the length of the generated session key. This will be 0 if no session key was requested.
Security	Audit Success	12544	2015-04-25 07:52:59	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: LTRANPHD$ Account Domain: WORKGROUP Logon ID: 0x3e7 Logon Type: 2 Impersonation Level: %%1833 New Logon: Security ID: S-1-5-21-1888849264-3803429180-4108621888-1001 Account Name: Liem Account Domain: LTRANPHD Logon ID: 0x1e889 Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x20c Process Name: C:\Windows\System32\winlogon.exe Network Information: Workstation Name: LTRANPHD Source Network Address: 127.0.0.1 Source Port: 0 Detailed Authentication Information: Logon Process: User32 Authentication Package: Negotiate Transited Services: - Package Name (NTLM only): - Key Length: 0 This event is generated when a logon session is created. It is generated on the computer that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service such as the Server service, or a local process such as Winlogon.exe or Services.exe. The logon type field indicates the kind of logon that occurred. The most common types are 2 (interactive) and 3 (network). The New Logon fields indicate the account for whom the new logon was created, i.e. the account that was logged on. The network fields indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impersonation level field indicates the extent to which a process in the logon session can impersonate. The authentication information fields provide detailed

					information about this specific logon request. - Logon GUID is a unique identifier that can be used to correlate this event with a KDC event. - Transited services indicate which intermediate services have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indicates the length of the generated session key. This will be 0 if no session key was requested.
Security	Audit Success	12544	2015-04-25 07:52:59	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: LTRANPHD$ Account Domain: WORKGROUP Logon ID: 0x3e7 Logon Type: 5 Impersonation Level: %%1833 New Logon: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Logon ID: 0x3e7 Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x228 Process Name: C:\Windows\System32\services.exe Network Information: Workstation Name: Source Network Address: - Source Port: - Detailed Authentication Information: Logon Process: Advapi Authentication Package: Negotiate Transited Services: - Package Name (NTLM only): - Key Length: 0 This event is generated when a logon session is created. It is generated on the computer that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service such as the Server service, or a local process such as Winlogon.exe or Services.exe. The logon type field indicates the kind of logon that occurred. The most common types are 2 (interactive) and 3 (network). The New Logon fields indicate the account for whom the new logon was created, i.e. the account that was logged on. The network fields indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impersonation level field indicates the extent to which a process in the logon session can impersonate. The authentication information fields provide detailed information about this specific logon request. - Logon GUID is a unique identifier that can be used to correlate this event with a KDC event. - Transited services indicate which intermediate services have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indicates the length of the generated session key. This will be 0 if no session key was requested.
Security	Audit Success	12548	2015-04-25 07:52:59	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-21-1888849264-3803429180-4108621888-1001 Account Name: Liem Account Domain: LTRANPHD Logon ID: 0x1e830 Privileges: SeSecurityPrivilege SeTakeOwnershipPrivilege SeLoadDriverPrivilege SeBackupPrivilege SeRestorePrivilege SeDebugPrivilege SeSystemEnvironmentPrivilege SeImpersonatePrivilege
Security	Audit Success	12548	2015-04-25 07:52:59	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Logon ID: 0x3e7 Privileges: SeAssignPrimaryTokenPrivilege SeTcbPrivilege SeSecurityPrivilege SeTakeOwnershipPrivilege SeLoadDriverPrivilege SeBackupPrivilege SeRestorePrivilege SeDebugPrivilege SeAuditPrivilege SeSystemEnvironmentPrivilege SeImpersonatePrivilege
Security	Audit Success	13824	2015-04-25 07:53:01	Microsoft-Windows-Security-Auditing	4797: An attempt was made to query the existence of a blank password for an account. Subject: Security ID: S-1-5-19 Account Name: LOCAL SERVICE Account Domain: NT AUTHORITY Logon ID: 0x3e5 Additional Information: Caller Workstation: LTRANPHD Target Account Name: Administrator Target Account Domain: LTRANPHD
Security	Audit Success	13824	2015-04-25 07:53:01	Microsoft-Windows-Security-Auditing	4797: An attempt was made to query the existence of a blank password for an account. Subject: Security ID: S-1-5-19 Account Name: LOCAL SERVICE Account Domain: NT AUTHORITY Logon ID: 0x3e5 Additional Information: Caller Workstation: LTRANPHD Target Account Name: Guest Target Account Domain: LTRANPHD
Security	Audit Success	13824	2015-04-25 07:53:01	Microsoft-Windows-Security-Auditing	4797: An attempt was made to query the existence of a blank password for an account. Subject: Security ID: S-1-5-19 Account Name: LOCAL SERVICE Account Domain: NT AUTHORITY Logon ID: 0x3e5 Additional Information: Caller Workstation: LTRANPHD Target Account Name: Liem Target Account Domain: LTRANPHD
Security	Audit Success	13824	2015-04-25 07:53:01	Microsoft-Windows-Security-Auditing	4797: An attempt was made to query the existence of a blank password for an account. Subject: Security ID: S-1-5-19 Account Name: LOCAL SERVICE Account Domain: NT AUTHORITY Logon ID: 0x3e5 Additional Information: Caller Workstation: LTRANPHD Target Account Name: Liem Target Account Domain: LTRANPHD
Security	Audit Success	13824	2015-04-25 07:53:01	Microsoft-Windows-Security-Auditing	4797: An attempt was made to query the existence of a blank password for an account. Subject: Security ID: S-1-5-21-1888849264-3803429180-4108621888-1001 Account Name: Liem Account Domain: LTRANPHD Logon ID: 0x1e889 Additional Information: Caller Workstation: LTRANPHD Target Account Name: Administrator Target Account Domain: LTRANPHD
Security	Audit Success	13824	2015-04-25 07:53:01	Microsoft-Windows-Security-Auditing	4797: An attempt was made to query the existence of a blank password for an account. Subject: Security ID: S-1-5-21-1888849264-3803429180-4108621888-1001 Account Name: Liem Account Domain: LTRANPHD Logon ID: 0x1e889 Additional Information: Caller Workstation: LTRANPHD Target Account Name: Guest Target Account Domain: LTRANPHD
Security	Audit Success	13824	2015-04-25 07:53:01	Microsoft-Windows-Security-Auditing	4797: An attempt was made to query the existence of a blank password for an account. Subject: Security ID: S-1-5-21-1888849264-3803429180-4108621888-1001 Account Name: Liem Account Domain: LTRANPHD Logon ID: 0x1e889 Additional Information: Caller Workstation: LTRANPHD Target Account Name: Administrator Target Account Domain: LTRANPHD
Security	Audit Success	13824	2015-04-25 07:53:01	Microsoft-Windows-Security-Auditing	4797: An attempt was made to query the existence of a blank password for an account. Subject: Security ID: S-1-5-21-1888849264-3803429180-4108621888-1001 Account Name: Liem Account Domain: LTRANPHD Logon ID: 0x1e889 Additional Information: Caller Workstation: LTRANPHD Target Account Name: Guest Target Account Domain: LTRANPHD
Security	Audit Success	13824	2015-04-25 07:55:17	Microsoft-Windows-Security-Auditing	4797: An attempt was made to query the existence of a blank password for an account. Subject: Security ID: S-1-5-21-1888849264-3803429180-4108621888-1001 Account Name: Liem Account Domain: LTRANPHD Logon ID: 0x1e889 Additional Information: Caller Workstation: LTRANPHD Target Account Name: Administrator Target Account Domain: LTRANPHD

Security	Audit Success	13824	2015-04-25 07:55:17	Microsoft-Windows-Security-Auditing	4797: An attempt was made to query the existence of a blank password for an account. Subject: Security ID: S-1-5-21-1888849264-3803429180-4108621888-1001 Account Name: Liem Account Domain: LTRANPHD Logon ID: 0x1e889 Additional Information: Caller Workstation: LTRANPHD Target Account Name: Guest Target Account Domain: LTRANPHD
Security	Audit Success	13824	2015-04-25 07:55:17	Microsoft-Windows-Security-Auditing	4797: An attempt was made to query the existence of a blank password for an account. Subject: Security ID: S-1-5-21-1888849264-3803429180-4108621888-1001 Account Name: Liem Account Domain: LTRANPHD Logon ID: 0x1e889 Additional Information: Caller Workstation: LTRANPHD Target Account Name: Administrator Target Account Domain: LTRANPHD
Security	Audit Success	13824	2015-04-25 07:55:17	Microsoft-Windows-Security-Auditing	4797: An attempt was made to query the existence of a blank password for an account. Subject: Security ID: S-1-5-21-1888849264-3803429180-4108621888-1001 Account Name: Liem Account Domain: LTRANPHD Logon ID: 0x1e889 Additional Information: Caller Workstation: LTRANPHD Target Account Name: Guest Target Account Domain: LTRANPHD
Security	Audit Success	12544	2015-04-25 08:04:24	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: LTRANPHD$ Account Domain: WORKGROUP Logon ID: 0x3e7 Logon Type: 5 Impersonation Level: %%1833 New Logon: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Logon ID: 0x3e7 Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x228 Process Name: C:\Windows\System32\services.exe Network Information: Workstation Name: Source Network Address: - Source Port: - Detailed Authentication Information: Logon Process: Advapi Authentication Package: Negotiate Transited Services: - Package Name (NTLM only): - Key Length: 0 This event is generated when a logon session is created. It is generated on the computer that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service such as the Server service, or a local process such as Winlogon.exe or Services.exe. The logon type field indicates the kind of logon that occurred. The most common types are 2 (interactive) and 3 (network). The New Logon fields indicate the account for whom the new logon was created, i.e. the account that was logged on. The network fields indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impersonation level field indicates the extent to which a process in the logon session can impersonate. The authentication information fields provide detailed information about this specific logon request. - Logon GUID is a unique identifier that can be used to correlate this event with a KDC event. - Transited services indicate which intermediate services have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indicates the length of the generated session key. This will be 0 if no session key was requested.
Security	Audit Success	12548	2015-04-25 08:04:24	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Logon ID: 0x3e7 Privileges: SeAssignPrimaryTokenPrivilege SeTcbPrivilege SeSecurityPrivilege SeTakeOwnershipPrivilege SeLoadDriverPrivilege SeBackupPrivilege SeRestorePrivilege SeDebugPrivilege SeAuditPrivilege SeSystemEnvironmentPrivilege SeImpersonatePrivilege
Security	Audit Success	12544	2015-04-25 08:04:26	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: LTRANPHD$ Account Domain: WORKGROUP Logon ID: 0x3e7 Logon Type: 5 Impersonation Level: %%1833 New Logon: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Logon ID: 0x3e7 Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x228 Process Name: C:\Windows\System32\services.exe Network Information: Workstation Name: Source Network Address: - Source Port: - Detailed Authentication Information: Logon Process: Advapi Authentication Package: Negotiate Transited Services: - Package Name (NTLM only): - Key Length: 0 This event is generated when a logon session is created. It is generated on the computer that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service such as the Server service, or a local process such as Winlogon.exe or Services.exe. The logon type field indicates the kind of logon that occurred. The most common types are 2 (interactive) and 3 (network). The New Logon fields indicate the account for whom the new logon was created, i.e. the account that was logged on. The network fields indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impersonation level field indicates the extent to which a process in the logon session can impersonate. The authentication information fields provide detailed information about this specific logon request. - Logon GUID is a unique identifier that can be used to correlate this event with a KDC event. - Transited services indicate which intermediate services have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indicates the length of the generated session key. This will be 0 if no session key was requested.
Security	Audit Success	12548	2015-04-25 08:04:26	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Logon ID: 0x3e7 Privileges: SeAssignPrimaryTokenPrivilege SeTcbPrivilege SeSecurityPrivilege SeTakeOwnershipPrivilege SeLoadDriverPrivilege SeBackupPrivilege SeRestorePrivilege SeDebugPrivilege SeAuditPrivilege SeSystemEnvironmentPrivilege SeImpersonatePrivilege
Security	Audit Success	12544	2015-04-25 08:14:39	Microsoft-Windows-Security-Auditing	4648: A logon was attempted using explicit credentials. Subject: Security ID: S-1-5-18 Account Name: LTRANPHD$ Account Domain: WORKGROUP Logon ID: 0x3e7 Logon GUID: {00000000-0000-0000-0000-000000000000} Account Whose Credentials Were Used: Account Name: Liem Account Domain: LTRANPHD Logon GUID: {00000000-0000-0000-0000-000000000000} Target Server: Target Server Name: localhost Additional Information: localhost Process Information: Process ID: 0x20c Process Name: C:\Windows\System32\winlogon.exe Network Information: Network Address: 127.0.0.1 Port: 0 This event is generated when a process attempts to log on an account by explicitly specifying that account's credentials. This most commonly occurs in batch-type configurations such as scheduled tasks, or when using the RUNAS

					command.
Security	Audit Success	12544	2015-04-25 08:14:39	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: LTRANPHD$ Account Domain: WORKGROUP Logon ID: 0x3e7 Logon Type: 7 Impersonation Level: %%1833 New Logon: Security ID: S-1-5-21-1888849264-3803429180-4108621888-1001 Account Name: Liem Account Domain: LTRANPHD Logon ID: 0xe8cf4d Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x20c Process Name: C:\Windows\System32\winlogon.exe Network Information: Workstation Name: LTRANPHD Source Network Address: 127.0.0.1 Source Port: 0 Detailed Authentication Information: Logon Process: User32 Authentication Package: Negotiate Transited Services: - Package Name (NTLM only): - Key Length: 0 This event is generated when a logon session is created. It is generated on the computer that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service such as the Server service, or a local process such as Winlogon.exe or Services.exe. The logon type field indicates the kind of logon that occurred. The most common types are 2 (interactive) and 3 (network). The New Logon fields indicate the account for whom the new logon was created, i.e. the account that was logged on. The network fields indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impersonation level field indicates the extent to which a process in the logon session can impersonate. The authentication information fields provide detailed information about this specific logon request. - Logon GUID is a unique identifier that can be used to correlate this event with a KDC event. - Transited services indicate which intermediate services have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indicates the length of the generated session key. This will be 0 if no session key was requested.
Security	Audit Success	12544	2015-04-25 08:14:39	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: LTRANPHD$ Account Domain: WORKGROUP Logon ID: 0x3e7 Logon Type: 7 Impersonation Level: %%1833 New Logon: Security ID: S-1-5-21-1888849264-3803429180-4108621888-1001 Account Name: Liem Account Domain: LTRANPHD Logon ID: 0xe8cf96 Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x20c Process Name: C:\Windows\System32\winlogon.exe Network Information: Workstation Name: LTRANPHD Source Network Address: 127.0.0.1 Source Port: 0 Detailed Authentication Information: Logon Process: User32 Authentication Package: Negotiate Transited Services: - Package Name (NTLM only): - Key Length: 0 This event is generated when a logon session is created. It is generated on the computer that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service such as the Server service, or a local process such as Winlogon.exe or Services.exe. The logon type field indicates the kind of logon that occurred. The most common types are 2 (interactive) and 3 (network). The New Logon fields indicate the account for whom the new logon was created, i.e. the account that was logged on. The network fields indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impersonation level field indicates the extent to which a process in the logon session can impersonate. The authentication information fields provide detailed information about this specific logon request. - Logon GUID is a unique identifier that can be used to correlate this event with a KDC event. - Transited services indicate which intermediate services have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indicates the length of the generated session key. This will be 0 if no session key was requested.
Security	Audit Success	12545	2015-04-25 08:14:39	Microsoft-Windows-Security-Auditing	4634: An account was logged off. Subject: Security ID: S-1-5-21-1888849264-3803429180-4108621888-1001 Account Name: Liem Account Domain: LTRANPHD Logon ID: 0xe8cf96 Logon Type: 7 This event is generated when a logon session is destroyed. It may be positively correlated with a logon event using the Logon ID value. Logon IDs are only unique between reboots on the same computer.
Security	Audit Success	12545	2015-04-25 08:14:39	Microsoft-Windows-Security-Auditing	4634: An account was logged off. Subject: Security ID: S-1-5-21-1888849264-3803429180-4108621888-1001 Account Name: Liem Account Domain: LTRANPHD Logon ID: 0xe8cf4d Logon Type: 7 This event is generated when a logon session is destroyed. It may be positively correlated with a logon event using the Logon ID value. Logon IDs are only unique between reboots on the same computer.
Security	Audit Success	12548	2015-04-25 08:14:39	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-21-1888849264-3803429180-4108621888-1001 Account Name: Liem Account Domain: LTRANPHD Logon ID: 0xe8cf4d Privileges: SeSecurityPrivilege SeTakeOwnershipPrivilege SeLoadDriverPrivilege SeBackupPrivilege SeRestorePrivilege SeDebugPrivilege SeSystemEnvironmentPrivilege SeImpersonatePrivilege
Security	Audit Success	12544	2015-04-25 08:24:45	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: LTRANPHD$ Account Domain: WORKGROUP Logon ID: 0x3e7 Logon Type: 5 Impersonation Level: %%1833 New Logon: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Logon ID: 0x3e7 Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x228 Process Name: C:\Windows\System32\services.exe Network Information: Workstation Name: Source Network Address: - Source Port: - Detailed Authentication Information: Logon Process: Advapi Authentication Package: Negotiate Transited Services: - Package Name (NTLM only): - Key Length: 0 This event is generated when a logon session is created. It is generated on the computer that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service such as the Server service, or a local process such as Winlogon.exe or Services.exe. The logon type field indicates the kind of logon that occurred. The most common types are 2 (interactive) and 3 (network). The New Logon fields indicate the account for whom the new logon was created, i.e. the account that was logged on. The network fields indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some

					cases. The impersonation level field indicates the extent to which a process in the logon session can impersonate. The authentication information fields provide detailed information about this specific logon request. - Logon GUID is a unique identifier that can be used to correlate this event with a KDC event. - Transited services indicate which intermediate services have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indicates the length of the generated session key. This will be 0 if no session key was requested.
Security	Audit Success	12548	2015-04-25 08:24:45	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Logon ID: 0x3e7 Privileges: SeAssignPrimaryTokenPrivilege SeTcbPrivilege SeSecurityPrivilege SeTakeOwnershipPrivilege SeLoadDriverPrivilege SeBackupPrivilege SeRestorePrivilege SeDebugPrivilege SeAuditPrivilege SeSystemEnvironmentPrivilege SeImpersonatePrivilege
Security	Audit Success	12544	2015-04-25 08:24:46	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: LTRANPHD$ Account Domain: WORKGROUP Logon ID: 0x3e7 Logon Type: 5 Impersonation Level: %%1833 New Logon: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Logon ID: 0x3e7 Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x228 Process Name: C:\Windows\System32\services.exe Network Information: Workstation Name: Source Network Address: - Source Port: - Detailed Authentication Information: Logon Process: Advapi Authentication Package: Negotiate Transited Services: - Package Name (NTLM only): - Key Length: 0 This event is generated when a logon session is created. It is generated on the computer that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service such as the Server service, or a local process such as Winlogon.exe or Services.exe. The logon type field indicates the kind of logon that occurred. The most common types are 2 (interactive) and 3 (network). The New Logon fields indicate the account for whom the new logon was created, i.e. the account that was logged on. The network fields indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impersonation level field indicates the extent to which a process in the logon session can impersonate. The authentication information fields provide detailed information about this specific logon request. - Logon GUID is a unique identifier that can be used to correlate this event with a KDC event. - Transited services indicate which intermediate services have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indicates the length of the generated session key. This will be 0 if no session key was requested.
Security	Audit Success	12548	2015-04-25 08:24:46	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Logon ID: 0x3e7 Privileges: SeAssignPrimaryTokenPrivilege SeTcbPrivilege SeSecurityPrivilege SeTakeOwnershipPrivilege SeLoadDriverPrivilege SeBackupPrivilege SeRestorePrivilege SeDebugPrivilege SeAuditPrivilege SeSystemEnvironmentPrivilege SeImpersonatePrivilege
Security	Audit Success	12544	2015-04-25 08:25:08	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: LTRANPHD$ Account Domain: WORKGROUP Logon ID: 0x3e7 Logon Type: 5 Impersonation Level: %%1833 New Logon: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Logon ID: 0x3e7 Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x228 Process Name: C:\Windows\System32\services.exe Network Information: Workstation Name: Source Network Address: - Source Port: - Detailed Authentication Information: Logon Process: Advapi Authentication Package: Negotiate Transited Services: - Package Name (NTLM only): - Key Length: 0 This event is generated when a logon session is created. It is generated on the computer that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service such as the Server service, or a local process such as Winlogon.exe or Services.exe. The logon type field indicates the kind of logon that occurred. The most common types are 2 (interactive) and 3 (network). The New Logon fields indicate the account for whom the new logon was created, i.e. the account that was logged on. The network fields indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impersonation level field indicates the extent to which a process in the logon session can impersonate. The authentication information fields provide detailed information about this specific logon request. - Logon GUID is a unique identifier that can be used to correlate this event with a KDC event. - Transited services indicate which intermediate services have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indicates the length of the generated session key. This will be 0 if no session key was requested.
Security	Audit Success	12548	2015-04-25 08:25:08	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Logon ID: 0x3e7 Privileges: SeAssignPrimaryTokenPrivilege SeTcbPrivilege SeSecurityPrivilege SeTakeOwnershipPrivilege SeLoadDriverPrivilege SeBackupPrivilege SeRestorePrivilege SeDebugPrivilege SeAuditPrivilege SeSystemEnvironmentPrivilege SeImpersonatePrivilege
Security	Audit Success	12544	2015-04-25	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: LTRANPHD$ Account Domain: WORKGROUP Logon ID: 0x3e7 Logon Type: 5 Impersonation Level: %%1833 New Logon: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Logon ID: 0x3e7 Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x228 Process Name: C:\Windows\System32\services.exe Network Information: Workstation Name: Source Network Address: - Source Port: - Detailed Authentication Information: Logon Process: Advapi Authentication Package: Negotiate Transited Services: - Package Name (NTLM only): - Key Length: 0 This event is generated when a logon session is created. It is generated on the computer that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service such as the Server service, or a local process such as Winlogon.exe or Services.exe. The logon type field indicates the kind of logon that occurred.

			08:25:38		The most common types are 2 (interactive) and 3 (network). The New Logon fields indicate the account for whom the new logon was created, i.e. the account that was logged on. The network fields indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impersonation level field indicates the extent to which a process in the logon session can impersonate. The authentication information fields provide detailed information about this specific logon request. - Logon GUID is a unique identifier that can be used to correlate this event with a KDC event. - Transited services indicate which intermediate services have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indicates the length of the generated session key. This will be 0 if no session key was requested.
Security	Audit Success	12548	2015-04-25 08:25:38	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Logon ID: 0x3e7 Privileges: SeAssignPrimaryTokenPrivilege SeTcbPrivilege SeSecurityPrivilege SeTakeOwnershipPrivilege SeLoadDriverPrivilege SeBackupPrivilege SeRestorePrivilege SeDebugPrivilege SeAuditPrivilege SeSystemEnvironmentPrivilege SeImpersonatePrivilege
Security	Audit Success	12288	2015-04-25 08:44:54	Microsoft-Windows-Security-Auditing	4608: Windows is starting up. This event is logged when LSASS.EXE starts and the auditing subsystem is initialized.
Security	Audit Success	12544	2015-04-25 08:44:54	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-0-0 Account Name: - Account Domain: - Logon ID: 0x0 Logon Type: 0 Impersonation Level: - New Logon: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Logon ID: 0x3e7 Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x4 Process Name: Network Information: Workstation Name: - Source Network Address: - Source Port: - Detailed Authentication Information: Logon Process: - Authentication Package: - Transited Services: - Package Name (NTLM only): - Key Length: 0 This event is generated when a logon session is created. It is generated on the computer that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service such as the Server service, or a local process such as Winlogon.exe or Services.exe. The logon type field indicates the kind of logon that occurred. The most common types are 2 (interactive) and 3 (network). The New Logon fields indicate the account for whom the new logon was created, i.e. the account that was logged on. The network fields indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impersonation level field indicates the extent to which a process in the logon session can impersonate. The authentication information fields provide detailed information about this specific logon request. - Logon GUID is a unique identifier that can be used to correlate this event with a KDC event. - Transited services indicate which intermediate services have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indicates the length of the generated session key. This will be 0 if no session key was requested.
Security	Audit Success	13568	2015-04-25 08:44:54	Microsoft-Windows-Security-Auditing	4902: The Per-user audit policy table was created. Number of Elements: 0 Policy ID: 0x9683
Security	Audit Success	12544	2015-04-25 08:44:55	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: LTRANPHD$ Account Domain: WORKGROUP Logon ID: 0x3e7 Logon Type: 5 Impersonation Level: %%1833 New Logon: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Logon ID: 0x3e7 Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x234 Process Name: C:\Windows\System32\services.exe Network Information: Workstation Name: Source Network Address: - Source Port: - Detailed Authentication Information: Logon Process: Advapi Authentication Package: Negotiate Transited Services: - Package Name (NTLM only): - Key Length: 0 This event is generated when a logon session is created. It is generated on the computer that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service such as the Server service, or a local process such as Winlogon.exe or Services.exe. The logon type field indicates the kind of logon that occurred. The most common types are 2 (interactive) and 3 (network). The New Logon fields indicate the account for whom the new logon was created, i.e. the account that was logged on. The network fields indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impersonation level field indicates the extent to which a process in the logon session can impersonate. The authentication information fields provide detailed information about this specific logon request. - Logon GUID is a unique identifier that can be used to correlate this event with a KDC event. - Transited services indicate which intermediate services have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indicates the length of the generated session key. This will be 0 if no session key was requested.
Security	Audit Success	12544	2015-04-25	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: LTRANPHD$ Account Domain: WORKGROUP Logon ID: 0x3e7 Logon Type: 5 Impersonation Level: %%1833 New Logon: Security ID: S-1-5-20 Account Name: NETWORK SERVICE Account Domain: NT AUTHORITY Logon ID: 0x3e4 Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x234 Process Name: C:\Windows\System32\services.exe Network Information: Workstation Name: Source Network Address: - Source Port: - Detailed Authentication Information: Logon Process: Advapi Authentication Package: Negotiate Transited Services: - Package Name (NTLM only): - Key Length: 0 This event is generated when a logon session is created. It is generated on the computer that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service such as the Server service, or a local process such as Winlogon.exe or Services.exe. The logon type field indicates the kind of logon that occurred.

			08:44:55		The most common types are 2 (interactive) and 3 (network). The New Logon fields indicate the account for whom the new logon was created, i.e. the account that was logged on. The network fields indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impersonation level field indicates the extent to which a process in the logon session can impersonate. The authentication information fields provide detailed information about this specific logon request. - Logon GUID is a unique identifier that can be used to correlate this event with a KDC event. - Transited services indicate which intermediate services have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indicates the length of the generated session key. This will be 0 if no session key was requested.
Security	Audit Success	12544	2015-04-25 08:44:55	Microsoft-Windows-Security-Auditing	4648: A logon was attempted using explicit credentials. Subject: Security ID: S-1-5-18 Account Name: LTRANPHD$ Account Domain: WORKGROUP Logon ID: 0x3e7 Logon GUID: {00000000-0000-0000-0000-000000000000} Account Whose Credentials Were Used: Account Name: DWM-1 Account Domain: Window Manager Logon GUID: {00000000-0000-0000-0000-000000000000} Target Server: Target Server Name: localhost Additional Information: localhost Process Information: Process ID: 0x20c Process Name: C:\Windows\System32\winlogon.exe Network Information: Network Address: - Port: - This event is generated when a process attempts to log on an account by explicitly specifying that account's credentials. This most commonly occurs in batch-type configurations such as scheduled tasks, or when using the RUNAS command.
Security	Audit Success	12544	2015-04-25 08:44:55	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: LTRANPHD$ Account Domain: WORKGROUP Logon ID: 0x3e7 Logon Type: 2 Impersonation Level: %%1833 New Logon: Security ID: S-1-5-90-1 Account Name: DWM-1 Account Domain: Window Manager Logon ID: 0xe673 Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x20c Process Name: C:\Windows\System32\winlogon.exe Network Information: Workstation Name: Source Network Address: - Source Port: - Detailed Authentication Information: Logon Process: Advapi Authentication Package: Negotiate Transited Services: - Package Name (NTLM only): - Key Length: 0 This event is generated when a logon session is created. It is generated on the computer that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service such as the Server service, or a local process such as Winlogon.exe or Services.exe. The logon type field indicates the kind of logon that occurred. The most common types are 2 (interactive) and 3 (network). The New Logon fields indicate the account for whom the new logon was created, i.e. the account that was logged on. The network fields indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impersonation level field indicates the extent to which a process in the logon session can impersonate. The authentication information fields provide detailed information about this specific logon request. - Logon GUID is a unique identifier that can be used to correlate this event with a KDC event. - Transited services indicate which intermediate services have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indicates the length of the generated session key. This will be 0 if no session key was requested.
Security	Audit Success	12544	2015-04-25 08:44:55	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: LTRANPHD$ Account Domain: WORKGROUP Logon ID: 0x3e7 Logon Type: 2 Impersonation Level: %%1833 New Logon: Security ID: S-1-5-90-1 Account Name: DWM-1 Account Domain: Window Manager Logon ID: 0xe69f Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x20c Process Name: C:\Windows\System32\winlogon.exe Network Information: Workstation Name: Source Network Address: - Source Port: - Detailed Authentication Information: Logon Process: Advapi Authentication Package: Negotiate Transited Services: - Package Name (NTLM only): - Key Length: 0 This event is generated when a logon session is created. It is generated on the computer that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service such as the Server service, or a local process such as Winlogon.exe or Services.exe. The logon type field indicates the kind of logon that occurred. The most common types are 2 (interactive) and 3 (network). The New Logon fields indicate the account for whom the new logon was created, i.e. the account that was logged on. The network fields indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impersonation level field indicates the extent to which a process in the logon session can impersonate. The authentication information fields provide detailed information about this specific logon request. - Logon GUID is a unique identifier that can be used to correlate this event with a KDC event. - Transited services indicate which intermediate services have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indicates the length of the generated session key. This will be 0 if no session key was requested.
Security	Audit Success	12544	2015-04-25 08:44:55	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: LTRANPHD$ Account Domain: WORKGROUP Logon ID: 0x3e7 Logon Type: 5 Impersonation Level: %%1833 New Logon: Security ID: S-1-5-19 Account Name: LOCAL SERVICE Account Domain: NT AUTHORITY Logon ID: 0x3e5 Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x234 Process Name: C:\Windows\System32\services.exe Network Information: Workstation Name: Source Network Address: - Source Port: - Detailed Authentication Information: Logon Process: Advapi Authentication Package: Negotiate Transited Services: - Package Name (NTLM only): - Key Length: 0 This event is generated when a logon session is created. It is generated on the computer that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service such as the Server service, or a local process such as Winlogon.exe or Services.exe. The logon type field indicates the kind of logon that occurred. The most common types are 2 (interactive) and 3 (network). The New Logon fields indicate the account for whom the new logon was created, i.e. the account that was logged on. The network fields indicate where a

					remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impersonation level field indicates the extent to which a process in the logon session can impersonate. The authentication information fields provide detailed information about this specific logon request. - Logon GUID is a unique identifier that can be used to correlate this event with a KDC event. - Transited services indicate which intermediate services have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indicates the length of the generated session key. This will be 0 if no session key was requested.
Security	Audit Success	12544	2015-04-25 08:44:55	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: LTRANPHD$ Account Domain: WORKGROUP Logon ID: 0x3e7 Logon Type: 5 Impersonation Level: %%1833 New Logon: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Logon ID: 0x3e7 Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x234 Process Name: C:\Windows\System32\services.exe Network Information: Workstation Name: Source Network Address: - Source Port: - Detailed Authentication Information: Logon Process: Advapi Authentication Package: Negotiate Transited Services: - Package Name (NTLM only): - Key Length: 0 This event is generated when a logon session is created. It is generated on the computer that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service such as the Server service, or a local process such as Winlogon.exe or Services.exe. The logon type field indicates the kind of logon that occurred. The most common types are 2 (interactive) and 3 (network). The New Logon fields indicate the account for whom the new logon was created, i.e. the account that was logged on. The network fields indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impersonation level field indicates the extent to which a process in the logon session can impersonate. The authentication information fields provide detailed information about this specific logon request. - Logon GUID is a unique identifier that can be used to correlate this event with a KDC event. - Transited services indicate which intermediate services have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indicates the length of the generated session key. This will be 0 if no session key was requested.
Security	Audit Success	12544	2015-04-25 08:44:55	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: LTRANPHD$ Account Domain: WORKGROUP Logon ID: 0x3e7 Logon Type: 5 Impersonation Level: %%1833 New Logon: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Logon ID: 0x3e7 Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x234 Process Name: C:\Windows\System32\services.exe Network Information: Workstation Name: Source Network Address: - Source Port: - Detailed Authentication Information: Logon Process: Advapi Authentication Package: Negotiate Transited Services: - Package Name (NTLM only): - Key Length: 0 This event is generated when a logon session is created. It is generated on the computer that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service such as the Server service, or a local process such as Winlogon.exe or Services.exe. The logon type field indicates the kind of logon that occurred. The most common types are 2 (interactive) and 3 (network). The New Logon fields indicate the account for whom the new logon was created, i.e. the account that was logged on. The network fields indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impersonation level field indicates the extent to which a process in the logon session can impersonate. The authentication information fields provide detailed information about this specific logon request. - Logon GUID is a unique identifier that can be used to correlate this event with a KDC event. - Transited services indicate which intermediate services have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indicates the length of the generated session key. This will be 0 if no session key was requested.
Security	Audit Success	12548	2015-04-25 08:44:55	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Logon ID: 0x3e7 Privileges: SeAssignPrimaryTokenPrivilege SeTcbPrivilege SeSecurityPrivilege SeTakeOwnershipPrivilege SeLoadDriverPrivilege SeBackupPrivilege SeRestorePrivilege SeDebugPrivilege SeAuditPrivilege SeSystemEnvironmentPrivilege SeImpersonatePrivilege
Security	Audit Success	12548	2015-04-25 08:44:55	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-20 Account Name: NETWORK SERVICE Account Domain: NT AUTHORITY Logon ID: 0x3e4 Privileges: SeAssignPrimaryTokenPrivilege SeAuditPrivilege SeImpersonatePrivilege
Security	Audit Success	12548	2015-04-25 08:44:55	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-90-1 Account Name: DWM-1 Account Domain: Window Manager Logon ID: 0xe673 Privileges: SeAssignPrimaryTokenPrivilege SeAuditPrivilege SeImpersonatePrivilege
Security	Audit Success	12548	2015-04-25 08:44:55	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-90-1 Account Name: DWM-1 Account Domain: Window Manager Logon ID: 0xe69f Privileges: SeAssignPrimaryTokenPrivilege SeAuditPrivilege
Security	Audit Success	12548	2015-04-25 08:44:55	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-19 Account Name: LOCAL SERVICE Account Domain: NT AUTHORITY Logon ID: 0x3e5 Privileges: SeAssignPrimaryTokenPrivilege SeAuditPrivilege SeImpersonatePrivilege
Security	Audit Success	12548	2015-04-25 08:44:55	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Logon ID: 0x3e7 Privileges: SeAssignPrimaryTokenPrivilege SeTcbPrivilege SeSecurityPrivilege SeTakeOwnershipPrivilege SeLoadDriverPrivilege SeBackupPrivilege SeRestorePrivilege SeDebugPrivilege SeAuditPrivilege SeSystemEnvironmentPrivilege SeImpersonatePrivilege

Security	Audit Success	12548	2015-04-25 08:44:55	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Logon ID: 0x3e7 Privileges: SeAssignPrimaryTokenPrivilege SeTcbPrivilege SeSecurityPrivilege SeTakeOwnershipPrivilege SeLoadDriverPrivilege SeBackupPrivilege SeRestorePrivilege SeDebugPrivilege SeAuditPrivilege SeSystemEnvironmentPrivilege SeImpersonatePrivilege
Security	Audit Success	12292	2015-04-25 08:44:57	Microsoft-Windows-Security-Auditing	5033: The Windows Firewall Driver started successfully.
Security	Audit Success	12292	2015-04-25 08:44:57	Microsoft-Windows-Security-Auditing	5024: The Windows Firewall service started successfully.
Security	Audit Success	12544	2015-04-25 08:44:57	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: LTRANPHD$ Account Domain: WORKGROUP Logon ID: 0x3e7 Logon Type: 5 Impersonation Level: %%1833 New Logon: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Logon ID: 0x3e7 Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x234 Process Name: C:\Windows\System32\services.exe Network Information: Workstation Name: Source Network Address: - Source Port: - Detailed Authentication Information: Logon Process: Advapi Authentication Package: Negotiate Transited Services: - Package Name (NTLM only): - Key Length: 0 This event is generated when a logon session is created. It is generated on the computer that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service such as the Server service, or a local process such as Winlogon.exe or Services.exe. The logon type field indicates the kind of logon that occurred. The most common types are 2 (interactive) and 3 (network). The New Logon fields indicate the account for whom the new logon was created, i.e. the account that was logged on. The network fields indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impersonation level field indicates the extent to which a process in the logon session can impersonate. The authentication information fields provide detailed information about this specific logon request. - Logon GUID is a unique identifier that can be used to correlate this event with a KDC event. - Transited services indicate which intermediate services have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indicates the length of the generated session key. This will be 0 if no session key was requested.
Security	Audit Success	12544	2015-04-25 08:44:57	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: LTRANPHD$ Account Domain: WORKGROUP Logon ID: 0x3e7 Logon Type: 5 Impersonation Level: %%1833 New Logon: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Logon ID: 0x3e7 Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x234 Process Name: C:\Windows\System32\services.exe Network Information: Workstation Name: Source Network Address: - Source Port: - Detailed Authentication Information: Logon Process: Advapi Authentication Package: Negotiate Transited Services: - Package Name (NTLM only): - Key Length: 0 This event is generated when a logon session is created. It is generated on the computer that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service such as the Server service, or a local process such as Winlogon.exe or Services.exe. The logon type field indicates the kind of logon that occurred. The most common types are 2 (interactive) and 3 (network). The New Logon fields indicate the account for whom the new logon was created, i.e. the account that was logged on. The network fields indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impersonation level field indicates the extent to which a process in the logon session can impersonate. The authentication information fields provide detailed information about this specific logon request. - Logon GUID is a unique identifier that can be used to correlate this event with a KDC event. - Transited services indicate which intermediate services have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indicates the length of the generated session key. This will be 0 if no session key was requested.
Security	Audit Success	12544	2015-04-25 08:44:57	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: LTRANPHD$ Account Domain: WORKGROUP Logon ID: 0x3e7 Logon Type: 5 Impersonation Level: %%1833 New Logon: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Logon ID: 0x3e7 Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x234 Process Name: C:\Windows\System32\services.exe Network Information: Workstation Name: Source Network Address: - Source Port: - Detailed Authentication Information: Logon Process: Advapi Authentication Package: Negotiate Transited Services: - Package Name (NTLM only): - Key Length: 0 This event is generated when a logon session is created. It is generated on the computer that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service such as the Server service, or a local process such as Winlogon.exe or Services.exe. The logon type field indicates the kind of logon that occurred. The most common types are 2 (interactive) and 3 (network). The New Logon fields indicate the account for whom the new logon was created, i.e. the account that was logged on. The network fields indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impersonation level field indicates the extent to which a process in the logon session can impersonate. The authentication information fields provide detailed information about this specific logon request. - Logon GUID is a unique identifier that can be used to correlate this event with a KDC event. - Transited services indicate which intermediate services have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indicates the length of the generated

					session key. This will be 0 if no session key was requested.
Security	Audit Success	12544	2015-04-25 08:44:57	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-0-0 Account Name: - Account Domain: - Logon ID: 0x0 Logon Type: 3 Impersonation Level: %%1833 New Logon: Security ID: S-1-5-7 Account Name: ANONYMOUS LOGON Account Domain: NT AUTHORITY Logon ID: 0x18b22 Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x0 Process Name: - Network Information: Workstation Name: Source Network Address: - Source Port: - Detailed Authentication Information: Logon Process: NtLmSsp Authentication Package: NTLM Transited Services: - Package Name (NTLM only): NTLM V1 Key Length: 0 This event is generated when a logon session is created. It is generated on the computer that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service such as the Server service, or a local process such as Winlogon.exe or Services.exe. The logon type field indicates the kind of logon that occurred. The most common types are 2 (interactive) and 3 (network). The New Logon fields indicate the account for whom the new logon was created, i.e. the account that was logged on. The network fields indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impersonation level field indicates the extent to which a process in the logon session can impersonate. The authentication information fields provide detailed information about this specific logon request. - Logon GUID is a unique identifier that can be used to correlate this event with a KDC event. - Transited services indicate which intermediate services have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indicates the length of the generated session key. This will be 0 if no session key was requested.
Security	Audit Success	12548	2015-04-25 08:44:57	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Logon ID: 0x3e7 Privileges: SeAssignPrimaryTokenPrivilege SeTcbPrivilege SeSecurityPrivilege SeTakeOwnershipPrivilege SeLoadDriverPrivilege SeBackupPrivilege SeRestorePrivilege SeDebugPrivilege SeAuditPrivilege SeSystemEnvironmentPrivilege SeImpersonatePrivilege
Security	Audit Success	12548	2015-04-25 08:44:57	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Logon ID: 0x3e7 Privileges: SeAssignPrimaryTokenPrivilege SeTcbPrivilege SeSecurityPrivilege SeTakeOwnershipPrivilege SeLoadDriverPrivilege SeBackupPrivilege SeRestorePrivilege SeDebugPrivilege SeAuditPrivilege SeSystemEnvironmentPrivilege SeImpersonatePrivilege
Security	Audit Success	12548	2015-04-25 08:44:57	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Logon ID: 0x3e7 Privileges: SeAssignPrimaryTokenPrivilege SeTcbPrivilege SeSecurityPrivilege SeTakeOwnershipPrivilege SeLoadDriverPrivilege SeBackupPrivilege SeRestorePrivilege SeDebugPrivilege SeAuditPrivilege SeSystemEnvironmentPrivilege SeImpersonatePrivilege
Security	Audit Success	103	2015-04-25 08:45:37	Microsoft-Windows-Eventlog	1100: The event logging service has shut down.
Security	Audit Success	12288	2015-04-25 08:45:49	Microsoft-Windows-Security-Auditing	4608: Windows is starting up. This event is logged when LSASS.EXE starts and the auditing subsystem is initialized.
Security	Audit Success	12292	2015-04-25 08:45:49	Microsoft-Windows-Security-Auditing	5033: The Windows Firewall Driver started successfully.
Security	Audit Success	12544	2015-04-25 08:45:49	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-0-0 Account Name: - Account Domain: - Logon ID: 0x0 Logon Type: 0 Impersonation Level: - New Logon: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Logon ID: 0x3e7 Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x4 Process Name: Network Information: Workstation Name: - Source Network Address: - Source Port: - Detailed Authentication Information: Logon Process: - Authentication Package: - Transited Services: - Package Name (NTLM only): - Key Length: 0 This event is generated when a logon session is created. It is generated on the computer that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service such as the Server service, or a local process such as Winlogon.exe or Services.exe. The logon type field indicates the kind of logon that occurred. The most common types are 2 (interactive) and 3 (network). The New Logon fields indicate the account for whom the new logon was created, i.e. the account that was logged on. The network fields indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impersonation level field indicates the extent to which a process in the logon session can impersonate. The authentication information fields provide detailed information about this specific logon request. - Logon GUID is a unique identifier that can be used to correlate this event with a KDC event. - Transited services indicate which intermediate services have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indicates the length of the generated session key. This will be 0 if no session key was requested.
					4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: LTRANPHD$ Account Domain: WORKGROUP Logon ID: 0x3e7 Logon Type: 5 Impersonation Level: %%1833 New Logon: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Logon ID: 0x3e7 Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x240 Process Name: C:\Windows\System32\services.exe Network Information: Workstation Name: Source Network Address: - Source Port: - Detailed Authentication Information: Logon Process: Advapi Authentication Package: Negotiate Transited Services: - Package Name (NTLM only): - Key Length: 0 This event is generated when a logon session is

Security	Audit Success	12544	2015-04-25 08:45:49	Microsoft-Windows-Security-Auditing	created. It is generated on the computer that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service such as the Server service, or a local process such as Winlogon.exe or Services.exe. The logon type field indicates the kind of logon that occurred. The most common types are 2 (interactive) and 3 (network). The New Logon fields indicate the account for whom the new logon was created, i.e. the account that was logged on. The network fields indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impersonation level field indicates the extent to which a process in the logon session can impersonate. The authentication information fields provide detailed information about this specific logon request. - Logon GUID is a unique identifier that can be used to correlate this event with a KDC event. - Transited services indicate which intermediate services have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indicates the length of the generated session key. This will be 0 if no session key was requested.
Security	Audit Success	12544	2015-04-25 08:45:49	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: LTRANPHD$ Account Domain: WORKGROUP Logon ID: 0x3e7 Logon Type: 5 Impersonation Level: %%1833 New Logon: Security ID: S-1-5-20 Account Name: NETWORK SERVICE Account Domain: NT AUTHORITY Logon ID: 0x3e4 Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x240 Process Name: C:\Windows\System32\services.exe Network Information: Workstation Name: Source Network Address: - Source Port: - Detailed Authentication Information: Logon Process: Advapi Authentication Package: Negotiate Transited Services: - Package Name (NTLM only): - Key Length: 0 This event is generated when a logon session is created. It is generated on the computer that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service such as the Server service, or a local process such as Winlogon.exe or Services.exe. The logon type field indicates the kind of logon that occurred. The most common types are 2 (interactive) and 3 (network). The New Logon fields indicate the account for whom the new logon was created, i.e. the account that was logged on. The network fields indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impersonation level field indicates the extent to which a process in the logon session can impersonate. The authentication information fields provide detailed information about this specific logon request. - Logon GUID is a unique identifier that can be used to correlate this event with a KDC event. - Transited services indicate which intermediate services have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indicates the length of the generated session key. This will be 0 if no session key was requested.
Security	Audit Success	12544	2015-04-25 08:45:49	Microsoft-Windows-Security-Auditing	4648: A logon was attempted using explicit credentials. Subject: Security ID: S-1-5-18 Account Name: LTRANPHD$ Account Domain: WORKGROUP Logon ID: 0x3e7 Logon GUID: {00000000-0000-0000-0000-000000000000} Account Whose Credentials Were Used: Account Name: DWM-1 Account Domain: Window Manager Logon GUID: {00000000-0000-0000-0000-000000000000} Target Server: Target Server Name: localhost Additional Information: localhost Process Information: Process ID: 0x210 Process Name: C:\Windows\System32\winlogon.exe Network Information: Network Address: - Port: - This event is generated when a process attempts to log on an account by explicitly specifying that account's credentials. This most commonly occurs in batch-type configurations such as scheduled tasks, or when using the RUNAS command.
Security	Audit Success	12544	2015-04-25 08:45:49	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: LTRANPHD$ Account Domain: WORKGROUP Logon ID: 0x3e7 Logon Type: 2 Impersonation Level: %%1833 New Logon: Security ID: S-1-5-90-1 Account Name: DWM-1 Account Domain: Window Manager Logon ID: 0xc4ae Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x210 Process Name: C:\Windows\System32\winlogon.exe Network Information: Workstation Name: Source Network Address: - Source Port: - Detailed Authentication Information: Logon Process: Advapi Authentication Package: Negotiate Transited Services: - Package Name (NTLM only): - Key Length: 0 This event is generated when a logon session is created. It is generated on the computer that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service such as the Server service, or a local process such as Winlogon.exe or Services.exe. The logon type field indicates the kind of logon that occurred. The most common types are 2 (interactive) and 3 (network). The New Logon fields indicate the account for whom the new logon was created, i.e. the account that was logged on. The network fields indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impersonation level field indicates the extent to which a process in the logon session can impersonate. The authentication information fields provide detailed information about this specific logon request. - Logon GUID is a unique identifier that can be used to correlate this event with a KDC event. - Transited services indicate which intermediate services have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indicates the length of the generated session key. This will be 0 if no session key was requested.
			2015-04-		4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: LTRANPHD$ Account Domain: WORKGROUP Logon ID: 0x3e7 Logon Type: 2 Impersonation Level: %%1833 New Logon: Security ID: S-1-5-90-1 Account Name: DWM-1 Account Domain: Window Manager Logon ID: 0xc4ca Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x210 Process Name: C:\Windows\System32\winlogon.exe Network Information: Workstation Name: Source Network Address: - Source Port: - Detailed Authentication Information: Logon Process: Advapi Authentication Package: Negotiate Transited Services: - Package Name (NTLM only): - Key Length: 0 This event is generated when a logon session is created. It is generated on the computer that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service such as the Server service, or a local

Security	Audit Success	12544	25 08:45:49	Microsoft-Windows-Security-Auditing	process such as Winlogon.exe or Services.exe. The logon type field indicates the kind of logon that occurred. The most common types are 2 (interactive) and 3 (network). The New Logon fields indicate the account for whom the new logon was created, i.e. the account that was logged on. The network fields indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impersonation level field indicates the extent to which a process in the logon session can impersonate. The authentication information fields provide detailed information about this specific logon request. - Logon GUID is a unique identifier that can be used to correlate this event with a KDC event. - Transited services indicate which intermediate services have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indicates the length of the generated session key. This will be 0 if no session key was requested.
Security	Audit Success	12544	2015-04-25 08:45:49	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: LTRANPHD$ Account Domain: WORKGROUP Logon ID: 0x3e7 Logon Type: 5 Impersonation Level: %%1833 New Logon: Security ID: S-1-5-19 Account Name: LOCAL SERVICE Account Domain: NT AUTHORITY Logon ID: 0x3e5 Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x240 Process Name: C:\Windows\System32\services.exe Network Information: Workstation Name: Source Network Address: - Source Port: - Detailed Authentication Information: Logon Process: Advapi Authentication Package: Negotiate Transited Services: - Package Name (NTLM only): - Key Length: 0 This event is generated when a logon session is created. It is generated on the computer that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service such as the Server service, or a local process such as Winlogon.exe or Services.exe. The logon type field indicates the kind of logon that occurred. The most common types are 2 (interactive) and 3 (network). The New Logon fields indicate the account for whom the new logon was created, i.e. the account that was logged on. The network fields indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impersonation level field indicates the extent to which a process in the logon session can impersonate. The authentication information fields provide detailed information about this specific logon request. - Logon GUID is a unique identifier that can be used to correlate this event with a KDC event. - Transited services indicate which intermediate services have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indicates the length of the generated session key. This will be 0 if no session key was requested.
Security	Audit Success	12544	2015-04-25 08:45:49	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: LTRANPHD$ Account Domain: WORKGROUP Logon ID: 0x3e7 Logon Type: 5 Impersonation Level: %%1833 New Logon: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Logon ID: 0x3e7 Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x240 Process Name: C:\Windows\System32\services.exe Network Information: Workstation Name: Source Network Address: - Source Port: - Detailed Authentication Information: Logon Process: Advapi Authentication Package: Negotiate Transited Services: - Package Name (NTLM only): - Key Length: 0 This event is generated when a logon session is created. It is generated on the computer that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service such as the Server service, or a local process such as Winlogon.exe or Services.exe. The logon type field indicates the kind of logon that occurred. The most common types are 2 (interactive) and 3 (network). The New Logon fields indicate the account for whom the new logon was created, i.e. the account that was logged on. The network fields indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impersonation level field indicates the extent to which a process in the logon session can impersonate. The authentication information fields provide detailed information about this specific logon request. - Logon GUID is a unique identifier that can be used to correlate this event with a KDC event. - Transited services indicate which intermediate services have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indicates the length of the generated session key. This will be 0 if no session key was requested.
Security	Audit Success	12544	2015-04-25 08:45:49	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: LTRANPHD$ Account Domain: WORKGROUP Logon ID: 0x3e7 Logon Type: 5 Impersonation Level: %%1833 New Logon: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Logon ID: 0x3e7 Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x240 Process Name: C:\Windows\System32\services.exe Network Information: Workstation Name: Source Network Address: - Source Port: - Detailed Authentication Information: Logon Process: Advapi Authentication Package: Negotiate Transited Services: - Package Name (NTLM only): - Key Length: 0 This event is generated when a logon session is created. It is generated on the computer that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service such as the Server service, or a local process such as Winlogon.exe or Services.exe. The logon type field indicates the kind of logon that occurred. The most common types are 2 (interactive) and 3 (network). The New Logon fields indicate the account for whom the new logon was created, i.e. the account that was logged on. The network fields indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impersonation level field indicates the extent to which a process in the logon session can impersonate. The authentication information fields provide detailed information about this specific logon request. - Logon GUID is a unique identifier that can be used to correlate this event with a KDC event. - Transited services indicate which intermediate services have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indicates the length of the generated

					session key. This will be 0 if no session key was requested.
Security	Audit Success	12544	2015-04-25 08:45:49	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: LTRANPHD$ Account Domain: WORKGROUP Logon ID: 0x3e7 Logon Type: 5 Impersonation Level: %%1833 New Logon: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Logon ID: 0x3e7 Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x240 Process Name: C:\Windows\System32\services.exe Network Information: Workstation Name: Source Network Address: - Source Port: - Detailed Authentication Information: Logon Process: Advapi Authentication Package: Negotiate Transited Services: - Package Name (NTLM only): - Key Length: 0 This event is generated when a logon session is created. It is generated on the computer that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service such as the Server service, or a local process such as Winlogon.exe or Services.exe. The logon type field indicates the kind of logon that occurred. The most common types are 2 (interactive) and 3 (network). The New Logon fields indicate the account for whom the new logon was created, i.e. the account that was logged on. The network fields indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impersonation level field indicates the extent to which a process in the logon session can impersonate. The authentication information fields provide detailed information about this specific logon request. - Logon GUID is a unique identifier that can be used to correlate this event with a KDC event. - Transited services indicate which intermediate services have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indicates the length of the generated session key. This will be 0 if no session key was requested.
Security	Audit Success	12544	2015-04-25 08:45:49	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: LTRANPHD$ Account Domain: WORKGROUP Logon ID: 0x3e7 Logon Type: 5 Impersonation Level: %%1833 New Logon: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Logon ID: 0x3e7 Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x240 Process Name: C:\Windows\System32\services.exe Network Information: Workstation Name: Source Network Address: - Source Port: - Detailed Authentication Information: Logon Process: Advapi Authentication Package: Negotiate Transited Services: - Package Name (NTLM only): - Key Length: 0 This event is generated when a logon session is created. It is generated on the computer that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service such as the Server service, or a local process such as Winlogon.exe or Services.exe. The logon type field indicates the kind of logon that occurred. The most common types are 2 (interactive) and 3 (network). The New Logon fields indicate the account for whom the new logon was created, i.e. the account that was logged on. The network fields indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impersonation level field indicates the extent to which a process in the logon session can impersonate. The authentication information fields provide detailed information about this specific logon request. - Logon GUID is a unique identifier that can be used to correlate this event with a KDC event. - Transited services indicate which intermediate services have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indicates the length of the generated session key. This will be 0 if no session key was requested.
Security	Audit Success	12548	2015-04-25 08:45:49	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Logon ID: 0x3e7 Privileges: SeAssignPrimaryTokenPrivilege SeTcbPrivilege SeSecurityPrivilege SeTakeOwnershipPrivilege SeLoadDriverPrivilege SeBackupPrivilege SeRestorePrivilege SeDebugPrivilege SeAuditPrivilege SeSystemEnvironmentPrivilege SeImpersonatePrivilege
Security	Audit Success	12548	2015-04-25 08:45:49	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-20 Account Name: NETWORK SERVICE Account Domain: NT AUTHORITY Logon ID: 0x3e4 Privileges: SeAssignPrimaryTokenPrivilege SeAuditPrivilege SeImpersonatePrivilege
Security	Audit Success	12548	2015-04-25 08:45:49	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-90-1 Account Name: DWM-1 Account Domain: Window Manager Logon ID: 0xc4ae Privileges: SeAssignPrimaryTokenPrivilege SeAuditPrivilege SeImpersonatePrivilege
Security	Audit Success	12548	2015-04-25 08:45:49	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-90-1 Account Name: DWM-1 Account Domain: Window Manager Logon ID: 0xc4ca Privileges: SeAssignPrimaryTokenPrivilege SeAuditPrivilege
Security	Audit Success	12548	2015-04-25 08:45:49	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-19 Account Name: LOCAL SERVICE Account Domain: NT AUTHORITY Logon ID: 0x3e5 Privileges: SeAssignPrimaryTokenPrivilege SeAuditPrivilege SeImpersonatePrivilege
Security	Audit Success	12548	2015-04-25 08:45:49	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Logon ID: 0x3e7 Privileges: SeAssignPrimaryTokenPrivilege SeTcbPrivilege SeSecurityPrivilege SeTakeOwnershipPrivilege SeLoadDriverPrivilege SeBackupPrivilege SeRestorePrivilege SeDebugPrivilege SeAuditPrivilege SeSystemEnvironmentPrivilege SeImpersonatePrivilege
Security	Audit Success	12548	2015-04-25 08:45:49	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Logon ID: 0x3e7 Privileges: SeAssignPrimaryTokenPrivilege SeTcbPrivilege SeSecurityPrivilege SeTakeOwnershipPrivilege SeLoadDriverPrivilege SeBackupPrivilege SeRestorePrivilege SeDebugPrivilege SeAuditPrivilege SeSystemEnvironmentPrivilege SeImpersonatePrivilege
Security	Audit	12548	2015-04-25	Microsoft-Windows-Security-	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Logon ID: 0x3e7 Privileges: SeAssignPrimaryTokenPrivilege SeTcbPrivilege

	Success		08:45:49	Auditing	SeSecurityPrivilege SeTakeOwnershipPrivilege SeLoadDriverPrivilege SeBackupPrivilege SeRestorePrivilege SeDebugPrivilege SeAuditPrivilege SeSystemEnvironmentPrivilege SeImpersonatePrivilege
Security	Audit Success	12548	2015-04-25 08:45:49	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Logon ID: 0x3e7 Privileges: SeAssignPrimaryTokenPrivilege SeTcbPrivilege SeSecurityPrivilege SeTakeOwnershipPrivilege SeLoadDriverPrivilege SeBackupPrivilege SeRestorePrivilege SeDebugPrivilege SeAuditPrivilege SeSystemEnvironmentPrivilege SeImpersonatePrivilege
Security	Audit Success	13568	2015-04-25 08:45:49	Microsoft-Windows-Security-Auditing	4902: The Per-user audit policy table was created. Number of Elements: 0 Policy ID: 0x761a
Security	Audit Success	12292	2015-04-25 08:45:50	Microsoft-Windows-Security-Auditing	5024: The Windows Firewall service started successfully.
Security	Audit Success	12544	2015-04-25 08:45:50	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: LTRANPHD$ Account Domain: WORKGROUP Logon ID: 0x3e7 Logon Type: 5 Impersonation Level: %%1833 New Logon: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Logon ID: 0x3e7 Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x240 Process Name: C:\Windows\System32\services.exe Network Information: Workstation Name: Source Network Address: - Source Port: - Detailed Authentication Information: Logon Process: Advapi Authentication Package: Negotiate Transited Services: - Package Name (NTLM only): - Key Length: 0 This event is generated when a logon session is created. It is generated on the computer that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service such as the Server service, or a local process such as Winlogon.exe or Services.exe. The logon type field indicates the kind of logon that occurred. The most common types are 2 (interactive) and 3 (network). The New Logon fields indicate the account for whom the new logon was created, i.e. the account that was logged on. The network fields indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impersonation level field indicates the extent to which a process in the logon session can impersonate. The authentication information fields provide detailed information about this specific logon request. - Logon GUID is a unique identifier that can be used to correlate this event with a KDC event. - Transited services indicate which intermediate services have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indicates the length of the generated session key. This will be 0 if no session key was requested.
Security	Audit Success	12544	2015-04-25 08:45:50	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-0-0 Account Name: - Account Domain: - Logon ID: 0x0 Logon Type: 3 Impersonation Level: %%1833 New Logon: Security ID: S-1-5-7 Account Name: ANONYMOUS LOGON Account Domain: NT AUTHORITY Logon ID: 0x17076 Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x0 Process Name: - Network Information: Workstation Name: Source Network Address: - Source Port: - Detailed Authentication Information: Logon Process: NtLmSsp Authentication Package: NTLM Transited Services: - Package Name (NTLM only): NTLM V1 Key Length: 0 This event is generated when a logon session is created. It is generated on the computer that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service such as the Server service, or a local process such as Winlogon.exe or Services.exe. The logon type field indicates the kind of logon that occurred. The most common types are 2 (interactive) and 3 (network). The New Logon fields indicate the account for whom the new logon was created, i.e. the account that was logged on. The network fields indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impersonation level field indicates the extent to which a process in the logon session can impersonate. The authentication information fields provide detailed information about this specific logon request. - Logon GUID is a unique identifier that can be used to correlate this event with a KDC event. - Transited services indicate which intermediate services have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indicates the length of the generated session key. This will be 0 if no session key was requested.
Security	Audit Success	12548	2015-04-25 08:45:50	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Logon ID: 0x3e7 Privileges: SeAssignPrimaryTokenPrivilege SeTcbPrivilege SeSecurityPrivilege SeTakeOwnershipPrivilege SeLoadDriverPrivilege SeBackupPrivilege SeRestorePrivilege SeDebugPrivilege SeAuditPrivilege SeSystemEnvironmentPrivilege SeImpersonatePrivilege
Security	Audit Success	12544	2015-04-25 08:45:59	Microsoft-Windows-Security-Auditing	4648: A logon was attempted using explicit credentials. Subject: Security ID: S-1-5-18 Account Name: LTRANPHD$ Account Domain: WORKGROUP Logon ID: 0x3e7 Logon GUID: {00000000-0000-0000-0000-000000000000} Account Whose Credentials Were Used: Account Name: Liem Account Domain: LTRANPHD Logon GUID: {00000000-0000-0000-0000-000000000000} Target Server: Target Server Name: localhost Additional Information: localhost Process Information: Process ID: 0x210 Process Name: C:\Windows\System32\winlogon.exe Network Information: Network Address: 127.0.0.1 Port: 0 This event is generated when a process attempts to log on an account by explicitly specifying that account's credentials. This most commonly occurs in batch-type configurations such as scheduled tasks, or when using the RUNAS command.
					4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: LTRANPHD$ Account Domain: WORKGROUP Logon ID: 0x3e7 Logon Type: 2 Impersonation Level: %%1833 New Logon: Security ID: S-1-5-21-1888849264-3803429180-4108621888-1001 Account Name: Liem Account Domain: LTRANPHD Logon ID: 0x1fb68 Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information:

Security	Audit Success	12544	2015-04-25 08:45:59	Microsoft-Windows-Security-Auditing	Process ID: 0x210 Process Name: C:\Windows\System32\winlogon.exe Network Information: Workstation Name: LTRANPHD Source Network Address: 127.0.0.1 Source Port: 0 Detailed Authentication Information: Logon Process: User32 Authentication Package: Negotiate Transited Services: - Package Name (NTLM only): - Key Length: 0 This event is generated when a logon session is created. It is generated on the computer that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service such as the Server service, or a local process such as Winlogon.exe or Services.exe. The logon type field indicates the kind of logon that occurred. The most common types are 2 (interactive) and 3 (network). The New Logon fields indicate the account for whom the new logon was created, i.e. the account that was logged on. The network fields indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impersonation level field indicates the extent to which a process in the logon session can impersonate. The authentication information fields provide detailed information about this specific logon request. - Logon GUID is a unique identifier that can be used to correlate this event with a KDC event. - Transited services indicate which intermediate services have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indicates the length of the generated session key. This will be 0 if no session key was requested.
Security	Audit Success	12544	2015-04-25 08:45:59	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: LTRANPHD$ Account Domain: WORKGROUP Logon ID: 0x3e7 Logon Type: 2 Impersonation Level: %%1833 New Logon: Security ID: S-1-5-21-1888849264-3803429180-4108621888-1001 Account Name: Liem Account Domain: LTRANPHD Logon ID: 0x1fb9f Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x210 Process Name: C:\Windows\System32\winlogon.exe Network Information: Workstation Name: LTRANPHD Source Network Address: 127.0.0.1 Source Port: 0 Detailed Authentication Information: Logon Process: User32 Authentication Package: Negotiate Transited Services: - Package Name (NTLM only): - Key Length: 0 This event is generated when a logon session is created. It is generated on the computer that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service such as the Server service, or a local process such as Winlogon.exe or Services.exe. The logon type field indicates the kind of logon that occurred. The most common types are 2 (interactive) and 3 (network). The New Logon fields indicate the account for whom the new logon was created, i.e. the account that was logged on. The network fields indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impersonation level field indicates the extent to which a process in the logon session can impersonate. The authentication information fields provide detailed information about this specific logon request. - Logon GUID is a unique identifier that can be used to correlate this event with a KDC event. - Transited services indicate which intermediate services have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indicates the length of the generated session key. This will be 0 if no session key was requested.
Security	Audit Success	12548	2015-04-25 08:45:59	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-21-1888849264-3803429180-4108621888-1001 Account Name: Liem Account Domain: LTRANPHD Logon ID: 0x1fb68 Privileges: SeSecurityPrivilege SeTakeOwnershipPrivilege SeLoadDriverPrivilege SeBackupPrivilege SeRestorePrivilege SeDebugPrivilege SeSystemEnvironmentPrivilege SeImpersonatePrivilege
Security	Audit Success	12544	2015-04-25 08:46:00	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: LTRANPHD$ Account Domain: WORKGROUP Logon ID: 0x3e7 Logon Type: 5 Impersonation Level: %%1833 New Logon: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Logon ID: 0x3e7 Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x240 Process Name: C:\Windows\System32\services.exe Network Information: Workstation Name: Source Network Address: - Source Port: - Detailed Authentication Information: Logon Process: Advapi Authentication Package: Negotiate Transited Services: - Package Name (NTLM only): - Key Length: 0 This event is generated when a logon session is created. It is generated on the computer that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service such as the Server service, or a local process such as Winlogon.exe or Services.exe. The logon type field indicates the kind of logon that occurred. The most common types are 2 (interactive) and 3 (network). The New Logon fields indicate the account for whom the new logon was created, i.e. the account that was logged on. The network fields indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impersonation level field indicates the extent to which a process in the logon session can impersonate. The authentication information fields provide detailed information about this specific logon request. - Logon GUID is a unique identifier that can be used to correlate this event with a KDC event. - Transited services indicate which intermediate services have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indicates the length of the generated session key. This will be 0 if no session key was requested.
Security	Audit Success	12548	2015-04-25 08:46:00	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Logon ID: 0x3e7 Privileges: SeAssignPrimaryTokenPrivilege SeTcbPrivilege SeSecurityPrivilege SeTakeOwnershipPrivilege SeLoadDriverPrivilege SeBackupPrivilege SeRestorePrivilege SeDebugPrivilege SeAuditPrivilege SeSystemEnvironmentPrivilege SeImpersonatePrivilege
Security	Audit Success	13824	2015-04-25 08:46:01	Microsoft-Windows-Security-Auditing	4797: An attempt was made to query the existence of a blank password for an account. Subject: Security ID: S-1-5-19 Account Name: LOCAL SERVICE Account Domain: NT AUTHORITY Logon ID: 0x3e5 Additional Information: Caller Workstation: LTRANPHD Target Account Name: Administrator Target Account Domain: LTRANPHD
	Audit		2015-04-	Microsoft-Windows-Security-	4797: An attempt was made to query the existence of a blank password for an account. Subject: Security ID:

Security	Success	13824	25 08:46:01	Auditing	S-1-5-19 Account Name: LOCAL SERVICE Account Domain: NT AUTHORITY Logon ID: 0x3e5 Additional Information: Caller Workstation: LTRANPHD Target Account Name: Guest Target Account Domain: LTRANPHD
Security	Audit Success	13824	2015-04-25 08:46:01	Microsoft-Windows-Security-Auditing	4797: An attempt was made to query the existence of a blank password for an account. Subject: Security ID: S-1-5-19 Account Name: LOCAL SERVICE Account Domain: NT AUTHORITY Logon ID: 0x3e5 Additional Information: Caller Workstation: LTRANPHD Target Account Name: Liem Target Account Domain: LTRANPHD
Security	Audit Success	13824	2015-04-25 08:46:01	Microsoft-Windows-Security-Auditing	4797: An attempt was made to query the existence of a blank password for an account. Subject: Security ID: S-1-5-19 Account Name: LOCAL SERVICE Account Domain: NT AUTHORITY Logon ID: 0x3e5 Additional Information: Caller Workstation: LTRANPHD Target Account Name: Liem Target Account Domain: LTRANPHD
Security	Audit Success	13824	2015-04-25 08:46:01	Microsoft-Windows-Security-Auditing	4797: An attempt was made to query the existence of a blank password for an account. Subject: Security ID: S-1-5-19 Account Name: LOCAL SERVICE Account Domain: NT AUTHORITY Logon ID: 0x3e5 Additional Information: Caller Workstation: LTRANPHD Target Account Name: Administrator Target Account Domain: LTRANPHD
Security	Audit Success	13824	2015-04-25 08:46:01	Microsoft-Windows-Security-Auditing	4797: An attempt was made to query the existence of a blank password for an account. Subject: Security ID: S-1-5-19 Account Name: LOCAL SERVICE Account Domain: NT AUTHORITY Logon ID: 0x3e5 Additional Information: Caller Workstation: LTRANPHD Target Account Name: Guest Target Account Domain: LTRANPHD
Security	Audit Success	13824	2015-04-25 08:46:01	Microsoft-Windows-Security-Auditing	4797: An attempt was made to query the existence of a blank password for an account. Subject: Security ID: S-1-5-19 Account Name: LOCAL SERVICE Account Domain: NT AUTHORITY Logon ID: 0x3e5 Additional Information: Caller Workstation: LTRANPHD Target Account Name: Liem Target Account Domain: LTRANPHD
Security	Audit Success	13824	2015-04-25 08:46:01	Microsoft-Windows-Security-Auditing	4797: An attempt was made to query the existence of a blank password for an account. Subject: Security ID: S-1-5-19 Account Name: LOCAL SERVICE Account Domain: NT AUTHORITY Logon ID: 0x3e5 Additional Information: Caller Workstation: LTRANPHD Target Account Name: Administrator Target Account Domain: LTRANPHD
Security	Audit Success	13824	2015-04-25 08:46:01	Microsoft-Windows-Security-Auditing	4797: An attempt was made to query the existence of a blank password for an account. Subject: Security ID: S-1-5-19 Account Name: LOCAL SERVICE Account Domain: NT AUTHORITY Logon ID: 0x3e5 Additional Information: Caller Workstation: LTRANPHD Target Account Name: Liem Target Account Domain: LTRANPHD
Security	Audit Success	13824	2015-04-25 08:46:01	Microsoft-Windows-Security-Auditing	4797: An attempt was made to query the existence of a blank password for an account. Subject: Security ID: S-1-5-19 Account Name: LOCAL SERVICE Account Domain: NT AUTHORITY Logon ID: 0x3e5 Additional Information: Caller Workstation: LTRANPHD Target Account Name: Administrator Target Account Domain: LTRANPHD
Security	Audit Success	13824	2015-04-25 08:46:01	Microsoft-Windows-Security-Auditing	4797: An attempt was made to query the existence of a blank password for an account. Subject: Security ID: S-1-5-19 Account Name: LOCAL SERVICE Account Domain: NT AUTHORITY Logon ID: 0x3e5 Additional Information: Caller Workstation: LTRANPHD Target Account Name: Guest Target Account Domain: LTRANPHD
Security	Audit Success	13824	2015-04-25 08:46:01	Microsoft-Windows-Security-Auditing	4797: An attempt was made to query the existence of a blank password for an account. Subject: Security ID: S-1-5-19 Account Name: LOCAL SERVICE Account Domain: NT AUTHORITY Logon ID: 0x3e5 Additional Information: Caller Workstation: LTRANPHD Target Account Name: Liem Target Account Domain: LTRANPHD
Security	Audit Success	13824	2015-04-25 08:46:01	Microsoft-Windows-Security-Auditing	4797: An attempt was made to query the existence of a blank password for an account. Subject: Security ID: S-1-5-19 Account Name: LOCAL SERVICE Account Domain: NT AUTHORITY Logon ID: 0x3e5 Additional Information: Caller Workstation: LTRANPHD Target Account Name: Liem Target Account Domain: LTRANPHD
Security	Audit Success	13824	2015-04-25 08:46:01	Microsoft-Windows-Security-Auditing	4797: An attempt was made to query the existence of a blank password for an account. Subject: Security ID: S-1-5-19 Account Name: LOCAL SERVICE Account Domain: NT AUTHORITY Logon ID: 0x3e5 Additional Information: Caller Workstation: LTRANPHD Target Account Name: Administrator Target Account Domain: LTRANPHD
Security	Audit Success	13824	2015-04-25 08:46:01	Microsoft-Windows-Security-Auditing	4797: An attempt was made to query the existence of a blank password for an account. Subject: Security ID: S-1-5-19 Account Name: LOCAL SERVICE Account Domain: NT AUTHORITY Logon ID: 0x3e5 Additional Information: Caller Workstation: LTRANPHD Target Account Name: Guest Target Account Domain: LTRANPHD
Security	Audit Success	13824	2015-04-25 08:46:01	Microsoft-Windows-Security-Auditing	4797: An attempt was made to query the existence of a blank password for an account. Subject: Security ID: S-1-5-19 Account Name: LOCAL SERVICE Account Domain: NT AUTHORITY Logon ID: 0x3e5 Additional Information: Caller Workstation: LTRANPHD Target Account Name: Liem Target Account Domain: LTRANPHD
Security	Audit Success	13824	2015-04-25 08:46:01	Microsoft-Windows-Security-Auditing	4797: An attempt was made to query the existence of a blank password for an account. Subject: Security ID: S-1-5-19 Account Name: LOCAL SERVICE Account Domain: NT AUTHORITY Logon ID: 0x3e5 Additional Information: Caller Workstation: LTRANPHD Target Account Name: Liem Target Account Domain: LTRANPHD
Security	Audit Success	13824	2015-04-25 08:46:02	Microsoft-Windows-Security-Auditing	4797: An attempt was made to query the existence of a blank password for an account. Subject: Security ID: S-1-5-21-1888849264-3803429180-4108621888-1001 Account Name: Liem Account Domain: LTRANPHD Logon ID: 0x1fb9f Additional Information: Caller Workstation: LTRANPHD Target Account Name: Administrator Target Account Domain: LTRANPHD
Security	Audit Success	13824	2015-04-25 08:46:02	Microsoft-Windows-Security-Auditing	4797: An attempt was made to query the existence of a blank password for an account. Subject: Security ID: S-1-5-21-1888849264-3803429180-4108621888-1001 Account Name: Liem Account Domain: LTRANPHD Logon ID: 0x1fb9f Additional Information: Caller Workstation: LTRANPHD Target Account Name: Guest Target Account Domain: LTRANPHD
Security	Audit Success	13824	2015-04-25 08:46:02	Microsoft-Windows-Security-Auditing	4797: An attempt was made to query the existence of a blank password for an account. Subject: Security ID: S-1-5-21-1888849264-3803429180-4108621888-1001 Account Name: Liem Account Domain: LTRANPHD Logon ID: 0x1fb9f Additional Information: Caller Workstation: LTRANPHD Target Account Name: Administrator Target Account Domain: LTRANPHD

Security	Audit Success	13824	2015-04-25 08:46:02	Microsoft-Windows-Security-Auditing	4797: An attempt was made to query the existence of a blank password for an account. Subject: Security ID: S-1-5-21-1888849264-3803429180-4108621888-1001 Account Name: Liem Account Domain: LTRANPHD Logon ID: 0x1fb9f Additional Information: Caller Workstation: LTRANPHD Target Account Name: Guest Target Account Domain: LTRANPHD
Security	Audit Success	12544	2015-04-25 08:53:22	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: LTRANPHD$ Account Domain: WORKGROUP Logon ID: 0x3e7 Logon Type: 5 Impersonation Level: %%1833 New Logon: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Logon ID: 0x3e7 Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x240 Process Name: C:\Windows\System32\services.exe Network Information: Workstation Name: Source Network Address: - Source Port: - Detailed Authentication Information: Logon Process: Advapi Authentication Package: Negotiate Transited Services: - Package Name (NTLM only): - Key Length: 0 This event is generated when a logon session is created. It is generated on the computer that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service such as the Server service, or a local process such as Winlogon.exe or Services.exe. The logon type field indicates the kind of logon that occurred. The most common types are 2 (interactive) and 3 (network). The New Logon fields indicate the account for whom the new logon was created, i.e. the account that was logged on. The network fields indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impersonation level field indicates the extent to which a process in the logon session can impersonate. The authentication information fields provide detailed information about this specific logon request. - Logon GUID is a unique identifier that can be used to correlate this event with a KDC event. - Transited services indicate which intermediate services have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indicates the length of the generated session key. This will be 0 if no session key was requested.
Security	Audit Success	12548	2015-04-25 08:53:22	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Logon ID: 0x3e7 Privileges: SeAssignPrimaryTokenPrivilege SeTcbPrivilege SeSecurityPrivilege SeTakeOwnershipPrivilege SeLoadDriverPrivilege SeBackupPrivilege SeRestorePrivilege SeDebugPrivilege SeAuditPrivilege SeSystemEnvironmentPrivilege SeImpersonatePrivilege
Security	Audit Success	12544	2015-04-25 08:53:23	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: LTRANPHD$ Account Domain: WORKGROUP Logon ID: 0x3e7 Logon Type: 5 Impersonation Level: %%1833 New Logon: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Logon ID: 0x3e7 Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x240 Process Name: C:\Windows\System32\services.exe Network Information: Workstation Name: Source Network Address: - Source Port: - Detailed Authentication Information: Logon Process: Advapi Authentication Package: Negotiate Transited Services: - Package Name (NTLM only): - Key Length: 0 This event is generated when a logon session is created. It is generated on the computer that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service such as the Server service, or a local process such as Winlogon.exe or Services.exe. The logon type field indicates the kind of logon that occurred. The most common types are 2 (interactive) and 3 (network). The New Logon fields indicate the account for whom the new logon was created, i.e. the account that was logged on. The network fields indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impersonation level field indicates the extent to which a process in the logon session can impersonate. The authentication information fields provide detailed information about this specific logon request. - Logon GUID is a unique identifier that can be used to correlate this event with a KDC event. - Transited services indicate which intermediate services have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indicates the length of the generated session key. This will be 0 if no session key was requested.
Security	Audit Success	12548	2015-04-25 08:53:23	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Logon ID: 0x3e7 Privileges: SeAssignPrimaryTokenPrivilege SeTcbPrivilege SeSecurityPrivilege SeTakeOwnershipPrivilege SeLoadDriverPrivilege SeBackupPrivilege SeRestorePrivilege SeDebugPrivilege SeAuditPrivilege SeSystemEnvironmentPrivilege SeImpersonatePrivilege
Security	Audit Success	12544	2015-04-25 09:01:12	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: LTRANPHD$ Account Domain: WORKGROUP Logon ID: 0x3e7 Logon Type: 5 Impersonation Level: %%1833 New Logon: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Logon ID: 0x3e7 Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x240 Process Name: C:\Windows\System32\services.exe Network Information: Workstation Name: Source Network Address: - Source Port: - Detailed Authentication Information: Logon Process: Advapi Authentication Package: Negotiate Transited Services: - Package Name (NTLM only): - Key Length: 0 This event is generated when a logon session is created. It is generated on the computer that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service such as the Server service, or a local process such as Winlogon.exe or Services.exe. The logon type field indicates the kind of logon that occurred. The most common types are 2 (interactive) and 3 (network). The New Logon fields indicate the account for whom the new logon was created, i.e. the account that was logged on. The network fields indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impersonation level field indicates the extent to which a process in the logon session can impersonate. The authentication information fields provide detailed information about this specific logon request. - Logon GUID is a unique identifier that can be used to correlate this event with a KDC event. - Transited

					services indicate which intermediate services have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indicates the length of the generated session key. This will be 0 if no session key was requested.
Security	Audit Success	12548	2015-04-25 09:01:12	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Logon ID: 0x3e7 Privileges: SeAssignPrimaryTokenPrivilege SeTcbPrivilege SeSecurityPrivilege SeTakeOwnershipPrivilege SeLoadDriverPrivilege SeBackupPrivilege SeRestorePrivilege SeDebugPrivilege SeAuditPrivilege SeSystemEnvironmentPrivilege SeImpersonatePrivilege
Security	Audit Success	12544	2015-04-25 09:01:28	Microsoft-Windows-Security-Auditing	4648: A logon was attempted using explicit credentials. Subject: Security ID: S-1-5-18 Account Name: LTRANPHD$ Account Domain: WORKGROUP Logon ID: 0x3e7 Logon GUID: {00000000-0000-0000-0000-000000000000} Account Whose Credentials Were Used: Account Name: Liem Account Domain: LTRANPHD Logon GUID: {00000000-0000-0000-0000-000000000000} Target Server: Target Server Name: localhost Additional Information: localhost Process Information: Process ID: 0x210 Process Name: C:\Windows\System32\winlogon.exe Network Information: Network Address: 127.0.0.1 Port: 0 This event is generated when a process attempts to log on an account by explicitly specifying that account's credentials. This most commonly occurs in batch-type configurations such as scheduled tasks, or when using the RUNAS command.
Security	Audit Success	12544	2015-04-25 09:01:28	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: LTRANPHD$ Account Domain: WORKGROUP Logon ID: 0x3e7 Logon Type: 7 Impersonation Level: %%1833 New Logon: Security ID: S-1-5-21-1888849264-3803429180-4108621888-1001 Account Name: Liem Account Domain: LTRANPHD Logon ID: 0x12b868 Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x210 Process Name: C:\Windows\System32\winlogon.exe Network Information: Workstation Name: LTRANPHD Source Network Address: 127.0.0.1 Source Port: 0 Detailed Authentication Information: Logon Process: User32 Authentication Package: Negotiate Transited Services: - Package Name (NTLM only): - Key Length: 0 This event is generated when a logon session is created. It is generated on the computer that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service such as the Server service, or a local process such as Winlogon.exe or Services.exe. The logon type field indicates the kind of logon that occurred. The most common types are 2 (interactive) and 3 (network). The New Logon fields indicate the account for whom the new logon was created, i.e. the account that was logged on. The network fields indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impersonation level field indicates the extent to which a process in the logon session can impersonate. The authentication information fields provide detailed information about this specific logon request. - Logon GUID is a unique identifier that can be used to correlate this event with a KDC event. - Transited services indicate which intermediate services have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indicates the length of the generated session key. This will be 0 if no session key was requested.
Security	Audit Success	12544	2015-04-25 09:01:28	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: LTRANPHD$ Account Domain: WORKGROUP Logon ID: 0x3e7 Logon Type: 7 Impersonation Level: %%1833 New Logon: Security ID: S-1-5-21-1888849264-3803429180-4108621888-1001 Account Name: Liem Account Domain: LTRANPHD Logon ID: 0x12b886 Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x210 Process Name: C:\Windows\System32\winlogon.exe Network Information: Workstation Name: LTRANPHD Source Network Address: 127.0.0.1 Source Port: 0 Detailed Authentication Information: Logon Process: User32 Authentication Package: Negotiate Transited Services: - Package Name (NTLM only): - Key Length: 0 This event is generated when a logon session is created. It is generated on the computer that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service such as the Server service, or a local process such as Winlogon.exe or Services.exe. The logon type field indicates the kind of logon that occurred. The most common types are 2 (interactive) and 3 (network). The New Logon fields indicate the account for whom the new logon was created, i.e. the account that was logged on. The network fields indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impersonation level field indicates the extent to which a process in the logon session can impersonate. The authentication information fields provide detailed information about this specific logon request. - Logon GUID is a unique identifier that can be used to correlate this event with a KDC event. - Transited services indicate which intermediate services have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indicates the length of the generated session key. This will be 0 if no session key was requested.
Security	Audit Success	12545	2015-04-25 09:01:28	Microsoft-Windows-Security-Auditing	4634: An account was logged off. Subject: Security ID: S-1-5-21-1888849264-3803429180-4108621888-1001 Account Name: Liem Account Domain: LTRANPHD Logon ID: 0x12b886 Logon Type: 7 This event is generated when a logon session is destroyed. It may be positively correlated with a logon event using the Logon ID value. Logon IDs are only unique between reboots on the same computer.
Security	Audit Success	12545	2015-04-25 09:01:28	Microsoft-Windows-Security-Auditing	4634: An account was logged off. Subject: Security ID: S-1-5-21-1888849264-3803429180-4108621888-1001 Account Name: Liem Account Domain: LTRANPHD Logon ID: 0x12b868 Logon Type: 7 This event is generated when a logon session is destroyed. It may be positively correlated with a logon event using the Logon ID value. Logon IDs are only unique between reboots on the same computer.
	Audit		2015-04-	Microsoft-Windows-Security-	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-21-1888849264-3803429180-4108621888-1001 Account Name: Liem Account Domain: LTRANPHD Logon ID: 0x12b868 Privileges:

Security	Success	12548	25 09:01:28	Auditing	SeSecurityPrivilege SeTakeOwnershipPrivilege SeLoadDriverPrivilege SeBackupPrivilege SeRestorePrivilege SeDebugPrivilege SeSystemEnvironmentPrivilege SeImpersonatePrivilege
Security	Audit Success	12544	2015-04-25 09:02:48	Microsoft-Windows-Security-Auditing	4648: A logon was attempted using explicit credentials. Subject: Security ID: S-1-5-18 Account Name: LTRANPHD$ Account Domain: WORKGROUP Logon ID: 0x3e7 Logon GUID: {00000000-0000-0000-0000-000000000000} Account Whose Credentials Were Used: Account Name: Liem Account Domain: LTRANPHD Logon GUID: {00000000-0000-0000-0000-000000000000} Target Server: Target Server Name: localhost Additional Information: localhost Process Information: Process ID: 0x210 Process Name: C:\Windows\System32\winlogon.exe Network Information: Network Address: 127.0.0.1 Port: 0 This event is generated when a process attempts to log on an account by explicitly specifying that account's credentials. This most commonly occurs in batch-type configurations such as scheduled tasks, or when using the RUNAS command.
Security	Audit Success	12544	2015-04-25 09:02:48	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: LTRANPHD$ Account Domain: WORKGROUP Logon ID: 0x3e7 Logon Type: 7 Impersonation Level: %%1833 New Logon: Security ID: S-1-5-21-1888849264-3803429180-4108621888-1001 Account Name: Liem Account Domain: LTRANPHD Logon ID: 0x138668 Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x210 Process Name: C:\Windows\System32\winlogon.exe Network Information: Workstation Name: LTRANPHD Source Network Address: 127.0.0.1 Source Port: 0 Detailed Authentication Information: Logon Process: User32 Authentication Package: Negotiate Transited Services: - Package Name (NTLM only): - Key Length: 0 This event is generated when a logon session is created. It is generated on the computer that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service such as the Server service, or a local process such as Winlogon.exe or Services.exe. The logon type field indicates the kind of logon that occurred. The most common types are 2 (interactive) and 3 (network). The New Logon fields indicate the account for whom the new logon was created, i.e. the account that was logged on. The network fields indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impersonation level field indicates the extent to which a process in the logon session can impersonate. The authentication information fields provide detailed information about this specific logon request. - Logon GUID is a unique identifier that can be used to correlate this event with a KDC event. - Transited services indicate which intermediate services have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indicates the length of the generated session key. This will be 0 if no session key was requested.
Security	Audit Success	12544	2015-04-25 09:02:48	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: LTRANPHD$ Account Domain: WORKGROUP Logon ID: 0x3e7 Logon Type: 7 Impersonation Level: %%1833 New Logon: Security ID: S-1-5-21-1888849264-3803429180-4108621888-1001 Account Name: Liem Account Domain: LTRANPHD Logon ID: 0x138688 Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x210 Process Name: C:\Windows\System32\winlogon.exe Network Information: Workstation Name: LTRANPHD Source Network Address: 127.0.0.1 Source Port: 0 Detailed Authentication Information: Logon Process: User32 Authentication Package: Negotiate Transited Services: - Package Name (NTLM only): - Key Length: 0 This event is generated when a logon session is created. It is generated on the computer that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service such as the Server service, or a local process such as Winlogon.exe or Services.exe. The logon type field indicates the kind of logon that occurred. The most common types are 2 (interactive) and 3 (network). The New Logon fields indicate the account for whom the new logon was created, i.e. the account that was logged on. The network fields indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impersonation level field indicates the extent to which a process in the logon session can impersonate. The authentication information fields provide detailed information about this specific logon request. - Logon GUID is a unique identifier that can be used to correlate this event with a KDC event. - Transited services indicate which intermediate services have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indicates the length of the generated session key. This will be 0 if no session key was requested.
Security	Audit Success	12545	2015-04-25 09:02:48	Microsoft-Windows-Security-Auditing	4634: An account was logged off. Subject: Security ID: S-1-5-21-1888849264-3803429180-4108621888-1001 Account Name: Liem Account Domain: LTRANPHD Logon ID: 0x138688 Logon Type: 7 This event is generated when a logon session is destroyed. It may be positively correlated with a logon event using the Logon ID value. Logon IDs are only unique between reboots on the same computer.
Security	Audit Success	12545	2015-04-25 09:02:48	Microsoft-Windows-Security-Auditing	4634: An account was logged off. Subject: Security ID: S-1-5-21-1888849264-3803429180-4108621888-1001 Account Name: Liem Account Domain: LTRANPHD Logon ID: 0x138668 Logon Type: 7 This event is generated when a logon session is destroyed. It may be positively correlated with a logon event using the Logon ID value. Logon IDs are only unique between reboots on the same computer.
Security	Audit Success	12548	2015-04-25 09:02:48	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-21-1888849264-3803429180-4108621888-1001 Account Name: Liem Account Domain: LTRANPHD Logon ID: 0x138668 Privileges: SeSecurityPrivilege SeTakeOwnershipPrivilege SeLoadDriverPrivilege SeBackupPrivilege SeRestorePrivilege SeDebugPrivilege SeSystemEnvironmentPrivilege SeImpersonatePrivilege
					4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: LTRANPHD$ Account Domain: WORKGROUP Logon ID: 0x3e7 Logon Type: 5 Impersonation Level: %%1833 New Logon:

Security	Audit Success	12544	2015-04-25 09:13:04	Microsoft-Windows-Security-Auditing	Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Logon ID: 0x3e7 Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x240 Process Name: C:\Windows\System32\services.exe Network Information: Workstation Name: Source Network Address: - Source Port: - Detailed Authentication Information: Logon Process: Advapi Authentication Package: Negotiate Transited Services: - Package Name (NTLM only): - Key Length: 0 This event is generated when a logon session is created. It is generated on the computer that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service such as the Server service, or a local process such as Winlogon.exe or Services.exe. The logon type field indicates the kind of logon that occurred. The most common types are 2 (interactive) and 3 (network). The New Logon fields indicate the account for whom the new logon was created, i.e. the account that was logged on. The network fields indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impersonation level field indicates the extent to which a process in the logon session can impersonate. The authentication information fields provide detailed information about this specific logon request. - Logon GUID is a unique identifier that can be used to correlate this event with a KDC event. - Transited services indicate which intermediate services have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indicates the length of the generated session key. This will be 0 if no session key was requested.
Security	Audit Success	12548	2015-04-25 09:13:04	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Logon ID: 0x3e7 Privileges: SeAssignPrimaryTokenPrivilege SeTcbPrivilege SeSecurityPrivilege SeTakeOwnershipPrivilege SeLoadDriverPrivilege SeBackupPrivilege SeRestorePrivilege SeDebugPrivilege SeAuditPrivilege SeSystemEnvironmentPrivilege SeImpersonatePrivilege
Security	Audit Success	12544	2015-04-25 09:22:24	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: LTRANPHD$ Account Domain: WORKGROUP Logon ID: 0x3e7 Logon Type: 5 Impersonation Level: %%1833 New Logon: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Logon ID: 0x3e7 Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x240 Process Name: C:\Windows\System32\services.exe Network Information: Workstation Name: Source Network Address: - Source Port: - Detailed Authentication Information: Logon Process: Advapi Authentication Package: Negotiate Transited Services: - Package Name (NTLM only): - Key Length: 0 This event is generated when a logon session is created. It is generated on the computer that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service such as the Server service, or a local process such as Winlogon.exe or Services.exe. The logon type field indicates the kind of logon that occurred. The most common types are 2 (interactive) and 3 (network). The New Logon fields indicate the account for whom the new logon was created, i.e. the account that was logged on. The network fields indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impersonation level field indicates the extent to which a process in the logon session can impersonate. The authentication information fields provide detailed information about this specific logon request. - Logon GUID is a unique identifier that can be used to correlate this event with a KDC event. - Transited services indicate which intermediate services have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indicates the length of the generated session key. This will be 0 if no session key was requested.
Security	Audit Success	12548	2015-04-25 09:22:24	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Logon ID: 0x3e7 Privileges: SeAssignPrimaryTokenPrivilege SeTcbPrivilege SeSecurityPrivilege SeTakeOwnershipPrivilege SeLoadDriverPrivilege SeBackupPrivilege SeRestorePrivilege SeDebugPrivilege SeAuditPrivilege SeSystemEnvironmentPrivilege SeImpersonatePrivilege
Security	Audit Success	12544	2015-04-25 09:29:05	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: LTRANPHD$ Account Domain: WORKGROUP Logon ID: 0x3e7 Logon Type: 5 Impersonation Level: %%1833 New Logon: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Logon ID: 0x3e7 Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x240 Process Name: C:\Windows\System32\services.exe Network Information: Workstation Name: Source Network Address: - Source Port: - Detailed Authentication Information: Logon Process: Advapi Authentication Package: Negotiate Transited Services: - Package Name (NTLM only): - Key Length: 0 This event is generated when a logon session is created. It is generated on the computer that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service such as the Server service, or a local process such as Winlogon.exe or Services.exe. The logon type field indicates the kind of logon that occurred. The most common types are 2 (interactive) and 3 (network). The New Logon fields indicate the account for whom the new logon was created, i.e. the account that was logged on. The network fields indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impersonation level field indicates the extent to which a process in the logon session can impersonate. The authentication information fields provide detailed information about this specific logon request. - Logon GUID is a unique identifier that can be used to correlate this event with a KDC event. - Transited services indicate which intermediate services have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indicates the length of the generated session key. This will be 0 if no session key was requested.
Security	Audit Success	12548	2015-04-25 09:29:05	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Logon ID: 0x3e7 Privileges: SeAssignPrimaryTokenPrivilege SeTcbPrivilege SeSecurityPrivilege SeTakeOwnershipPrivilege SeLoadDriverPrivilege SeBackupPrivilege SeRestorePrivilege

					SeDebugPrivilege SeAuditPrivilege SeSystemEnvironmentPrivilege SeImpersonatePrivilege
Security	Audit Success	12288	2015-04-25 10:14:22	Microsoft-Windows-Security-Auditing	4608: Windows is starting up. This event is logged when LSASS.EXE starts and the auditing subsystem is initialized.
Security	Audit Success	12544	2015-04-25 10:14:22	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-0-0 Account Name: - Account Domain: - Logon ID: 0x0 Logon Type: 0 Impersonation Level: - New Logon: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Logon ID: 0x3e7 Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x4 Process Name: Network Information: Workstation Name: - Source Network Address: - Source Port: - Detailed Authentication Information: Logon Process: - Authentication Package: - Transited Services: - Package Name (NTLM only): - Key Length: 0 This event is generated when a logon session is created. It is generated on the computer that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service such as the Server service, or a local process such as Winlogon.exe or Services.exe. The logon type field indicates the kind of logon that occurred. The most common types are 2 (interactive) and 3 (network). The New Logon fields indicate the account for whom the new logon was created, i.e. the account that was logged on. The network fields indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impersonation level field indicates the extent to which a process in the logon session can impersonate. The authentication information fields provide detailed information about this specific logon request. - Logon GUID is a unique identifier that can be used to correlate this event with a KDC event. - Transited services indicate which intermediate services have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indicates the length of the generated session key. This will be 0 if no session key was requested.
Security	Audit Success	12544	2015-04-25 10:14:22	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: LTRANPHD$ Account Domain: WORKGROUP Logon ID: 0x3e7 Logon Type: 5 Impersonation Level: %%1833 New Logon: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Logon ID: 0x3e7 Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x238 Process Name: C:\Windows\System32\services.exe Network Information: Workstation Name: Source Network Address: - Source Port: - Detailed Authentication Information: Logon Process: Advapi Authentication Package: Negotiate Transited Services: - Package Name (NTLM only): - Key Length: 0 This event is generated when a logon session is created. It is generated on the computer that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service such as the Server service, or a local process such as Winlogon.exe or Services.exe. The logon type field indicates the kind of logon that occurred. The most common types are 2 (interactive) and 3 (network). The New Logon fields indicate the account for whom the new logon was created, i.e. the account that was logged on. The network fields indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impersonation level field indicates the extent to which a process in the logon session can impersonate. The authentication information fields provide detailed information about this specific logon request. - Logon GUID is a unique identifier that can be used to correlate this event with a KDC event. - Transited services indicate which intermediate services have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indicates the length of the generated session key. This will be 0 if no session key was requested.
Security	Audit Success	12544	2015-04-25 10:14:22	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: LTRANPHD$ Account Domain: WORKGROUP Logon ID: 0x3e7 Logon Type: 5 Impersonation Level: %%1833 New Logon: Security ID: S-1-5-20 Account Name: NETWORK SERVICE Account Domain: NT AUTHORITY Logon ID: 0x3e4 Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x238 Process Name: C:\Windows\System32\services.exe Network Information: Workstation Name: Source Network Address: - Source Port: - Detailed Authentication Information: Logon Process: Advapi Authentication Package: Negotiate Transited Services: - Package Name (NTLM only): - Key Length: 0 This event is generated when a logon session is created. It is generated on the computer that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service such as the Server service, or a local process such as Winlogon.exe or Services.exe. The logon type field indicates the kind of logon that occurred. The most common types are 2 (interactive) and 3 (network). The New Logon fields indicate the account for whom the new logon was created, i.e. the account that was logged on. The network fields indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impersonation level field indicates the extent to which a process in the logon session can impersonate. The authentication information fields provide detailed information about this specific logon request. - Logon GUID is a unique identifier that can be used to correlate this event with a KDC event. - Transited services indicate which intermediate services have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indicates the length of the generated session key. This will be 0 if no session key was requested.
Security	Audit Success	12544	2015-04-25 10:14:22	Microsoft-Windows-Security-Auditing	4648: A logon was attempted using explicit credentials. Subject: Security ID: S-1-5-18 Account Name: LTRANPHD$ Account Domain: WORKGROUP Logon ID: 0x3e7 Logon GUID: {00000000-0000-0000-0000-000000000000} Account Whose Credentials Were Used: Account Name: DWM-1 Account Domain: Window Manager Logon GUID: {00000000-0000-0000-0000-000000000000} Target Server: Target Server Name: localhost Additional Information: localhost Process Information: Process ID: 0x20c Process Name: C:\Windows\System32\winlogon.exe Network Information: Network Address: - Port: - This event is generated

					when a process attempts to log on an account by explicitly specifying that account's credentials. This most commonly occurs in batch-type configurations such as scheduled tasks, or when using the RUNAS command.
Security	Audit Success	12544	2015-04-25 10:14:22	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: LTRANPHD$ Account Domain: WORKGROUP Logon ID: 0x3e7 Logon Type: 2 Impersonation Level: %%1833 New Logon: Security ID: S-1-5-90-1 Account Name: DWM-1 Account Domain: Window Manager Logon ID: 0xd60c Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x20c Process Name: C:\Windows\System32\winlogon.exe Network Information: Workstation Name: Source Network Address: - Source Port: - Detailed Authentication Information: Logon Process: Advapi Authentication Package: Negotiate Transited Services: - Package Name (NTLM only): - Key Length: 0 This event is generated when a logon session is created. It is generated on the computer that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service such as the Server service, or a local process such as Winlogon.exe or Services.exe. The logon type field indicates the kind of logon that occurred. The most common types are 2 (interactive) and 3 (network). The New Logon fields indicate the account for whom the new logon was created, i.e. the account that was logged on. The network fields indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impersonation level field indicates the extent to which a process in the logon session can impersonate. The authentication information fields provide detailed information about this specific logon request. - Logon GUID is a unique identifier that can be used to correlate this event with a KDC event. - Transited services indicate which intermediate services have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indicates the length of the generated session key. This will be 0 if no session key was requested.
Security	Audit Success	12544	2015-04-25 10:14:22	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: LTRANPHD$ Account Domain: WORKGROUP Logon ID: 0x3e7 Logon Type: 2 Impersonation Level: %%1833 New Logon: Security ID: S-1-5-90-1 Account Name: DWM-1 Account Domain: Window Manager Logon ID: 0xd63b Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x20c Process Name: C:\Windows\System32\winlogon.exe Network Information: Workstation Name: Source Network Address: - Source Port: - Detailed Authentication Information: Logon Process: Advapi Authentication Package: Negotiate Transited Services: - Package Name (NTLM only): - Key Length: 0 This event is generated when a logon session is created. It is generated on the computer that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service such as the Server service, or a local process such as Winlogon.exe or Services.exe. The logon type field indicates the kind of logon that occurred. The most common types are 2 (interactive) and 3 (network). The New Logon fields indicate the account for whom the new logon was created, i.e. the account that was logged on. The network fields indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impersonation level field indicates the extent to which a process in the logon session can impersonate. The authentication information fields provide detailed information about this specific logon request. - Logon GUID is a unique identifier that can be used to correlate this event with a KDC event. - Transited services indicate which intermediate services have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indicates the length of the generated session key. This will be 0 if no session key was requested.
Security	Audit Success	12544	2015-04-25 10:14:22	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: LTRANPHD$ Account Domain: WORKGROUP Logon ID: 0x3e7 Logon Type: 5 Impersonation Level: %%1833 New Logon: Security ID: S-1-5-19 Account Name: LOCAL SERVICE Account Domain: NT AUTHORITY Logon ID: 0x3e5 Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x238 Process Name: C:\Windows\System32\services.exe Network Information: Workstation Name: Source Network Address: - Source Port: - Detailed Authentication Information: Logon Process: Advapi Authentication Package: Negotiate Transited Services: - Package Name (NTLM only): - Key Length: 0 This event is generated when a logon session is created. It is generated on the computer that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service such as the Server service, or a local process such as Winlogon.exe or Services.exe. The logon type field indicates the kind of logon that occurred. The most common types are 2 (interactive) and 3 (network). The New Logon fields indicate the account for whom the new logon was created, i.e. the account that was logged on. The network fields indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impersonation level field indicates the extent to which a process in the logon session can impersonate. The authentication information fields provide detailed information about this specific logon request. - Logon GUID is a unique identifier that can be used to correlate this event with a KDC event. - Transited services indicate which intermediate services have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indicates the length of the generated session key. This will be 0 if no session key was requested.
					4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: LTRANPHD$ Account Domain: WORKGROUP Logon ID: 0x3e7 Logon Type: 5 Impersonation Level: %%1833 New Logon: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Logon ID: 0x3e7 Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x238 Process Name: C:\Windows\System32\services.exe Network Information: Workstation Name: Source Network Address: - Source Port: - Detailed Authentication Information: Logon Process: Advapi Authentication Package: Negotiate Transited Services: - Package Name (NTLM only): - Key Length: 0 This event is generated when a logon session is created. It is generated on the computer that was accessed. The subject fields indicate the account on the local

Security	Audit Success	12544	2015-04-25 10:14:22	Microsoft-Windows-Security-Auditing	system which requested the logon. This is most commonly a service such as the Server service, or a local process such as Winlogon.exe or Services.exe. The logon type field indicates the kind of logon that occurred. The most common types are 2 (interactive) and 3 (network). The New Logon fields indicate the account for whom the new logon was created, i.e. the account that was logged on. The network fields indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impersonation level field indicates the extent to which a process in the logon session can impersonate. The authentication information fields provide detailed information about this specific logon request. - Logon GUID is a unique identifier that can be used to correlate this event with a KDC event. - Transited services indicate which intermediate services have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indicates the length of the generated session key. This will be 0 if no session key was requested.
Security	Audit Success	12544	2015-04-25 10:14:22	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: LTRANPHD$ Account Domain: WORKGROUP Logon ID: 0x3e7 Logon Type: 5 Impersonation Level: %%1833 New Logon: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Logon ID: 0x3e7 Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x238 Process Name: C:\Windows\System32\services.exe Network Information: Workstation Name: Source Network Address: - Source Port: - Detailed Authentication Information: Logon Process: Advapi Authentication Package: Negotiate Transited Services: - Package Name (NTLM only): - Key Length: 0 This event is generated when a logon session is created. It is generated on the computer that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service such as the Server service, or a local process such as Winlogon.exe or Services.exe. The logon type field indicates the kind of logon that occurred. The most common types are 2 (interactive) and 3 (network). The New Logon fields indicate the account for whom the new logon was created, i.e. the account that was logged on. The network fields indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impersonation level field indicates the extent to which a process in the logon session can impersonate. The authentication information fields provide detailed information about this specific logon request. - Logon GUID is a unique identifier that can be used to correlate this event with a KDC event. - Transited services indicate which intermediate services have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indicates the length of the generated session key. This will be 0 if no session key was requested.
Security	Audit Success	12544	2015-04-25 10:14:22	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: LTRANPHD$ Account Domain: WORKGROUP Logon ID: 0x3e7 Logon Type: 5 Impersonation Level: %%1833 New Logon: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Logon ID: 0x3e7 Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x238 Process Name: C:\Windows\System32\services.exe Network Information: Workstation Name: Source Network Address: - Source Port: - Detailed Authentication Information: Logon Process: Advapi Authentication Package: Negotiate Transited Services: - Package Name (NTLM only): - Key Length: 0 This event is generated when a logon session is created. It is generated on the computer that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service such as the Server service, or a local process such as Winlogon.exe or Services.exe. The logon type field indicates the kind of logon that occurred. The most common types are 2 (interactive) and 3 (network). The New Logon fields indicate the account for whom the new logon was created, i.e. the account that was logged on. The network fields indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impersonation level field indicates the extent to which a process in the logon session can impersonate. The authentication information fields provide detailed information about this specific logon request. - Logon GUID is a unique identifier that can be used to correlate this event with a KDC event. - Transited services indicate which intermediate services have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indicates the length of the generated session key. This will be 0 if no session key was requested.
Security	Audit Success	12548	2015-04-25 10:14:22	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Logon ID: 0x3e7 Privileges: SeAssignPrimaryTokenPrivilege SeTcbPrivilege SeSecurityPrivilege SeTakeOwnershipPrivilege SeLoadDriverPrivilege SeBackupPrivilege SeRestorePrivilege SeDebugPrivilege SeAuditPrivilege SeSystemEnvironmentPrivilege SeImpersonatePrivilege
Security	Audit Success	12548	2015-04-25 10:14:22	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-20 Account Name: NETWORK SERVICE Account Domain: NT AUTHORITY Logon ID: 0x3e4 Privileges: SeAssignPrimaryTokenPrivilege SeAuditPrivilege SeImpersonatePrivilege
Security	Audit Success	12548	2015-04-25 10:14:22	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-90-1 Account Name: DWM-1 Account Domain: Window Manager Logon ID: 0xd60c Privileges: SeAssignPrimaryTokenPrivilege SeAuditPrivilege SeImpersonatePrivilege
Security	Audit Success	12548	2015-04-25 10:14:22	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-90-1 Account Name: DWM-1 Account Domain: Window Manager Logon ID: 0xd63b Privileges: SeAssignPrimaryTokenPrivilege SeAuditPrivilege
Security	Audit Success	12548	2015-04-25 10:14:22	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-19 Account Name: LOCAL SERVICE Account Domain: NT AUTHORITY Logon ID: 0x3e5 Privileges: SeAssignPrimaryTokenPrivilege SeAuditPrivilege SeImpersonatePrivilege
					4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account

Security	Audit Success	12548	2015-04-25 10:14:22	Microsoft-Windows-Security-Auditing	Domain: NT AUTHORITY Logon ID: 0x3e7 Privileges: SeAssignPrimaryTokenPrivilege SeTcbPrivilege SeSecurityPrivilege SeTakeOwnershipPrivilege SeLoadDriverPrivilege SeBackupPrivilege SeRestorePrivilege SeDebugPrivilege SeAuditPrivilege SeSystemEnvironmentPrivilege SeImpersonatePrivilege
Security	Audit Success	12548	2015-04-25 10:14:22	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Logon ID: 0x3e7 Privileges: SeAssignPrimaryTokenPrivilege SeTcbPrivilege SeSecurityPrivilege SeTakeOwnershipPrivilege SeLoadDriverPrivilege SeBackupPrivilege SeRestorePrivilege SeDebugPrivilege SeAuditPrivilege SeSystemEnvironmentPrivilege SeImpersonatePrivilege
Security	Audit Success	12548	2015-04-25 10:14:22	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Logon ID: 0x3e7 Privileges: SeAssignPrimaryTokenPrivilege SeTcbPrivilege SeSecurityPrivilege SeTakeOwnershipPrivilege SeLoadDriverPrivilege SeBackupPrivilege SeRestorePrivilege SeDebugPrivilege SeAuditPrivilege SeSystemEnvironmentPrivilege SeImpersonatePrivilege
Security	Audit Success	13568	2015-04-25 10:14:22	Microsoft-Windows-Security-Auditing	4902: The Per-user audit policy table was created. Number of Elements: 0 Policy ID: 0x83b0
Security	Audit Success	12292	2015-04-25 10:14:25	Microsoft-Windows-Security-Auditing	5033: The Windows Firewall Driver started successfully.
Security	Audit Success	12292	2015-04-25 10:14:25	Microsoft-Windows-Security-Auditing	5024: The Windows Firewall service started successfully.
Security	Audit Success	12544	2015-04-25 10:14:25	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: LTRANPHD$ Account Domain: WORKGROUP Logon ID: 0x3e7 Logon Type: 5 Impersonation Level: %%1833 New Logon: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Logon ID: 0x3e7 Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x238 Process Name: C:\Windows\System32\services.exe Network Information: Workstation Name: Source Network Address: - Source Port: - Detailed Authentication Information: Logon Process: Advapi Authentication Package: Negotiate Transited Services: - Package Name (NTLM only): - Key Length: 0 This event is generated when a logon session is created. It is generated on the computer that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service such as the Server service, or a local process such as Winlogon.exe or Services.exe. The logon type field indicates the kind of logon that occurred. The most common types are 2 (interactive) and 3 (network). The New Logon fields indicate the account for whom the new logon was created, i.e. the account that was logged on. The network fields indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impersonation level field indicates the extent to which a process in the logon session can impersonate. The authentication information fields provide detailed information about this specific logon request. - Logon GUID is a unique identifier that can be used to correlate this event with a KDC event. - Transited services indicate which intermediate services have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indicates the length of the generated session key. This will be 0 if no session key was requested.
Security	Audit Success	12544	2015-04-25 10:14:25	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: LTRANPHD$ Account Domain: WORKGROUP Logon ID: 0x3e7 Logon Type: 5 Impersonation Level: %%1833 New Logon: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Logon ID: 0x3e7 Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x238 Process Name: C:\Windows\System32\services.exe Network Information: Workstation Name: Source Network Address: - Source Port: - Detailed Authentication Information: Logon Process: Advapi Authentication Package: Negotiate Transited Services: - Package Name (NTLM only): - Key Length: 0 This event is generated when a logon session is created. It is generated on the computer that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service such as the Server service, or a local process such as Winlogon.exe or Services.exe. The logon type field indicates the kind of logon that occurred. The most common types are 2 (interactive) and 3 (network). The New Logon fields indicate the account for whom the new logon was created, i.e. the account that was logged on. The network fields indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impersonation level field indicates the extent to which a process in the logon session can impersonate. The authentication information fields provide detailed information about this specific logon request. - Logon GUID is a unique identifier that can be used to correlate this event with a KDC event. - Transited services indicate which intermediate services have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indicates the length of the generated session key. This will be 0 if no session key was requested.
					4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: LTRANPHD$ Account Domain: WORKGROUP Logon ID: 0x3e7 Logon Type: 5 Impersonation Level: %%1833 New Logon: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Logon ID: 0x3e7 Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x238 Process Name: C:\Windows\System32\services.exe Network Information: Workstation Name: Source Network Address: - Source Port: - Detailed Authentication Information: Logon Process: Advapi Authentication Package: Negotiate Transited Services: - Package Name (NTLM only): - Key Length: 0 This event is generated when a logon session is

Security	Audit Success	12544	2015-04-25 10:14:25	Microsoft-Windows-Security-Auditing	created. It is generated on the computer that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service such as the Server service, or a local process such as Winlogon.exe or Services.exe. The logon type field indicates the kind of logon that occurred. The most common types are 2 (interactive) and 3 (network). The New Logon fields indicate the account for whom the new logon was created, i.e. the account that was logged on. The network fields indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impersonation level field indicates the extent to which a process in the logon session can impersonate. The authentication information fields provide detailed information about this specific logon request. - Logon GUID is a unique identifier that can be used to correlate this event with a KDC event. - Transited services indicate which intermediate services have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indicates the length of the generated session key. This will be 0 if no session key was requested.
Security	Audit Success	12544	2015-04-25 10:14:25	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-0-0 Account Name: - Account Domain: - Logon ID: 0x0 Logon Type: 3 Impersonation Level: %%1833 New Logon: Security ID: S-1-5-7 Account Name: ANONYMOUS LOGON Account Domain: NT AUTHORITY Logon ID: 0x197e3 Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x0 Process Name: - Network Information: Workstation Name: Source Network Address: - Source Port: - Detailed Authentication Information: Logon Process: NtLmSsp Authentication Package: NTLM Transited Services: - Package Name (NTLM only): NTLM V1 Key Length: 0 This event is generated when a logon session is created. It is generated on the computer that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service such as the Server service, or a local process such as Winlogon.exe or Services.exe. The logon type field indicates the kind of logon that occurred. The most common types are 2 (interactive) and 3 (network). The New Logon fields indicate the account for whom the new logon was created, i.e. the account that was logged on. The network fields indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impersonation level field indicates the extent to which a process in the logon session can impersonate. The authentication information fields provide detailed information about this specific logon request. - Logon GUID is a unique identifier that can be used to correlate this event with a KDC event. - Transited services indicate which intermediate services have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indicates the length of the generated session key. This will be 0 if no session key was requested.
Security	Audit Success	12548	2015-04-25 10:14:25	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Logon ID: 0x3e7 Privileges: SeAssignPrimaryTokenPrivilege SeTcbPrivilege SeSecurityPrivilege SeTakeOwnershipPrivilege SeLoadDriverPrivilege SeBackupPrivilege SeRestorePrivilege SeDebugPrivilege SeAuditPrivilege SeSystemEnvironmentPrivilege SeImpersonatePrivilege
Security	Audit Success	12548	2015-04-25 10:14:25	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Logon ID: 0x3e7 Privileges: SeAssignPrimaryTokenPrivilege SeTcbPrivilege SeSecurityPrivilege SeTakeOwnershipPrivilege SeLoadDriverPrivilege SeBackupPrivilege SeRestorePrivilege SeDebugPrivilege SeAuditPrivilege SeSystemEnvironmentPrivilege SeImpersonatePrivilege
Security	Audit Success	12548	2015-04-25 10:14:25	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Logon ID: 0x3e7 Privileges: SeAssignPrimaryTokenPrivilege SeTcbPrivilege SeSecurityPrivilege SeTakeOwnershipPrivilege SeLoadDriverPrivilege SeBackupPrivilege SeRestorePrivilege SeDebugPrivilege SeAuditPrivilege SeSystemEnvironmentPrivilege SeImpersonatePrivilege
Security	Audit Success	12544	2015-04-25 10:14:29	Microsoft-Windows-Security-Auditing	4648: A logon was attempted using explicit credentials. Subject: Security ID: S-1-5-18 Account Name: LTRANPHD$ Account Domain: WORKGROUP Logon ID: 0x3e7 Logon GUID: {00000000-0000-0000-0000-000000000000} Account Whose Credentials Were Used: Account Name: Liem Account Domain: LTRANPHD Logon GUID: {00000000-0000-0000-0000-000000000000} Target Server: Target Server Name: localhost Additional Information: localhost Process Information: Process ID: 0x20c Process Name: C:\Windows\System32\winlogon.exe Network Information: Network Address: 127.0.0.1 Port: 0 This event is generated when a process attempts to log on an account by explicitly specifying that account's credentials. This most commonly occurs in batch-type configurations such as scheduled tasks, or when using the RUNAS command.
Security	Audit Success	12544	2015-04-25 10:14:29	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: LTRANPHD$ Account Domain: WORKGROUP Logon ID: 0x3e7 Logon Type: 2 Impersonation Level: %%1833 New Logon: Security ID: S-1-5-21-1888849264-3803429180-4108621888-1001 Account Name: Liem Account Domain: LTRANPHD Logon ID: 0x1dd6f Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x20c Process Name: C:\Windows\System32\winlogon.exe Network Information: Workstation Name: LTRANPHD Source Network Address: 127.0.0.1 Source Port: 0 Detailed Authentication Information: Logon Process: User32 Authentication Package: Negotiate Transited Services: - Package Name (NTLM only): - Key Length: 0 This event is generated when a logon session is created. It is generated on the computer that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service such as the Server service, or a local process such as Winlogon.exe or Services.exe. The logon type field indicates the kind of logon that occurred. The most common types are 2 (interactive) and 3 (network). The New Logon fields indicate the account for whom the new logon was created, i.e. the account that was logged on. The network fields indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impersonation level field indicates the extent to which a process in the logon session can impersonate. The authentication information fields provide detailed

					information about this specific logon request. - Logon GUID is a unique identifier that can be used to correlate this event with a KDC event. - Transited services indicate which intermediate services have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indicates the length of the generated session key. This will be 0 if no session key was requested.
Security	Audit Success	12544	2015-04-25 10:14:29	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: LTRANPHD$ Account Domain: WORKGROUP Logon ID: 0x3e7 Logon Type: 2 Impersonation Level: %%1833 New Logon: Security ID: S-1-5-21-1888849264-3803429180-4108621888-1001 Account Name: Liem Account Domain: LTRANPHD Logon ID: 0x1dd9e Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x20c Process Name: C:\Windows\System32\winlogon.exe Network Information: Workstation Name: LTRANPHD Source Network Address: 127.0.0.1 Source Port: 0 Detailed Authentication Information: Logon Process: User32 Authentication Package: Negotiate Transited Services: - Package Name (NTLM only): - Key Length: 0 This event is generated when a logon session is created. It is generated on the computer that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service such as the Server service, or a local process such as Winlogon.exe or Services.exe. The logon type field indicates the kind of logon that occurred. The most common types are 2 (interactive) and 3 (network). The New Logon fields indicate the account for whom the new logon was created, i.e. the account that was logged on. The network fields indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impersonation level field indicates the extent to which a process in the logon session can impersonate. The authentication information fields provide detailed information about this specific logon request. - Logon GUID is a unique identifier that can be used to correlate this event with a KDC event. - Transited services indicate which intermediate services have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indicates the length of the generated session key. This will be 0 if no session key was requested.
Security	Audit Success	12544	2015-04-25 10:14:29	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: LTRANPHD$ Account Domain: WORKGROUP Logon ID: 0x3e7 Logon Type: 5 Impersonation Level: %%1833 New Logon: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Logon ID: 0x3e7 Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x238 Process Name: C:\Windows\System32\services.exe Network Information: Workstation Name: Source Network Address: - Source Port: - Detailed Authentication Information: Logon Process: Advapi Authentication Package: Negotiate Transited Services: - Package Name (NTLM only): - Key Length: 0 This event is generated when a logon session is created. It is generated on the computer that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service such as the Server service, or a local process such as Winlogon.exe or Services.exe. The logon type field indicates the kind of logon that occurred. The most common types are 2 (interactive) and 3 (network). The New Logon fields indicate the account for whom the new logon was created, i.e. the account that was logged on. The network fields indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impersonation level field indicates the extent to which a process in the logon session can impersonate. The authentication information fields provide detailed information about this specific logon request. - Logon GUID is a unique identifier that can be used to correlate this event with a KDC event. - Transited services indicate which intermediate services have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indicates the length of the generated session key. This will be 0 if no session key was requested.
Security	Audit Success	12548	2015-04-25 10:14:29	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-21-1888849264-3803429180-4108621888-1001 Account Name: Liem Account Domain: LTRANPHD Logon ID: 0x1dd6f Privileges: SeSecurityPrivilege SeTakeOwnershipPrivilege SeLoadDriverPrivilege SeBackupPrivilege SeRestorePrivilege SeDebugPrivilege SeSystemEnvironmentPrivilege SeImpersonatePrivilege
Security	Audit Success	12548	2015-04-25 10:14:29	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Logon ID: 0x3e7 Privileges: SeAssignPrimaryTokenPrivilege SeTcbPrivilege SeSecurityPrivilege SeTakeOwnershipPrivilege SeLoadDriverPrivilege SeBackupPrivilege SeRestorePrivilege SeDebugPrivilege SeAuditPrivilege SeSystemEnvironmentPrivilege SeImpersonatePrivilege
Security	Audit Success	13824	2015-04-25 10:14:31	Microsoft-Windows-Security-Auditing	4797: An attempt was made to query the existence of a blank password for an account. Subject: Security ID: S-1-5-21-1888849264-3803429180-4108621888-1001 Account Name: Liem Account Domain: LTRANPHD Logon ID: 0x1dd9e Additional Information: Caller Workstation: LTRANPHD Target Account Name: Administrator Target Account Domain: LTRANPHD
Security	Audit Success	13824	2015-04-25 10:14:31	Microsoft-Windows-Security-Auditing	4797: An attempt was made to query the existence of a blank password for an account. Subject: Security ID: S-1-5-21-1888849264-3803429180-4108621888-1001 Account Name: Liem Account Domain: LTRANPHD Logon ID: 0x1dd9e Additional Information: Caller Workstation: LTRANPHD Target Account Name: Guest Target Account Domain: LTRANPHD
Security	Audit Success	13824	2015-04-25 10:14:31	Microsoft-Windows-Security-Auditing	4797: An attempt was made to query the existence of a blank password for an account. Subject: Security ID: S-1-5-21-1888849264-3803429180-4108621888-1001 Account Name: Liem Account Domain: LTRANPHD Logon ID: 0x1dd9e Additional Information: Caller Workstation: LTRANPHD Target Account Name: Administrator Target Account Domain: LTRANPHD
Security	Audit Success	13824	2015-04-25 10:14:31	Microsoft-Windows-Security-Auditing	4797: An attempt was made to query the existence of a blank password for an account. Subject: Security ID: S-1-5-21-1888849264-3803429180-4108621888-1001 Account Name: Liem Account Domain: LTRANPHD Logon ID: 0x1dd9e Additional Information: Caller Workstation: LTRANPHD Target Account Name: Guest Target Account Domain: LTRANPHD

Security	Audit Success	13824	2015-04-25 10:14:33	Microsoft-Windows-Security-Auditing	4797: An attempt was made to query the existence of a blank password for an account. Subject: Security ID: S-1-5-19 Account Name: LOCAL SERVICE Account Domain: NT AUTHORITY Logon ID: 0x3e5 Additional Information: Caller Workstation: LTRANPHD Target Account Name: Administrator Target Account Domain: LTRANPHD
Security	Audit Success	13824	2015-04-25 10:14:33	Microsoft-Windows-Security-Auditing	4797: An attempt was made to query the existence of a blank password for an account. Subject: Security ID: S-1-5-19 Account Name: LOCAL SERVICE Account Domain: NT AUTHORITY Logon ID: 0x3e5 Additional Information: Caller Workstation: LTRANPHD Target Account Name: Administrator Target Account Domain: LTRANPHD
Security	Audit Success	13824	2015-04-25 10:14:33	Microsoft-Windows-Security-Auditing	4797: An attempt was made to query the existence of a blank password for an account. Subject: Security ID: S-1-5-19 Account Name: LOCAL SERVICE Account Domain: NT AUTHORITY Logon ID: 0x3e5 Additional Information: Caller Workstation: LTRANPHD Target Account Name: Guest Target Account Domain: LTRANPHD
Security	Audit Success	13824	2015-04-25 10:14:33	Microsoft-Windows-Security-Auditing	4797: An attempt was made to query the existence of a blank password for an account. Subject: Security ID: S-1-5-19 Account Name: LOCAL SERVICE Account Domain: NT AUTHORITY Logon ID: 0x3e5 Additional Information: Caller Workstation: LTRANPHD Target Account Name: Guest Target Account Domain: LTRANPHD
Security	Audit Success	13824	2015-04-25 10:14:33	Microsoft-Windows-Security-Auditing	4797: An attempt was made to query the existence of a blank password for an account. Subject: Security ID: S-1-5-19 Account Name: LOCAL SERVICE Account Domain: NT AUTHORITY Logon ID: 0x3e5 Additional Information: Caller Workstation: LTRANPHD Target Account Name: Liem Target Account Domain: LTRANPHD
Security	Audit Success	13824	2015-04-25 10:14:33	Microsoft-Windows-Security-Auditing	4797: An attempt was made to query the existence of a blank password for an account. Subject: Security ID: S-1-5-19 Account Name: LOCAL SERVICE Account Domain: NT AUTHORITY Logon ID: 0x3e5 Additional Information: Caller Workstation: LTRANPHD Target Account Name: Liem Target Account Domain: LTRANPHD
Security	Audit Success	13824	2015-04-25 10:14:33	Microsoft-Windows-Security-Auditing	4797: An attempt was made to query the existence of a blank password for an account. Subject: Security ID: S-1-5-19 Account Name: LOCAL SERVICE Account Domain: NT AUTHORITY Logon ID: 0x3e5 Additional Information: Caller Workstation: LTRANPHD Target Account Name: Liem Target Account Domain: LTRANPHD
Security	Audit Success	13824	2015-04-25 10:14:33	Microsoft-Windows-Security-Auditing	4797: An attempt was made to query the existence of a blank password for an account. Subject: Security ID: S-1-5-19 Account Name: LOCAL SERVICE Account Domain: NT AUTHORITY Logon ID: 0x3e5 Additional Information: Caller Workstation: LTRANPHD Target Account Name: Liem Target Account Domain: LTRANPHD
Security	Audit Success	12544	2015-04-25 10:20:36	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: LTRANPHD$ Account Domain: WORKGROUP Logon ID: 0x3e7 Logon Type: 5 Impersonation Level: %%1833 New Logon: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Logon ID: 0x3e7 Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x238 Process Name: C:\Windows\System32\services.exe Network Information: Workstation Name: Source Network Address: - Source Port: - Detailed Authentication Information: Logon Process: Advapi Authentication Package: Negotiate Transited Services: - Package Name (NTLM only): - Key Length: 0 This event is generated when a logon session is created. It is generated on the computer that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service such as the Server service, or a local process such as Winlogon.exe or Services.exe. The logon type field indicates the kind of logon that occurred. The most common types are 2 (interactive) and 3 (network). The New Logon fields indicate the account for whom the new logon was created, i.e. the account that was logged on. The network fields indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impersonation level field indicates the extent to which a process in the logon session can impersonate. The authentication information fields provide detailed information about this specific logon request. - Logon GUID is a unique identifier that can be used to correlate this event with a KDC event. - Transited services indicate which intermediate services have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indicates the length of the generated session key. This will be 0 if no session key was requested.
Security	Audit Success	12548	2015-04-25 10:20:36	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Logon ID: 0x3e7 Privileges: SeAssignPrimaryTokenPrivilege SeTcbPrivilege SeSecurityPrivilege SeTakeOwnershipPrivilege SeLoadDriverPrivilege SeBackupPrivilege SeRestorePrivilege SeDebugPrivilege SeAuditPrivilege SeSystemEnvironmentPrivilege SeImpersonatePrivilege
Security	Audit Success	12544	2015-04-25 10:20:37	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: LTRANPHD$ Account Domain: WORKGROUP Logon ID: 0x3e7 Logon Type: 5 Impersonation Level: %%1833 New Logon: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Logon ID: 0x3e7 Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x238 Process Name: C:\Windows\System32\services.exe Network Information: Workstation Name: Source Network Address: - Source Port: - Detailed Authentication Information: Logon Process: Advapi Authentication Package: Negotiate Transited Services: - Package Name (NTLM only): - Key Length: 0 This event is generated when a logon session is created. It is generated on the computer that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service such as the Server service, or a local process such as Winlogon.exe or Services.exe. The logon type field indicates the kind of logon that occurred. The most common types are 2 (interactive) and 3 (network). The New Logon fields indicate the account for whom the new logon was created, i.e. the account that was logged on. The network fields indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impersonation level field indicates the extent to which a process in the logon session can impersonate. The authentication information fields provide detailed information about this specific logon request. - Logon GUID is a unique identifier that can be used to correlate this event with a KDC event. - Transited

					services indicate which intermediate services have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indicates the length of the generated session key. This will be 0 if no session key was requested.
Security	Audit Success	12548	2015-04-25 10:20:37	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Logon ID: 0x3e7 Privileges: SeAssignPrimaryTokenPrivilege SeTcbPrivilege SeSecurityPrivilege SeTakeOwnershipPrivilege SeLoadDriverPrivilege SeBackupPrivilege SeRestorePrivilege SeDebugPrivilege SeAuditPrivilege SeSystemEnvironmentPrivilege SeImpersonatePrivilege
Security	Audit Success	12545	2015-04-25 10:37:47	Microsoft-Windows-Security-Auditing	4647: User initiated logoff: Subject: Security ID: S-1-5-21-1888849264-3803429180-4108621888-1001 Account Name: Liem Account Domain: LTRANPHD Logon ID: 0x1dd9e This event is generated when a logoff is initiated. No further user-initiated activity can occur. This event can be interpreted as a logoff event.
Security	Audit Success	103	2015-04-25 10:37:48	Microsoft-Windows-Eventlog	1100: The event logging service has shut down.
Security	Audit Success	12288	2015-04-25 10:37:59	Microsoft-Windows-Security-Auditing	4608: Windows is starting up. This event is logged when LSASS.EXE starts and the auditing subsystem is initialized.
Security	Audit Success	12544	2015-04-25 10:37:59	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-0-0 Account Name: - Account Domain: - Logon ID: 0x0 Logon Type: 0 Impersonation Level: - New Logon: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Logon ID: 0x3e7 Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x4 Process Name: Network Information: Workstation Name: - Source Network Address: - Source Port: - Detailed Authentication Information: Logon Process: - Authentication Package: - Transited Services: - Package Name (NTLM only): - Key Length: 0 This event is generated when a logon session is created. It is generated on the computer that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service such as the Server service, or a local process such as Winlogon.exe or Services.exe. The logon type field indicates the kind of logon that occurred. The most common types are 2 (interactive) and 3 (network). The New Logon fields indicate the account for whom the new logon was created, i.e. the account that was logged on. The network fields indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impersonation level field indicates the extent to which a process in the logon session can impersonate. The authentication information fields provide detailed information about this specific logon request. - Logon GUID is a unique identifier that can be used to correlate this event with a KDC event. - Transited services indicate which intermediate services have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indicates the length of the generated session key. This will be 0 if no session key was requested.
Security	Audit Success	12544	2015-04-25 10:37:59	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: LTRANPHD$ Account Domain: WORKGROUP Logon ID: 0x3e7 Logon Type: 5 Impersonation Level: %%1833 New Logon: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Logon ID: 0x3e7 Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x240 Process Name: C:\Windows\System32\services.exe Network Information: Workstation Name: Source Network Address: - Source Port: - Detailed Authentication Information: Logon Process: Advapi Authentication Package: Negotiate Transited Services: - Package Name (NTLM only): - Key Length: 0 This event is generated when a logon session is created. It is generated on the computer that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service such as the Server service, or a local process such as Winlogon.exe or Services.exe. The logon type field indicates the kind of logon that occurred. The most common types are 2 (interactive) and 3 (network). The New Logon fields indicate the account for whom the new logon was created, i.e. the account that was logged on. The network fields indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impersonation level field indicates the extent to which a process in the logon session can impersonate. The authentication information fields provide detailed information about this specific logon request. - Logon GUID is a unique identifier that can be used to correlate this event with a KDC event. - Transited services indicate which intermediate services have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indicates the length of the generated session key. This will be 0 if no session key was requested.
Security	Audit Success	12544	2015-04-25 10:37:59	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: LTRANPHD$ Account Domain: WORKGROUP Logon ID: 0x3e7 Logon Type: 5 Impersonation Level: %%1833 New Logon: Security ID: S-1-5-20 Account Name: NETWORK SERVICE Account Domain: NT AUTHORITY Logon ID: 0x3e4 Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x240 Process Name: C:\Windows\System32\services.exe Network Information: Workstation Name: Source Network Address: - Source Port: - Detailed Authentication Information: Logon Process: Advapi Authentication Package: Negotiate Transited Services: - Package Name (NTLM only): - Key Length: 0 This event is generated when a logon session is created. It is generated on the computer that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service such as the Server service, or a local process such as Winlogon.exe or Services.exe. The logon type field indicates the kind of logon that occurred. The most common types are 2 (interactive) and 3 (network). The New Logon fields indicate the account for whom the new logon was created, i.e. the account that was logged on. The network fields indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some

					cases. The impersonation level field indicates the extent to which a process in the logon session can impersonate. The authentication information fields provide detailed information about this specific logon request. - Logon GUID is a unique identifier that can be used to correlate this event with a KDC event. - Transited services indicate which intermediate services have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indicates the length of the generated session key. This will be 0 if no session key was requested.
Security	Audit Success	12544	2015-04-25 10:37:59	Microsoft-Windows-Security-Auditing	4648: A logon was attempted using explicit credentials. Subject: Security ID: S-1-5-18 Account Name: LTRANPHD$ Account Domain: WORKGROUP Logon ID: 0x3e7 Logon GUID: {00000000-0000-0000-0000-000000000000} Account Whose Credentials Were Used: Account Name: DWM-1 Account Domain: Window Manager Logon GUID: {00000000-0000-0000-0000-000000000000} Target Server: Target Server Name: localhost Additional Information: localhost Process Information: Process ID: 0x210 Process Name: C:\Windows\System32\winlogon.exe Network Information: Network Address: - Port: - This event is generated when a process attempts to log on an account by explicitly specifying that account's credentials. This most commonly occurs in batch-type configurations such as scheduled tasks, or when using the RUNAS command.
Security	Audit Success	12544	2015-04-25 10:37:59	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: LTRANPHD$ Account Domain: WORKGROUP Logon ID: 0x3e7 Logon Type: 2 Impersonation Level: %%1833 New Logon: Security ID: S-1-5-90-1 Account Name: DWM-1 Account Domain: Window Manager Logon ID: 0xc33f Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x210 Process Name: C:\Windows\System32\winlogon.exe Network Information: Workstation Name: Source Network Address: - Source Port: - Detailed Authentication Information: Logon Process: Advapi Authentication Package: Negotiate Transited Services: - Package Name (NTLM only): - Key Length: 0 This event is generated when a logon session is created. It is generated on the computer that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service such as the Server service, or a local process such as Winlogon.exe or Services.exe. The logon type field indicates the kind of logon that occurred. The most common types are 2 (interactive) and 3 (network). The New Logon fields indicate the account for whom the new logon was created, i.e. the account that was logged on. The network fields indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impersonation level field indicates the extent to which a process in the logon session can impersonate. The authentication information fields provide detailed information about this specific logon request. - Logon GUID is a unique identifier that can be used to correlate this event with a KDC event. - Transited services indicate which intermediate services have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indicates the length of the generated session key. This will be 0 if no session key was requested.
Security	Audit Success	12544	2015-04-25 10:37:59	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: LTRANPHD$ Account Domain: WORKGROUP Logon ID: 0x3e7 Logon Type: 2 Impersonation Level: %%1833 New Logon: Security ID: S-1-5-90-1 Account Name: DWM-1 Account Domain: Window Manager Logon ID: 0xc351 Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x210 Process Name: C:\Windows\System32\winlogon.exe Network Information: Workstation Name: Source Network Address: - Source Port: - Detailed Authentication Information: Logon Process: Advapi Authentication Package: Negotiate Transited Services: - Package Name (NTLM only): - Key Length: 0 This event is generated when a logon session is created. It is generated on the computer that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service such as the Server service, or a local process such as Winlogon.exe or Services.exe. The logon type field indicates the kind of logon that occurred. The most common types are 2 (interactive) and 3 (network). The New Logon fields indicate the account for whom the new logon was created, i.e. the account that was logged on. The network fields indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impersonation level field indicates the extent to which a process in the logon session can impersonate. The authentication information fields provide detailed information about this specific logon request. - Logon GUID is a unique identifier that can be used to correlate this event with a KDC event. - Transited services indicate which intermediate services have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indicates the length of the generated session key. This will be 0 if no session key was requested.
Security	Audit Success	12544	2015-04-25 10:37:59	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: LTRANPHD$ Account Domain: WORKGROUP Logon ID: 0x3e7 Logon Type: 5 Impersonation Level: %%1833 New Logon: Security ID: S-1-5-19 Account Name: LOCAL SERVICE Account Domain: NT AUTHORITY Logon ID: 0x3e5 Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x240 Process Name: C:\Windows\System32\services.exe Network Information: Workstation Name: Source Network Address: - Source Port: - Detailed Authentication Information: Logon Process: Advapi Authentication Package: Negotiate Transited Services: - Package Name (NTLM only): - Key Length: 0 This event is generated when a logon session is created. It is generated on the computer that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service such as the Server service, or a local process such as Winlogon.exe or Services.exe. The logon type field indicates the kind of logon that occurred. The most common types are 2 (interactive) and 3 (network). The New Logon fields indicate the account for whom the new logon was created, i.e. the account that was logged on. The network fields indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impersonation level field indicates the extent to which a process in the logon session can impersonate. The authentication information fields provide detailed information about this specific logon request.

					- Logon GUID is a unique identifier that can be used to correlate this event with a KDC event. - Transited services indicate which intermediate services have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indicates the length of the generated session key. This will be 0 if no session key was requested.
Security	Audit Success	12544	2015-04-25 10:37:59	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: LTRANPHD$ Account Domain: WORKGROUP Logon ID: 0x3e7 Logon Type: 5 Impersonation Level: %%1833 New Logon: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Logon ID: 0x3e7 Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x240 Process Name: C:\Windows\System32\services.exe Network Information: Workstation Name: Source Network Address: - Source Port: - Detailed Authentication Information: Logon Process: Advapi Authentication Package: Negotiate Transited Services: - Package Name (NTLM only): - Key Length: 0 This event is generated when a logon session is created. It is generated on the computer that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service such as the Server service, or a local process such as Winlogon.exe or Services.exe. The logon type field indicates the kind of logon that occurred. The most common types are 2 (interactive) and 3 (network). The New Logon fields indicate the account for whom the new logon was created, i.e. the account that was logged on. The network fields indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impersonation level field indicates the extent to which a process in the logon session can impersonate. The authentication information fields provide detailed information about this specific logon request. - Logon GUID is a unique identifier that can be used to correlate this event with a KDC event. - Transited services indicate which intermediate services have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indicates the length of the generated session key. This will be 0 if no session key was requested.
Security	Audit Success	12544	2015-04-25 10:37:59	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: LTRANPHD$ Account Domain: WORKGROUP Logon ID: 0x3e7 Logon Type: 5 Impersonation Level: %%1833 New Logon: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Logon ID: 0x3e7 Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x240 Process Name: C:\Windows\System32\services.exe Network Information: Workstation Name: Source Network Address: - Source Port: - Detailed Authentication Information: Logon Process: Advapi Authentication Package: Negotiate Transited Services: - Package Name (NTLM only): - Key Length: 0 This event is generated when a logon session is created. It is generated on the computer that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service such as the Server service, or a local process such as Winlogon.exe or Services.exe. The logon type field indicates the kind of logon that occurred. The most common types are 2 (interactive) and 3 (network). The New Logon fields indicate the account for whom the new logon was created, i.e. the account that was logged on. The network fields indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impersonation level field indicates the extent to which a process in the logon session can impersonate. The authentication information fields provide detailed information about this specific logon request. - Logon GUID is a unique identifier that can be used to correlate this event with a KDC event. - Transited services indicate which intermediate services have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indicates the length of the generated session key. This will be 0 if no session key was requested.
Security	Audit Success	12544	2015-04-25 10:37:59	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: LTRANPHD$ Account Domain: WORKGROUP Logon ID: 0x3e7 Logon Type: 5 Impersonation Level: %%1833 New Logon: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Logon ID: 0x3e7 Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x240 Process Name: C:\Windows\System32\services.exe Network Information: Workstation Name: Source Network Address: - Source Port: - Detailed Authentication Information: Logon Process: Advapi Authentication Package: Negotiate Transited Services: - Package Name (NTLM only): - Key Length: 0 This event is generated when a logon session is created. It is generated on the computer that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service such as the Server service, or a local process such as Winlogon.exe or Services.exe. The logon type field indicates the kind of logon that occurred. The most common types are 2 (interactive) and 3 (network). The New Logon fields indicate the account for whom the new logon was created, i.e. the account that was logged on. The network fields indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impersonation level field indicates the extent to which a process in the logon session can impersonate. The authentication information fields provide detailed information about this specific logon request. - Logon GUID is a unique identifier that can be used to correlate this event with a KDC event. - Transited services indicate which intermediate services have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indicates the length of the generated session key. This will be 0 if no session key was requested.
Security	Audit Success	12548	2015-04-25 10:37:59	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Logon ID: 0x3e7 Privileges: SeAssignPrimaryTokenPrivilege SeTcbPrivilege SeSecurityPrivilege SeTakeOwnershipPrivilege SeLoadDriverPrivilege SeBackupPrivilege SeRestorePrivilege SeDebugPrivilege SeAuditPrivilege SeSystemEnvironmentPrivilege SeImpersonatePrivilege
	Audit		2015-04-	Microsoft-Windows-Security-	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-20 Account Name: NETWORK

Security	Success	12548	25 10:37:59	Auditing	SERVICE Account Domain: NT AUTHORITY Logon ID: 0x3e4 Privileges: SeAssignPrimaryTokenPrivilege SeAuditPrivilege SeImpersonatePrivilege
Security	Audit Success	12548	2015-04-25 10:37:59	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-90-1 Account Name: DWM-1 Account Domain: Window Manager Logon ID: 0xc33f Privileges: SeAssignPrimaryTokenPrivilege SeAuditPrivilege SeImpersonatePrivilege
Security	Audit Success	12548	2015-04-25 10:37:59	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-90-1 Account Name: DWM-1 Account Domain: Window Manager Logon ID: 0xc351 Privileges: SeAssignPrimaryTokenPrivilege SeAuditPrivilege
Security	Audit Success	12548	2015-04-25 10:37:59	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-19 Account Name: LOCAL SERVICE Account Domain: NT AUTHORITY Logon ID: 0x3e5 Privileges: SeAssignPrimaryTokenPrivilege SeAuditPrivilege SeImpersonatePrivilege
Security	Audit Success	12548	2015-04-25 10:37:59	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Logon ID: 0x3e7 Privileges: SeAssignPrimaryTokenPrivilege SeTcbPrivilege SeSecurityPrivilege SeTakeOwnershipPrivilege SeLoadDriverPrivilege SeBackupPrivilege SeRestorePrivilege SeDebugPrivilege SeAuditPrivilege SeSystemEnvironmentPrivilege SeImpersonatePrivilege
Security	Audit Success	12548	2015-04-25 10:37:59	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Logon ID: 0x3e7 Privileges: SeAssignPrimaryTokenPrivilege SeTcbPrivilege SeSecurityPrivilege SeTakeOwnershipPrivilege SeLoadDriverPrivilege SeBackupPrivilege SeRestorePrivilege SeDebugPrivilege SeAuditPrivilege SeSystemEnvironmentPrivilege SeImpersonatePrivilege
Security	Audit Success	12548	2015-04-25 10:37:59	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Logon ID: 0x3e7 Privileges: SeAssignPrimaryTokenPrivilege SeTcbPrivilege SeSecurityPrivilege SeTakeOwnershipPrivilege SeLoadDriverPrivilege SeBackupPrivilege SeRestorePrivilege SeDebugPrivilege SeAuditPrivilege SeSystemEnvironmentPrivilege SeImpersonatePrivilege
Security	Audit Success	13568	2015-04-25 10:37:59	Microsoft-Windows-Security-Auditing	4902: The Per-user audit policy table was created. Number of Elements: 0 Policy ID: 0x7437
Security	Audit Success	12292	2015-04-25 10:38:00	Microsoft-Windows-Security-Auditing	5033: The Windows Firewall Driver started successfully.
Security	Audit Success	12292	2015-04-25 10:38:00	Microsoft-Windows-Security-Auditing	5024: The Windows Firewall service started successfully.
Security	Audit Success	12544	2015-04-25 10:38:00	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: LTRANPHD$ Account Domain: WORKGROUP Logon ID: 0x3e7 Logon Type: 5 Impersonation Level: %%1833 New Logon: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Logon ID: 0x3e7 Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x240 Process Name: C:\Windows\System32\services.exe Network Information: Workstation Name: Source Network Address: - Source Port: - Detailed Authentication Information: Logon Process: Advapi Authentication Package: Negotiate Transited Services: - Package Name (NTLM only): - Key Length: 0 This event is generated when a logon session is created. It is generated on the computer that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service such as the Server service, or a local process such as Winlogon.exe or Services.exe. The logon type field indicates the kind of logon that occurred. The most common types are 2 (interactive) and 3 (network). The New Logon fields indicate the account for whom the new logon was created, i.e. the account that was logged on. The network fields indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impersonation level field indicates the extent to which a process in the logon session can impersonate. The authentication information fields provide detailed information about this specific logon request. - Logon GUID is a unique identifier that can be used to correlate this event with a KDC event. - Transited services indicate which intermediate services have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indicates the length of the generated session key. This will be 0 if no session key was requested.
Security	Audit Success	12544	2015-04-25 10:38:00	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: LTRANPHD$ Account Domain: WORKGROUP Logon ID: 0x3e7 Logon Type: 5 Impersonation Level: %%1833 New Logon: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Logon ID: 0x3e7 Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x240 Process Name: C:\Windows\System32\services.exe Network Information: Workstation Name: Source Network Address: - Source Port: - Detailed Authentication Information: Logon Process: Advapi Authentication Package: Negotiate Transited Services: - Package Name (NTLM only): - Key Length: 0 This event is generated when a logon session is created. It is generated on the computer that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service such as the Server service, or a local process such as Winlogon.exe or Services.exe. The logon type field indicates the kind of logon that occurred. The most common types are 2 (interactive) and 3 (network). The New Logon fields indicate the account for whom the new logon was created, i.e. the account that was logged on. The network fields indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impersonation level field indicates the extent to which a process in the logon session can

					impersonate. The authentication information fields provide detailed information about this specific logon request. - Logon GUID is a unique identifier that can be used to correlate this event with a KDC event. - Transited services indicate which intermediate services have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indicates the length of the generated session key. This will be 0 if no session key was requested.
Security	Audit Success	12544	2015-04-25 10:38:00	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-0-0 Account Name: - Account Domain: - Logon ID: 0x0 Logon Type: 3 Impersonation Level: %%1833 New Logon: Security ID: S-1-5-7 Account Name: ANONYMOUS LOGON Account Domain: NT AUTHORITY Logon ID: 0x15df5 Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x0 Process Name: - Network Information: Workstation Name: Source Network Address: - Source Port: - Detailed Authentication Information: Logon Process: NtLmSsp Authentication Package: NTLM Transited Services: - Package Name (NTLM only): NTLM V1 Key Length: 0 This event is generated when a logon session is created. It is generated on the computer that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service such as the Server service, or a local process such as Winlogon.exe or Services.exe. The logon type field indicates the kind of logon that occurred. The most common types are 2 (interactive) and 3 (network). The New Logon fields indicate the account for whom the new logon was created, i.e. the account that was logged on. The network fields indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impersonation level field indicates the extent to which a process in the logon session can impersonate. The authentication information fields provide detailed information about this specific logon request. - Logon GUID is a unique identifier that can be used to correlate this event with a KDC event. - Transited services indicate which intermediate services have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indicates the length of the generated session key. This will be 0 if no session key was requested.
Security	Audit Success	12548	2015-04-25 10:38:00	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Logon ID: 0x3e7 Privileges: SeAssignPrimaryTokenPrivilege SeTcbPrivilege SeSecurityPrivilege SeTakeOwnershipPrivilege SeLoadDriverPrivilege SeBackupPrivilege SeRestorePrivilege SeDebugPrivilege SeAuditPrivilege SeSystemEnvironmentPrivilege SeImpersonatePrivilege
Security	Audit Success	12548	2015-04-25 10:38:00	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Logon ID: 0x3e7 Privileges: SeAssignPrimaryTokenPrivilege SeTcbPrivilege SeSecurityPrivilege SeTakeOwnershipPrivilege SeLoadDriverPrivilege SeBackupPrivilege SeRestorePrivilege SeDebugPrivilege SeAuditPrivilege SeSystemEnvironmentPrivilege SeImpersonatePrivilege
Security	Audit Success	12544	2015-04-25 10:38:01	Microsoft-Windows-Security-Auditing	4648: A logon was attempted using explicit credentials. Subject: Security ID: S-1-5-18 Account Name: LTRANPHD$ Account Domain: WORKGROUP Logon ID: 0x3e7 Logon GUID: {00000000-0000-0000-0000-000000000000} Account Whose Credentials Were Used: Account Name: Liem Account Domain: LTRANPHD Logon GUID: {00000000-0000-0000-0000-000000000000} Target Server: Target Server Name: localhost Additional Information: localhost Process Information: Process ID: 0x210 Process Name: C:\Windows\System32\winlogon.exe Network Information: Network Address: 127.0.0.1 Port: 0 This event is generated when a process attempts to log on an account by explicitly specifying that account's credentials. This most commonly occurs in batch-type configurations such as scheduled tasks, or when using the RUNAS command.
Security	Audit Success	12544	2015-04-25 10:38:01	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: LTRANPHD$ Account Domain: WORKGROUP Logon ID: 0x3e7 Logon Type: 2 Impersonation Level: %%1833 New Logon: Security ID: S-1-5-21-1888849264-3803429180-4108621888-1001 Account Name: Liem Account Domain: LTRANPHD Logon ID: 0x1a1fd Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x210 Process Name: C:\Windows\System32\winlogon.exe Network Information: Workstation Name: LTRANPHD Source Network Address: 127.0.0.1 Source Port: 0 Detailed Authentication Information: Logon Process: User32 Authentication Package: Negotiate Transited Services: - Package Name (NTLM only): - Key Length: 0 This event is generated when a logon session is created. It is generated on the computer that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service such as the Server service, or a local process such as Winlogon.exe or Services.exe. The logon type field indicates the kind of logon that occurred. The most common types are 2 (interactive) and 3 (network). The New Logon fields indicate the account for whom the new logon was created, i.e. the account that was logged on. The network fields indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impersonation level field indicates the extent to which a process in the logon session can impersonate. The authentication information fields provide detailed information about this specific logon request. - Logon GUID is a unique identifier that can be used to correlate this event with a KDC event. - Transited services indicate which intermediate services have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indicates the length of the generated session key. This will be 0 if no session key was requested.
					4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: LTRANPHD$ Account Domain: WORKGROUP Logon ID: 0x3e7 Logon Type: 2 Impersonation Level: %%1833 New Logon: Security ID: S-1-5-21-1888849264-3803429180-4108621888-1001 Account Name: Liem Account Domain: LTRANPHD Logon ID: 0x1a22c Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x210 Process Name: C:\Windows\System32\winlogon.exe Network Information: Workstation Name: LTRANPHD Source Network Address: 127.0.0.1 Source Port: 0 Detailed Authentication Information: Logon Process: User32 Authentication Package: Negotiate Transited Services: - Package Name (NTLM only): -

Security	Audit Success	12544	2015-04-25 10:38:01	Microsoft-Windows-Security-Auditing	Key Length: 0 This event is generated when a logon session is created. It is generated on the computer that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service such as the Server service, or a local process such as Winlogon.exe or Services.exe. The logon type field indicates the kind of logon that occurred. The most common types are 2 (interactive) and 3 (network). The New Logon fields indicate the account for whom the new logon was created, i.e. the account that was logged on. The network fields indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impersonation level field indicates the extent to which a process in the logon session can impersonate. The authentication information fields provide detailed information about this specific logon request. - Logon GUID is a unique identifier that can be used to correlate this event with a KDC event. - Transited services indicate which intermediate services have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indicates the length of the generated session key. This will be 0 if no session key was requested.
Security	Audit Success	12548	2015-04-25 10:38:01	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-21-1888849264-3803429180-4108621888-1001 Account Name: Liem Account Domain: LTRANPHD Logon ID: 0x1a1fd Privileges: SeSecurityPrivilege SeTakeOwnershipPrivilege SeLoadDriverPrivilege SeBackupPrivilege SeRestorePrivilege SeDebugPrivilege SeSystemEnvironmentPrivilege SeImpersonatePrivilege
Security	Audit Success	12544	2015-04-25 10:38:02	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: LTRANPHD$ Account Domain: WORKGROUP Logon ID: 0x3e7 Logon Type: 5 Impersonation Level: %%1833 New Logon: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Logon ID: 0x3e7 Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x240 Process Name: C:\Windows\System32\services.exe Network Information: Workstation Name: Source Network Address: - Source Port: - Detailed Authentication Information: Logon Process: Advapi Authentication Package: Negotiate Transited Services: - Package Name (NTLM only): - Key Length: 0 This event is generated when a logon session is created. It is generated on the computer that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service such as the Server service, or a local process such as Winlogon.exe or Services.exe. The logon type field indicates the kind of logon that occurred. The most common types are 2 (interactive) and 3 (network). The New Logon fields indicate the account for whom the new logon was created, i.e. the account that was logged on. The network fields indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impersonation level field indicates the extent to which a process in the logon session can impersonate. The authentication information fields provide detailed information about this specific logon request. - Logon GUID is a unique identifier that can be used to correlate this event with a KDC event. - Transited services indicate which intermediate services have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indicates the length of the generated session key. This will be 0 if no session key was requested.
Security	Audit Success	12548	2015-04-25 10:38:02	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Logon ID: 0x3e7 Privileges: SeAssignPrimaryTokenPrivilege SeTcbPrivilege SeSecurityPrivilege SeTakeOwnershipPrivilege SeLoadDriverPrivilege SeBackupPrivilege SeRestorePrivilege SeDebugPrivilege SeAuditPrivilege SeSystemEnvironmentPrivilege SeImpersonatePrivilege
Security	Audit Success	13824	2015-04-25 10:38:03	Microsoft-Windows-Security-Auditing	4797: An attempt was made to query the existence of a blank password for an account. Subject: Security ID: S-1-5-21-1888849264-3803429180-4108621888-1001 Account Name: Liem Account Domain: LTRANPHD Logon ID: 0x1a22c Additional Information: Caller Workstation: LTRANPHD Target Account Name: Administrator Target Account Domain: LTRANPHD
Security	Audit Success	13824	2015-04-25 10:38:03	Microsoft-Windows-Security-Auditing	4797: An attempt was made to query the existence of a blank password for an account. Subject: Security ID: S-1-5-21-1888849264-3803429180-4108621888-1001 Account Name: Liem Account Domain: LTRANPHD Logon ID: 0x1a22c Additional Information: Caller Workstation: LTRANPHD Target Account Name: Guest Target Account Domain: LTRANPHD
Security	Audit Success	13824	2015-04-25 10:38:03	Microsoft-Windows-Security-Auditing	4797: An attempt was made to query the existence of a blank password for an account. Subject: Security ID: S-1-5-21-1888849264-3803429180-4108621888-1001 Account Name: Liem Account Domain: LTRANPHD Logon ID: 0x1a22c Additional Information: Caller Workstation: LTRANPHD Target Account Name: Administrator Target Account Domain: LTRANPHD
Security	Audit Success	13824	2015-04-25 10:38:03	Microsoft-Windows-Security-Auditing	4797: An attempt was made to query the existence of a blank password for an account. Subject: Security ID: S-1-5-21-1888849264-3803429180-4108621888-1001 Account Name: Liem Account Domain: LTRANPHD Logon ID: 0x1a22c Additional Information: Caller Workstation: LTRANPHD Target Account Name: Guest Target Account Domain: LTRANPHD
Security	Audit Success	13824	2015-04-25 10:38:08	Microsoft-Windows-Security-Auditing	4797: An attempt was made to query the existence of a blank password for an account. Subject: Security ID: S-1-5-19 Account Name: LOCAL SERVICE Account Domain: NT AUTHORITY Logon ID: 0x3e5 Additional Information: Caller Workstation: LTRANPHD Target Account Name: Administrator Target Account Domain: LTRANPHD
Security	Audit Success	13824	2015-04-25 10:38:08	Microsoft-Windows-Security-Auditing	4797: An attempt was made to query the existence of a blank password for an account. Subject: Security ID: S-1-5-19 Account Name: LOCAL SERVICE Account Domain: NT AUTHORITY Logon ID: 0x3e5 Additional Information: Caller Workstation: LTRANPHD Target Account Name: Guest Target Account Domain: LTRANPHD
Security	Audit Success	13824	2015-04-25 10:38:08	Microsoft-Windows-Security-Auditing	4797: An attempt was made to query the existence of a blank password for an account. Subject: Security ID: S-1-5-19 Account Name: LOCAL SERVICE Account Domain: NT AUTHORITY Logon ID: 0x3e5 Additional Information: Caller Workstation: LTRANPHD Target Account Name: Liem Target Account Domain: LTRANPHD

Security	Audit Success	13824	2015-04-25 10:38:08	Microsoft-Windows-Security-Auditing	4797: An attempt was made to query the existence of a blank password for an account. Subject: Security ID: S-1-5-19 Account Name: LOCAL SERVICE Account Domain: NT AUTHORITY Logon ID: 0x3e5 Additional Information: Caller Workstation: LTRANPHD Target Account Name: Administrator Target Account Domain: LTRANPHD
Security	Audit Success	13824	2015-04-25 10:38:08	Microsoft-Windows-Security-Auditing	4797: An attempt was made to query the existence of a blank password for an account. Subject: Security ID: S-1-5-19 Account Name: LOCAL SERVICE Account Domain: NT AUTHORITY Logon ID: 0x3e5 Additional Information: Caller Workstation: LTRANPHD Target Account Name: Liem Target Account Domain: LTRANPHD
Security	Audit Success	13824	2015-04-25 10:38:08	Microsoft-Windows-Security-Auditing	4797: An attempt was made to query the existence of a blank password for an account. Subject: Security ID: S-1-5-19 Account Name: LOCAL SERVICE Account Domain: NT AUTHORITY Logon ID: 0x3e5 Additional Information: Caller Workstation: LTRANPHD Target Account Name: Guest Target Account Domain: LTRANPHD
Security	Audit Success	13824	2015-04-25 10:38:08	Microsoft-Windows-Security-Auditing	4797: An attempt was made to query the existence of a blank password for an account. Subject: Security ID: S-1-5-19 Account Name: LOCAL SERVICE Account Domain: NT AUTHORITY Logon ID: 0x3e5 Additional Information: Caller Workstation: LTRANPHD Target Account Name: Liem Target Account Domain: LTRANPHD
Security	Audit Success	13824	2015-04-25 10:38:08	Microsoft-Windows-Security-Auditing	4797: An attempt was made to query the existence of a blank password for an account. Subject: Security ID: S-1-5-19 Account Name: LOCAL SERVICE Account Domain: NT AUTHORITY Logon ID: 0x3e5 Additional Information: Caller Workstation: LTRANPHD Target Account Name: Liem Target Account Domain: LTRANPHD
Security	Audit Success	13824	2015-04-25 10:40:54	Microsoft-Windows-Security-Auditing	4797: An attempt was made to query the existence of a blank password for an account. Subject: Security ID: S-1-5-21-1888849264-3803429180-4108621888-1001 Account Name: Liem Account Domain: LTRANPHD Logon ID: 0x1a22c Additional Information: Caller Workstation: LTRANPHD Target Account Name: Administrator Target Account Domain: LTRANPHD
Security	Audit Success	12544	2015-04-25 10:40:58	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: LTRANPHD$ Account Domain: WORKGROUP Logon ID: 0x3e7 Logon Type: 5 Impersonation Level: %%1833 New Logon: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Logon ID: 0x3e7 Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x240 Process Name: C:\Windows\System32\services.exe Network Information: Workstation Name: Source Network Address: - Source Port: - Detailed Authentication Information: Logon Process: Advapi Authentication Package: Negotiate Transited Services: - Package Name (NTLM only): - Key Length: 0 This event is generated when a logon session is created. It is generated on the computer that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service such as the Server service, or a local process such as Winlogon.exe or Services.exe. The logon type field indicates the kind of logon that occurred. The most common types are 2 (interactive) and 3 (network). The New Logon fields indicate the account for whom the new logon was created, i.e. the account that was logged on. The network fields indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impersonation level field indicates the extent to which a process in the logon session can impersonate. The authentication information fields provide detailed information about this specific logon request. - Logon GUID is a unique identifier that can be used to correlate this event with a KDC event. - Transited services indicate which intermediate services have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indicates the length of the generated session key. This will be 0 if no session key was requested.
Security	Audit Success	12548	2015-04-25 10:40:58	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Logon ID: 0x3e7 Privileges: SeAssignPrimaryTokenPrivilege SeTcbPrivilege SeSecurityPrivilege SeTakeOwnershipPrivilege SeLoadDriverPrivilege SeBackupPrivilege SeRestorePrivilege SeDebugPrivilege SeAuditPrivilege SeSystemEnvironmentPrivilege SeImpersonatePrivilege
Security	Audit Success	12545	2015-04-25 10:41:11	Microsoft-Windows-Security-Auditing	4647: User initiated logoff: Subject: Security ID: S-1-5-21-1888849264-3803429180-4108621888-1001 Account Name: Liem Account Domain: LTRANPHD Logon ID: 0x1a22c This event is generated when a logoff is initiated. No further user-initiated activity can occur. This event can be interpreted as a logoff event.
Security	Audit Success	103	2015-04-25 10:41:12	Microsoft-Windows-Eventlog	1100: The event logging service has shut down.
Security	Audit Success	12288	2015-04-25 10:42:28	Microsoft-Windows-Security-Auditing	4608: Windows is starting up. This event is logged when LSASS.EXE starts and the auditing subsystem is initialized.
Security	Audit Success	12292	2015-04-25 10:42:28	Microsoft-Windows-Security-Auditing	5033: The Windows Firewall Driver started successfully.
Security	Audit Success	12292	2015-04-25 10:42:28	Microsoft-Windows-Security-Auditing	5024: The Windows Firewall service started successfully.
					4624: An account was successfully logged on. Subject: Security ID: S-1-0-0 Account Name: - Account Domain: - Logon ID: 0x0 Logon Type: 0 Impersonation Level: - New Logon: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Logon ID: 0x3e7 Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x4 Process Name: Network Information: Workstation Name: - Source Network Address: - Source Port: - Detailed Authentication Information: Logon Process: - Authentication Package: - Transited Services: - Package Name (NTLM only): - Key Length: 0 This event is

Security	Audit Success	12544	2015-04-25 10:42:28	Microsoft-Windows-Security-Auditing	generated when a logon session is created. It is generated on the computer that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service such as the Server service, or a local process such as Winlogon.exe or Services.exe. The logon type field indicates the kind of logon that occurred. The most common types are 2 (interactive) and 3 (network). The New Logon fields indicate the account for whom the new logon was created, i.e. the account that was logged on. The network fields indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impersonation level field indicates the extent to which a process in the logon session can impersonate. The authentication information fields provide detailed information about this specific logon request. - Logon GUID is a unique identifier that can be used to correlate this event with a KDC event. - Transited services indicate which intermediate services have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indicates the length of the generated session key. This will be 0 if no session key was requested.
Security	Audit Success	12544	2015-04-25 10:42:28	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: LTRANPHD$ Account Domain: WORKGROUP Logon ID: 0x3e7 Logon Type: 5 Impersonation Level: %%1833 New Logon: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Logon ID: 0x3e7 Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x23c Process Name: C:\Windows\System32\services.exe Network Information: Workstation Name: Source Network Address: - Source Port: - Detailed Authentication Information: Logon Process: Advapi Authentication Package: Negotiate Transited Services: - Package Name (NTLM only): - Key Length: 0 This event is generated when a logon session is created. It is generated on the computer that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service such as the Server service, or a local process such as Winlogon.exe or Services.exe. The logon type field indicates the kind of logon that occurred. The most common types are 2 (interactive) and 3 (network). The New Logon fields indicate the account for whom the new logon was created, i.e. the account that was logged on. The network fields indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impersonation level field indicates the extent to which a process in the logon session can impersonate. The authentication information fields provide detailed information about this specific logon request. - Logon GUID is a unique identifier that can be used to correlate this event with a KDC event. - Transited services indicate which intermediate services have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indicates the length of the generated session key. This will be 0 if no session key was requested.
Security	Audit Success	12544	2015-04-25 10:42:28	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: LTRANPHD$ Account Domain: WORKGROUP Logon ID: 0x3e7 Logon Type: 5 Impersonation Level: %%1833 New Logon: Security ID: S-1-5-20 Account Name: NETWORK SERVICE Account Domain: NT AUTHORITY Logon ID: 0x3e4 Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x23c Process Name: C:\Windows\System32\services.exe Network Information: Workstation Name: Source Network Address: - Source Port: - Detailed Authentication Information: Logon Process: Advapi Authentication Package: Negotiate Transited Services: - Package Name (NTLM only): - Key Length: 0 This event is generated when a logon session is created. It is generated on the computer that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service such as the Server service, or a local process such as Winlogon.exe or Services.exe. The logon type field indicates the kind of logon that occurred. The most common types are 2 (interactive) and 3 (network). The New Logon fields indicate the account for whom the new logon was created, i.e. the account that was logged on. The network fields indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impersonation level field indicates the extent to which a process in the logon session can impersonate. The authentication information fields provide detailed information about this specific logon request. - Logon GUID is a unique identifier that can be used to correlate this event with a KDC event. - Transited services indicate which intermediate services have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indicates the length of the generated session key. This will be 0 if no session key was requested.
Security	Audit Success	12544	2015-04-25 10:42:28	Microsoft-Windows-Security-Auditing	4648: A logon was attempted using explicit credentials. Subject: Security ID: S-1-5-18 Account Name: LTRANPHD$ Account Domain: WORKGROUP Logon ID: 0x3e7 Logon GUID: {00000000-0000-0000-0000-000000000000} Account Whose Credentials Were Used: Account Name: DWM-1 Account Domain: Window Manager Logon GUID: {00000000-0000-0000-0000-000000000000} Target Server: Target Server Name: localhost Additional Information: localhost Process Information: Process ID: 0x20c Process Name: C:\Windows\System32\winlogon.exe Network Information: Network Address: - Port: - This event is generated when a process attempts to log on an account by explicitly specifying that account's credentials. This most commonly occurs in batch-type configurations such as scheduled tasks, or when using the RUNAS command.
			2015-04-		4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: LTRANPHD$ Account Domain: WORKGROUP Logon ID: 0x3e7 Logon Type: 2 Impersonation Level: %%1833 New Logon: Security ID: S-1-5-90-1 Account Name: DWM-1 Account Domain: Window Manager Logon ID: 0xc304 Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x20c Process Name: C:\Windows\System32\winlogon.exe Network Information: Workstation Name: Source Network Address: - Source Port: - Detailed Authentication Information: Logon Process: Advapi Authentication Package: Negotiate Transited Services: - Package Name (NTLM only): - Key Length: 0 This event is generated when a logon session is created. It is generated on the computer that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service such as the Server service, or a local

Security	Audit Success	12544	25 10:42:28	Microsoft-Windows-Security-Auditing	process such as Winlogon.exe or Services.exe. The logon type field indicates the kind of logon that occurred. The most common types are 2 (interactive) and 3 (network). The New Logon fields indicate the account for whom the new logon was created, i.e. the account that was logged on. The network fields indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impersonation level field indicates the extent to which a process in the logon session can impersonate. The authentication information fields provide detailed information about this specific logon request. - Logon GUID is a unique identifier that can be used to correlate this event with a KDC event. - Transited services indicate which intermediate services have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indicates the length of the generated session key. This will be 0 if no session key was requested.
Security	Audit Success	12544	2015-04-25 10:42:28	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: LTRANPHD$ Account Domain: WORKGROUP Logon ID: 0x3e7 Logon Type: 2 Impersonation Level: %%1833 New Logon: Security ID: S-1-5-90-1 Account Name: DWM-1 Account Domain: Window Manager Logon ID: 0xc334 Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x20c Process Name: C:\Windows\System32\winlogon.exe Network Information: Workstation Name: Source Network Address: - Source Port: - Detailed Authentication Information: Logon Process: Advapi Authentication Package: Negotiate Transited Services: - Package Name (NTLM only): - Key Length: 0 This event is generated when a logon session is created. It is generated on the computer that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service such as the Server service, or a local process such as Winlogon.exe or Services.exe. The logon type field indicates the kind of logon that occurred. The most common types are 2 (interactive) and 3 (network). The New Logon fields indicate the account for whom the new logon was created, i.e. the account that was logged on. The network fields indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impersonation level field indicates the extent to which a process in the logon session can impersonate. The authentication information fields provide detailed information about this specific logon request. - Logon GUID is a unique identifier that can be used to correlate this event with a KDC event. - Transited services indicate which intermediate services have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indicates the length of the generated session key. This will be 0 if no session key was requested.
Security	Audit Success	12544	2015-04-25 10:42:28	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: LTRANPHD$ Account Domain: WORKGROUP Logon ID: 0x3e7 Logon Type: 5 Impersonation Level: %%1833 New Logon: Security ID: S-1-5-19 Account Name: LOCAL SERVICE Account Domain: NT AUTHORITY Logon ID: 0x3e5 Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x23c Process Name: C:\Windows\System32\services.exe Network Information: Workstation Name: Source Network Address: - Source Port: - Detailed Authentication Information: Logon Process: Advapi Authentication Package: Negotiate Transited Services: - Package Name (NTLM only): - Key Length: 0 This event is generated when a logon session is created. It is generated on the computer that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service such as the Server service, or a local process such as Winlogon.exe or Services.exe. The logon type field indicates the kind of logon that occurred. The most common types are 2 (interactive) and 3 (network). The New Logon fields indicate the account for whom the new logon was created, i.e. the account that was logged on. The network fields indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impersonation level field indicates the extent to which a process in the logon session can impersonate. The authentication information fields provide detailed information about this specific logon request. - Logon GUID is a unique identifier that can be used to correlate this event with a KDC event. - Transited services indicate which intermediate services have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indicates the length of the generated session key. This will be 0 if no session key was requested.
Security	Audit Success	12544	2015-04-25 10:42:28	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: LTRANPHD$ Account Domain: WORKGROUP Logon ID: 0x3e7 Logon Type: 5 Impersonation Level: %%1833 New Logon: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Logon ID: 0x3e7 Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x23c Process Name: C:\Windows\System32\services.exe Network Information: Workstation Name: Source Network Address: - Source Port: - Detailed Authentication Information: Logon Process: Advapi Authentication Package: Negotiate Transited Services: - Package Name (NTLM only): - Key Length: 0 This event is generated when a logon session is created. It is generated on the computer that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service such as the Server service, or a local process such as Winlogon.exe or Services.exe. The logon type field indicates the kind of logon that occurred. The most common types are 2 (interactive) and 3 (network). The New Logon fields indicate the account for whom the new logon was created, i.e. the account that was logged on. The network fields indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impersonation level field indicates the extent to which a process in the logon session can impersonate. The authentication information fields provide detailed information about this specific logon request. - Logon GUID is a unique identifier that can be used to correlate this event with a KDC event. - Transited services indicate which intermediate services have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indicates the length of the generated

					session key. This will be 0 if no session key was requested.
Security	Audit Success	12544	2015-04-25 10:42:28	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: LTRANPHD$ Account Domain: WORKGROUP Logon ID: 0x3e7 Logon Type: 5 Impersonation Level: %%1833 New Logon: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Logon ID: 0x3e7 Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x23c Process Name: C:\Windows\System32\services.exe Network Information: Workstation Name: Source Network Address: - Source Port: - Detailed Authentication Information: Logon Process: Advapi Authentication Package: Negotiate Transited Services: - Package Name (NTLM only): - Key Length: 0 This event is generated when a logon session is created. It is generated on the computer that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service such as the Server service, or a local process such as Winlogon.exe or Services.exe. The logon type field indicates the kind of logon that occurred. The most common types are 2 (interactive) and 3 (network). The New Logon fields indicate the account for whom the new logon was created, i.e. the account that was logged on. The network fields indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impersonation level field indicates the extent to which a process in the logon session can impersonate. The authentication information fields provide detailed information about this specific logon request. - Logon GUID is a unique identifier that can be used to correlate this event with a KDC event. - Transited services indicate which intermediate services have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indicates the length of the generated session key. This will be 0 if no session key was requested.
Security	Audit Success	12544	2015-04-25 10:42:28	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: LTRANPHD$ Account Domain: WORKGROUP Logon ID: 0x3e7 Logon Type: 5 Impersonation Level: %%1833 New Logon: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Logon ID: 0x3e7 Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x23c Process Name: C:\Windows\System32\services.exe Network Information: Workstation Name: Source Network Address: - Source Port: - Detailed Authentication Information: Logon Process: Advapi Authentication Package: Negotiate Transited Services: - Package Name (NTLM only): - Key Length: 0 This event is generated when a logon session is created. It is generated on the computer that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service such as the Server service, or a local process such as Winlogon.exe or Services.exe. The logon type field indicates the kind of logon that occurred. The most common types are 2 (interactive) and 3 (network). The New Logon fields indicate the account for whom the new logon was created, i.e. the account that was logged on. The network fields indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impersonation level field indicates the extent to which a process in the logon session can impersonate. The authentication information fields provide detailed information about this specific logon request. - Logon GUID is a unique identifier that can be used to correlate this event with a KDC event. - Transited services indicate which intermediate services have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indicates the length of the generated session key. This will be 0 if no session key was requested.
Security	Audit Success	12544	2015-04-25 10:42:28	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: LTRANPHD$ Account Domain: WORKGROUP Logon ID: 0x3e7 Logon Type: 5 Impersonation Level: %%1833 New Logon: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Logon ID: 0x3e7 Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x23c Process Name: C:\Windows\System32\services.exe Network Information: Workstation Name: Source Network Address: - Source Port: - Detailed Authentication Information: Logon Process: Advapi Authentication Package: Negotiate Transited Services: - Package Name (NTLM only): - Key Length: 0 This event is generated when a logon session is created. It is generated on the computer that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service such as the Server service, or a local process such as Winlogon.exe or Services.exe. The logon type field indicates the kind of logon that occurred. The most common types are 2 (interactive) and 3 (network). The New Logon fields indicate the account for whom the new logon was created, i.e. the account that was logged on. The network fields indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impersonation level field indicates the extent to which a process in the logon session can impersonate. The authentication information fields provide detailed information about this specific logon request. - Logon GUID is a unique identifier that can be used to correlate this event with a KDC event. - Transited services indicate which intermediate services have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indicates the length of the generated session key. This will be 0 if no session key was requested.
			2015-04-		4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: LTRANPHD$ Account Domain: WORKGROUP Logon ID: 0x3e7 Logon Type: 5 Impersonation Level: %%1833 New Logon: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Logon ID: 0x3e7 Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x23c Process Name: C:\Windows\System32\services.exe Network Information: Workstation Name: Source Network Address: - Source Port: - Detailed Authentication Information: Logon Process: Advapi Authentication Package: Negotiate Transited Services: - Package Name (NTLM only): - Key Length: 0 This event is generated when a logon session is created. It is generated on the computer that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service such as the Server service, or a local

Security	Audit Success	12544	25 10:42:28	Microsoft-Windows-Security-Auditing	process such as Winlogon.exe or Services.exe. The logon type field indicates the kind of logon that occurred. The most common types are 2 (interactive) and 3 (network). The New Logon fields indicate the account for whom the new logon was created, i.e. the account that was logged on. The network fields indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impersonation level field indicates the extent to which a process in the logon session can impersonate. The authentication information fields provide detailed information about this specific logon request. - Logon GUID is a unique identifier that can be used to correlate this event with a KDC event. - Transited services indicate which intermediate services have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indicates the length of the generated session key. This will be 0 if no session key was requested.
Security	Audit Success	12544	2015-04-25 10:42:28	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-0-0 Account Name: - Account Domain: - Logon ID: 0x0 Logon Type: 3 Impersonation Level: %%1833 New Logon: Security ID: S-1-5-7 Account Name: ANONYMOUS LOGON Account Domain: NT AUTHORITY Logon ID: 0x18054 Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x0 Process Name: - Network Information: Workstation Name: Source Network Address: - Source Port: - Detailed Authentication Information: Logon Process: NtLmSsp Authentication Package: NTLM Transited Services: - Package Name (NTLM only): NTLM V1 Key Length: 0 This event is generated when a logon session is created. It is generated on the computer that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service such as the Server service, or a local process such as Winlogon.exe or Services.exe. The logon type field indicates the kind of logon that occurred. The most common types are 2 (interactive) and 3 (network). The New Logon fields indicate the account for whom the new logon was created, i.e. the account that was logged on. The network fields indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impersonation level field indicates the extent to which a process in the logon session can impersonate. The authentication information fields provide detailed information about this specific logon request. - Logon GUID is a unique identifier that can be used to correlate this event with a KDC event. - Transited services indicate which intermediate services have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indicates the length of the generated session key. This will be 0 if no session key was requested.
Security	Audit Success	12548	2015-04-25 10:42:28	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Logon ID: 0x3e7 Privileges: SeAssignPrimaryTokenPrivilege SeTcbPrivilege SeSecurityPrivilege SeTakeOwnershipPrivilege SeLoadDriverPrivilege SeBackupPrivilege SeRestorePrivilege SeDebugPrivilege SeAuditPrivilege SeSystemEnvironmentPrivilege SeImpersonatePrivilege
Security	Audit Success	12548	2015-04-25 10:42:28	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-20 Account Name: NETWORK SERVICE Account Domain: NT AUTHORITY Logon ID: 0x3e4 Privileges: SeAssignPrimaryTokenPrivilege SeAuditPrivilege SeImpersonatePrivilege
Security	Audit Success	12548	2015-04-25 10:42:28	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-90-1 Account Name: DWM-1 Account Domain: Window Manager Logon ID: 0xc304 Privileges: SeAssignPrimaryTokenPrivilege SeAuditPrivilege SeImpersonatePrivilege
Security	Audit Success	12548	2015-04-25 10:42:28	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-90-1 Account Name: DWM-1 Account Domain: Window Manager Logon ID: 0xc334 Privileges: SeAssignPrimaryTokenPrivilege SeAuditPrivilege
Security	Audit Success	12548	2015-04-25 10:42:28	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-19 Account Name: LOCAL SERVICE Account Domain: NT AUTHORITY Logon ID: 0x3e5 Privileges: SeAssignPrimaryTokenPrivilege SeAuditPrivilege SeImpersonatePrivilege
Security	Audit Success	12548	2015-04-25 10:42:28	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Logon ID: 0x3e7 Privileges: SeAssignPrimaryTokenPrivilege SeTcbPrivilege SeSecurityPrivilege SeTakeOwnershipPrivilege SeLoadDriverPrivilege SeBackupPrivilege SeRestorePrivilege SeDebugPrivilege SeAuditPrivilege SeSystemEnvironmentPrivilege SeImpersonatePrivilege
Security	Audit Success	12548	2015-04-25 10:42:28	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Logon ID: 0x3e7 Privileges: SeAssignPrimaryTokenPrivilege SeTcbPrivilege SeSecurityPrivilege SeTakeOwnershipPrivilege SeLoadDriverPrivilege SeBackupPrivilege SeRestorePrivilege SeDebugPrivilege SeAuditPrivilege SeSystemEnvironmentPrivilege SeImpersonatePrivilege
Security	Audit Success	12548	2015-04-25 10:42:28	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Logon ID: 0x3e7 Privileges: SeAssignPrimaryTokenPrivilege SeTcbPrivilege SeSecurityPrivilege SeTakeOwnershipPrivilege SeLoadDriverPrivilege SeBackupPrivilege SeRestorePrivilege SeDebugPrivilege SeAuditPrivilege SeSystemEnvironmentPrivilege SeImpersonatePrivilege
Security	Audit Success	12548	2015-04-25 10:42:28	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Logon ID: 0x3e7 Privileges: SeAssignPrimaryTokenPrivilege SeTcbPrivilege SeSecurityPrivilege SeTakeOwnershipPrivilege SeLoadDriverPrivilege SeBackupPrivilege SeRestorePrivilege SeDebugPrivilege SeAuditPrivilege SeSystemEnvironmentPrivilege SeImpersonatePrivilege
Security	Audit Success	12548	2015-04-25 10:42:28	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Logon ID: 0x3e7 Privileges: SeAssignPrimaryTokenPrivilege SeTcbPrivilege SeSecurityPrivilege SeTakeOwnershipPrivilege SeLoadDriverPrivilege SeBackupPrivilege SeRestorePrivilege SeDebugPrivilege SeAuditPrivilege SeSystemEnvironmentPrivilege SeImpersonatePrivilege

Security	Audit Success	13568	2015-04-25 10:42:28	Microsoft-Windows-Security-Auditing	4902: The Per-user audit policy table was created. Number of Elements: 0 Policy ID: 0x744e
Security	Audit Success	12544	2015-04-25 10:42:30	Microsoft-Windows-Security-Auditing	4648: A logon was attempted using explicit credentials. Subject: Security ID: S-1-5-18 Account Name: LTRANPHD$ Account Domain: WORKGROUP Logon ID: 0x3e7 Logon GUID: {00000000-0000-0000-0000-000000000000} Account Whose Credentials Were Used: Account Name: Liem Account Domain: LTRANPHD Logon GUID: {00000000-0000-0000-0000-000000000000} Target Server: Target Server Name: localhost Additional Information: localhost Process Information: Process ID: 0x20c Process Name: C:\Windows\System32\winlogon.exe Network Information: Network Address: 127.0.0.1 Port: 0 This event is generated when a process attempts to log on an account by explicitly specifying that account's credentials. This most commonly occurs in batch-type configurations such as scheduled tasks, or when using the RUNAS command.
Security	Audit Success	12544	2015-04-25 10:42:30	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: LTRANPHD$ Account Domain: WORKGROUP Logon ID: 0x3e7 Logon Type: 2 Impersonation Level: %%1833 New Logon: Security ID: S-1-5-21-1888849264-3803429180-4108621888-1001 Account Name: Liem Account Domain: LTRANPHD Logon ID: 0x1958f Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x20c Process Name: C:\Windows\System32\winlogon.exe Network Information: Workstation Name: LTRANPHD Source Network Address: 127.0.0.1 Source Port: 0 Detailed Authentication Information: Logon Process: User32 Authentication Package: Negotiate Transited Services: - Package Name (NTLM only): - Key Length: 0 This event is generated when a logon session is created. It is generated on the computer that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service such as the Server service, or a local process such as Winlogon.exe or Services.exe. The logon type field indicates the kind of logon that occurred. The most common types are 2 (interactive) and 3 (network). The New Logon fields indicate the account for whom the new logon was created, i.e. the account that was logged on. The network fields indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impersonation level field indicates the extent to which a process in the logon session can impersonate. The authentication information fields provide detailed information about this specific logon request. - Logon GUID is a unique identifier that can be used to correlate this event with a KDC event. - Transited services indicate which intermediate services have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indicates the length of the generated session key. This will be 0 if no session key was requested.
Security	Audit Success	12544	2015-04-25 10:42:30	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: LTRANPHD$ Account Domain: WORKGROUP Logon ID: 0x3e7 Logon Type: 2 Impersonation Level: %%1833 New Logon: Security ID: S-1-5-21-1888849264-3803429180-4108621888-1001 Account Name: Liem Account Domain: LTRANPHD Logon ID: 0x195be Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x20c Process Name: C:\Windows\System32\winlogon.exe Network Information: Workstation Name: LTRANPHD Source Network Address: 127.0.0.1 Source Port: 0 Detailed Authentication Information: Logon Process: User32 Authentication Package: Negotiate Transited Services: - Package Name (NTLM only): - Key Length: 0 This event is generated when a logon session is created. It is generated on the computer that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service such as the Server service, or a local process such as Winlogon.exe or Services.exe. The logon type field indicates the kind of logon that occurred. The most common types are 2 (interactive) and 3 (network). The New Logon fields indicate the account for whom the new logon was created, i.e. the account that was logged on. The network fields indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impersonation level field indicates the extent to which a process in the logon session can impersonate. The authentication information fields provide detailed information about this specific logon request. - Logon GUID is a unique identifier that can be used to correlate this event with a KDC event. - Transited services indicate which intermediate services have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indicates the length of the generated session key. This will be 0 if no session key was requested.
Security	Audit Success	12544	2015-04-25 10:42:30	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: LTRANPHD$ Account Domain: WORKGROUP Logon ID: 0x3e7 Logon Type: 5 Impersonation Level: %%1833 New Logon: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Logon ID: 0x3e7 Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x23c Process Name: C:\Windows\System32\services.exe Network Information: Workstation Name: Source Network Address: - Source Port: - Detailed Authentication Information: Logon Process: Advapi Authentication Package: Negotiate Transited Services: - Package Name (NTLM only): - Key Length: 0 This event is generated when a logon session is created. It is generated on the computer that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service such as the Server service, or a local process such as Winlogon.exe or Services.exe. The logon type field indicates the kind of logon that occurred. The most common types are 2 (interactive) and 3 (network). The New Logon fields indicate the account for whom the new logon was created, i.e. the account that was logged on. The network fields indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impersonation level field indicates the extent to which a process in the logon session can impersonate. The authentication information fields provide detailed information about this specific logon request. - Logon GUID is a unique identifier that can be used to correlate this event with a KDC event. - Transited services indicate which intermediate services have participated in this logon request. - Package name indicates

					which sub-protocol was used among the NTLM protocols. - Key length indicates the length of the generated session key. This will be 0 if no session key was requested.
Security	Audit Success	12548	2015-04-25 10:42:30	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-21-1888849264-3803429180-4108621888-1001 Account Name: Liem Account Domain: LTRANPHD Logon ID: 0x1958f Privileges: SeSecurityPrivilege SeTakeOwnershipPrivilege SeLoadDriverPrivilege SeBackupPrivilege SeRestorePrivilege SeDebugPrivilege SeSystemEnvironmentPrivilege SeImpersonatePrivilege
Security	Audit Success	12548	2015-04-25 10:42:30	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Logon ID: 0x3e7 Privileges: SeAssignPrimaryTokenPrivilege SeTcbPrivilege SeSecurityPrivilege SeTakeOwnershipPrivilege SeLoadDriverPrivilege SeBackupPrivilege SeRestorePrivilege SeDebugPrivilege SeAuditPrivilege SeSystemEnvironmentPrivilege SeImpersonatePrivilege
Security	Audit Success	13824	2015-04-25 10:42:32	Microsoft-Windows-Security-Auditing	4797: An attempt was made to query the existence of a blank password for an account. Subject: Security ID: S-1-5-21-1888849264-3803429180-4108621888-1001 Account Name: Liem Account Domain: LTRANPHD Logon ID: 0x195be Additional Information: Caller Workstation: LTRANPHD Target Account Name: Administrator Target Account Domain: LTRANPHD
Security	Audit Success	13824	2015-04-25 10:42:32	Microsoft-Windows-Security-Auditing	4797: An attempt was made to query the existence of a blank password for an account. Subject: Security ID: S-1-5-21-1888849264-3803429180-4108621888-1001 Account Name: Liem Account Domain: LTRANPHD Logon ID: 0x195be Additional Information: Caller Workstation: LTRANPHD Target Account Name: Guest Target Account Domain: LTRANPHD
Security	Audit Success	13824	2015-04-25 10:42:32	Microsoft-Windows-Security-Auditing	4797: An attempt was made to query the existence of a blank password for an account. Subject: Security ID: S-1-5-21-1888849264-3803429180-4108621888-1001 Account Name: Liem Account Domain: LTRANPHD Logon ID: 0x195be Additional Information: Caller Workstation: LTRANPHD Target Account Name: Administrator Target Account Domain: LTRANPHD
Security	Audit Success	13824	2015-04-25 10:42:32	Microsoft-Windows-Security-Auditing	4797: An attempt was made to query the existence of a blank password for an account. Subject: Security ID: S-1-5-21-1888849264-3803429180-4108621888-1001 Account Name: Liem Account Domain: LTRANPHD Logon ID: 0x195be Additional Information: Caller Workstation: LTRANPHD Target Account Name: Guest Target Account Domain: LTRANPHD
Security	Audit Success	13824	2015-04-25 10:42:38	Microsoft-Windows-Security-Auditing	4797: An attempt was made to query the existence of a blank password for an account. Subject: Security ID: S-1-5-19 Account Name: LOCAL SERVICE Account Domain: NT AUTHORITY Logon ID: 0x3e5 Additional Information: Caller Workstation: LTRANPHD Target Account Name: Administrator Target Account Domain: LTRANPHD
Security	Audit Success	13824	2015-04-25 10:42:38	Microsoft-Windows-Security-Auditing	4797: An attempt was made to query the existence of a blank password for an account. Subject: Security ID: S-1-5-19 Account Name: LOCAL SERVICE Account Domain: NT AUTHORITY Logon ID: 0x3e5 Additional Information: Caller Workstation: LTRANPHD Target Account Name: Guest Target Account Domain: LTRANPHD
Security	Audit Success	13824	2015-04-25 10:42:38	Microsoft-Windows-Security-Auditing	4797: An attempt was made to query the existence of a blank password for an account. Subject: Security ID: S-1-5-19 Account Name: LOCAL SERVICE Account Domain: NT AUTHORITY Logon ID: 0x3e5 Additional Information: Caller Workstation: LTRANPHD Target Account Name: Liem Target Account Domain: LTRANPHD
Security	Audit Success	13824	2015-04-25 10:42:38	Microsoft-Windows-Security-Auditing	4797: An attempt was made to query the existence of a blank password for an account. Subject: Security ID: S-1-5-19 Account Name: LOCAL SERVICE Account Domain: NT AUTHORITY Logon ID: 0x3e5 Additional Information: Caller Workstation: LTRANPHD Target Account Name: Liem Target Account Domain: LTRANPHD
Security	Audit Success	103	2015-04-25 10:46:45	Microsoft-Windows-Eventlog	1100: The event logging service has shut down.
Security	Audit Success	12545	2015-04-25 10:46:45	Microsoft-Windows-Security-Auditing	4647: User initiated logoff: Subject: Security ID: S-1-5-21-1888849264-3803429180-4108621888-1001 Account Name: Liem Account Domain: LTRANPHD Logon ID: 0x195be This event is generated when a logoff is initiated. No further user-initiated activity can occur. This event can be interpreted as a logoff event.
Security	Audit Success	12288	2015-04-25 10:46:57	Microsoft-Windows-Security-Auditing	4608: Windows is starting up. This event is logged when LSASS.EXE starts and the auditing subsystem is initialized.
Security	Audit Success	12292	2015-04-25 10:46:57	Microsoft-Windows-Security-Auditing	5033: The Windows Firewall Driver started successfully.
Security	Audit Success	12544	2015-04-25 10:46:57	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-0-0 Account Name: - Account Domain: - Logon ID: 0x0 Logon Type: 0 Impersonation Level: - New Logon: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Logon ID: 0x3e7 Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x4 Process Name: Network Information: Workstation Name: - Source Network Address: - Source Port: - Detailed Authentication Information: Logon Process: - Authentication Package: - Transited Services: - Package Name (NTLM only): - Key Length: 0 This event is generated when a logon session is created. It is generated on the computer that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service such as the Server service, or a local process such as Winlogon.exe or Services.exe. The logon type field indicates the kind of logon that occurred. The most common types are 2 (interactive) and 3 (network). The New Logon fields indicate the account for whom the new logon was created, i.e. the account that was logged on. The network fields indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impersonation level field indicates the extent to which a

					process in the logon session can impersonate. The authentication information fields provide detailed information about this specific logon request. - Logon GUID is a unique identifier that can be used to correlate this event with a KDC event. - Transited services indicate which intermediate services have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indicates the length of the generated session key. This will be 0 if no session key was requested.
Security	Audit Success	12544	2015-04-25 10:46:57	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: LTRANPHD$ Account Domain: WORKGROUP Logon ID: 0x3e7 Logon Type: 5 Impersonation Level: %%1833 New Logon: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Logon ID: 0x3e7 Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x244 Process Name: C:\Windows\System32\services.exe Network Information: Workstation Name: Source Network Address: - Source Port: - Detailed Authentication Information: Logon Process: Advapi Authentication Package: Negotiate Transited Services: - Package Name (NTLM only): - Key Length: 0 This event is generated when a logon session is created. It is generated on the computer that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service such as the Server service, or a local process such as Winlogon.exe or Services.exe. The logon type field indicates the kind of logon that occurred. The most common types are 2 (interactive) and 3 (network). The New Logon fields indicate the account for whom the new logon was created, i.e. the account that was logged on. The network fields indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impersonation level field indicates the extent to which a process in the logon session can impersonate. The authentication information fields provide detailed information about this specific logon request. - Logon GUID is a unique identifier that can be used to correlate this event with a KDC event. - Transited services indicate which intermediate services have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indicates the length of the generated session key. This will be 0 if no session key was requested.
Security	Audit Success	12544	2015-04-25 10:46:57	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: LTRANPHD$ Account Domain: WORKGROUP Logon ID: 0x3e7 Logon Type: 5 Impersonation Level: %%1833 New Logon: Security ID: S-1-5-20 Account Name: NETWORK SERVICE Account Domain: NT AUTHORITY Logon ID: 0x3e4 Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x244 Process Name: C:\Windows\System32\services.exe Network Information: Workstation Name: Source Network Address: - Source Port: - Detailed Authentication Information: Logon Process: Advapi Authentication Package: Negotiate Transited Services: - Package Name (NTLM only): - Key Length: 0 This event is generated when a logon session is created. It is generated on the computer that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service such as the Server service, or a local process such as Winlogon.exe or Services.exe. The logon type field indicates the kind of logon that occurred. The most common types are 2 (interactive) and 3 (network). The New Logon fields indicate the account for whom the new logon was created, i.e. the account that was logged on. The network fields indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impersonation level field indicates the extent to which a process in the logon session can impersonate. The authentication information fields provide detailed information about this specific logon request. - Logon GUID is a unique identifier that can be used to correlate this event with a KDC event. - Transited services indicate which intermediate services have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indicates the length of the generated session key. This will be 0 if no session key was requested.
Security	Audit Success	12544	2015-04-25 10:46:57	Microsoft-Windows-Security-Auditing	4648: A logon was attempted using explicit credentials. Subject: Security ID: S-1-5-18 Account Name: LTRANPHD$ Account Domain: WORKGROUP Logon ID: 0x3e7 Logon GUID: {00000000-0000-0000-0000-000000000000} Account Whose Credentials Were Used: Account Name: DWM-1 Account Domain: Window Manager Logon GUID: {00000000-0000-0000-0000-000000000000} Target Server: Target Server Name: localhost Additional Information: localhost Process Information: Process ID: 0x214 Process Name: C:\Windows\System32\winlogon.exe Network Information: Network Address: - Port: - This event is generated when a process attempts to log on an account by explicitly specifying that account's credentials. This most commonly occurs in batch-type configurations such as scheduled tasks, or when using the RUNAS command.
Security	Audit Success	12544	2015-04-25 10:46:57	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: LTRANPHD$ Account Domain: WORKGROUP Logon ID: 0x3e7 Logon Type: 2 Impersonation Level: %%1833 New Logon: Security ID: S-1-5-90-1 Account Name: DWM-1 Account Domain: Window Manager Logon ID: 0xc322 Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x214 Process Name: C:\Windows\System32\winlogon.exe Network Information: Workstation Name: Source Network Address: - Source Port: - Detailed Authentication Information: Logon Process: Advapi Authentication Package: Negotiate Transited Services: - Package Name (NTLM only): - Key Length: 0 This event is generated when a logon session is created. It is generated on the computer that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service such as the Server service, or a local process such as Winlogon.exe or Services.exe. The logon type field indicates the kind of logon that occurred. The most common types are 2 (interactive) and 3 (network). The New Logon fields indicate the account for whom the new logon was created, i.e. the account that was logged on. The network fields indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impersonation level field indicates the extent to which a process in the logon session can impersonate. The authentication information fields provide detailed information about this specific logon request. - Logon GUID is a unique identifier that can be used to correlate this event with a KDC event. - Transited

					services indicate which intermediate services have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indicates the length of the generated session key. This will be 0 if no session key was requested.
Security	Audit Success	12544	2015-04-25 10:46:57	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: LTRANPHD$ Account Domain: WORKGROUP Logon ID: 0x3e7 Logon Type: 2 Impersonation Level: %%1833 New Logon: Security ID: S-1-5-90-1 Account Name: DWM-1 Account Domain: Window Manager Logon ID: 0xc33c Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x214 Process Name: C:\Windows\System32\winlogon.exe Network Information: Workstation Name: Source Network Address: - Source Port: - Detailed Authentication Information: Logon Process: Advapi Authentication Package: Negotiate Transited Services: - Package Name (NTLM only): - Key Length: 0 This event is generated when a logon session is created. It is generated on the computer that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service such as the Server service, or a local process such as Winlogon.exe or Services.exe. The logon type field indicates the kind of logon that occurred. The most common types are 2 (interactive) and 3 (network). The New Logon fields indicate the account for whom the new logon was created, i.e. the account that was logged on. The network fields indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impersonation level field indicates the extent to which a process in the logon session can impersonate. The authentication information fields provide detailed information about this specific logon request. - Logon GUID is a unique identifier that can be used to correlate this event with a KDC event. - Transited services indicate which intermediate services have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indicates the length of the generated session key. This will be 0 if no session key was requested.
Security	Audit Success	12544	2015-04-25 10:46:57	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: LTRANPHD$ Account Domain: WORKGROUP Logon ID: 0x3e7 Logon Type: 5 Impersonation Level: %%1833 New Logon: Security ID: S-1-5-19 Account Name: LOCAL SERVICE Account Domain: NT AUTHORITY Logon ID: 0x3e5 Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x244 Process Name: C:\Windows\System32\services.exe Network Information: Workstation Name: Source Network Address: - Source Port: - Detailed Authentication Information: Logon Process: Advapi Authentication Package: Negotiate Transited Services: - Package Name (NTLM only): - Key Length: 0 This event is generated when a logon session is created. It is generated on the computer that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service such as the Server service, or a local process such as Winlogon.exe or Services.exe. The logon type field indicates the kind of logon that occurred. The most common types are 2 (interactive) and 3 (network). The New Logon fields indicate the account for whom the new logon was created, i.e. the account that was logged on. The network fields indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impersonation level field indicates the extent to which a process in the logon session can impersonate. The authentication information fields provide detailed information about this specific logon request. - Logon GUID is a unique identifier that can be used to correlate this event with a KDC event. - Transited services indicate which intermediate services have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indicates the length of the generated session key. This will be 0 if no session key was requested.
Security	Audit Success	12544	2015-04-25 10:46:57	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: LTRANPHD$ Account Domain: WORKGROUP Logon ID: 0x3e7 Logon Type: 5 Impersonation Level: %%1833 New Logon: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Logon ID: 0x3e7 Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x244 Process Name: C:\Windows\System32\services.exe Network Information: Workstation Name: Source Network Address: - Source Port: - Detailed Authentication Information: Logon Process: Advapi Authentication Package: Negotiate Transited Services: - Package Name (NTLM only): - Key Length: 0 This event is generated when a logon session is created. It is generated on the computer that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service such as the Server service, or a local process such as Winlogon.exe or Services.exe. The logon type field indicates the kind of logon that occurred. The most common types are 2 (interactive) and 3 (network). The New Logon fields indicate the account for whom the new logon was created, i.e. the account that was logged on. The network fields indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impersonation level field indicates the extent to which a process in the logon session can impersonate. The authentication information fields provide detailed information about this specific logon request. - Logon GUID is a unique identifier that can be used to correlate this event with a KDC event. - Transited services indicate which intermediate services have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indicates the length of the generated session key. This will be 0 if no session key was requested.
					4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: LTRANPHD$ Account Domain: WORKGROUP Logon ID: 0x3e7 Logon Type: 5 Impersonation Level: %%1833 New Logon: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Logon ID: 0x3e7 Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x244 Process Name: C:\Windows\System32\services.exe Network Information: Workstation Name: Source Network Address: - Source Port: - Detailed Authentication Information: Logon Process: Advapi Authentication Package: Negotiate Transited Services: - Package Name (NTLM only): - Key Length: 0 This event is generated when a logon session is

Security	Audit Success	12544	2015-04-25 10:46:57	Microsoft-Windows-Security-Auditing	created. It is generated on the computer that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service such as the Server service, or a local process such as Winlogon.exe or Services.exe. The logon type field indicates the kind of logon that occurred. The most common types are 2 (interactive) and 3 (network). The New Logon fields indicate the account for whom the new logon was created, i.e. the account that was logged on. The network fields indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impersonation level field indicates the extent to which a process in the logon session can impersonate. The authentication information fields provide detailed information about this specific logon request. - Logon GUID is a unique identifier that can be used to correlate this event with a KDC event. - Transited services indicate which intermediate services have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indicates the length of the generated session key. This will be 0 if no session key was requested.
Security	Audit Success	12544	2015-04-25 10:46:57	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: LTRANPHD$ Account Domain: WORKGROUP Logon ID: 0x3e7 Logon Type: 5 Impersonation Level: %%1833 New Logon: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Logon ID: 0x3e7 Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x244 Process Name: C:\Windows\System32\services.exe Network Information: Workstation Name: Source Network Address: - Source Port: - Detailed Authentication Information: Logon Process: Advapi Authentication Package: Negotiate Transited Services: - Package Name (NTLM only): - Key Length: 0 This event is generated when a logon session is created. It is generated on the computer that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service such as the Server service, or a local process such as Winlogon.exe or Services.exe. The logon type field indicates the kind of logon that occurred. The most common types are 2 (interactive) and 3 (network). The New Logon fields indicate the account for whom the new logon was created, i.e. the account that was logged on. The network fields indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impersonation level field indicates the extent to which a process in the logon session can impersonate. The authentication information fields provide detailed information about this specific logon request. - Logon GUID is a unique identifier that can be used to correlate this event with a KDC event. - Transited services indicate which intermediate services have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indicates the length of the generated session key. This will be 0 if no session key was requested.
Security	Audit Success	12544	2015-04-25 10:46:57	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: LTRANPHD$ Account Domain: WORKGROUP Logon ID: 0x3e7 Logon Type: 5 Impersonation Level: %%1833 New Logon: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Logon ID: 0x3e7 Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x244 Process Name: C:\Windows\System32\services.exe Network Information: Workstation Name: Source Network Address: - Source Port: - Detailed Authentication Information: Logon Process: Advapi Authentication Package: Negotiate Transited Services: - Package Name (NTLM only): - Key Length: 0 This event is generated when a logon session is created. It is generated on the computer that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service such as the Server service, or a local process such as Winlogon.exe or Services.exe. The logon type field indicates the kind of logon that occurred. The most common types are 2 (interactive) and 3 (network). The New Logon fields indicate the account for whom the new logon was created, i.e. the account that was logged on. The network fields indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impersonation level field indicates the extent to which a process in the logon session can impersonate. The authentication information fields provide detailed information about this specific logon request. - Logon GUID is a unique identifier that can be used to correlate this event with a KDC event. - Transited services indicate which intermediate services have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indicates the length of the generated session key. This will be 0 if no session key was requested.
Security	Audit Success	12548	2015-04-25 10:46:57	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Logon ID: 0x3e7 Privileges: SeAssignPrimaryTokenPrivilege SeTcbPrivilege SeSecurityPrivilege SeTakeOwnershipPrivilege SeLoadDriverPrivilege SeBackupPrivilege SeRestorePrivilege SeDebugPrivilege SeAuditPrivilege SeSystemEnvironmentPrivilege SeImpersonatePrivilege
Security	Audit Success	12548	2015-04-25 10:46:57	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-20 Account Name: NETWORK SERVICE Account Domain: NT AUTHORITY Logon ID: 0x3e4 Privileges: SeAssignPrimaryTokenPrivilege SeAuditPrivilege SeImpersonatePrivilege
Security	Audit Success	12548	2015-04-25 10:46:57	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-90-1 Account Name: DWM-1 Account Domain: Window Manager Logon ID: 0xc322 Privileges: SeAssignPrimaryTokenPrivilege SeAuditPrivilege SeImpersonatePrivilege
Security	Audit Success	12548	2015-04-25 10:46:57	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-90-1 Account Name: DWM-1 Account Domain: Window Manager Logon ID: 0xc33c Privileges: SeAssignPrimaryTokenPrivilege SeAuditPrivilege
Security	Audit Success	12548	2015-04-25 10:46:57	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-19 Account Name: LOCAL SERVICE Account Domain: NT AUTHORITY Logon ID: 0x3e5 Privileges: SeAssignPrimaryTokenPrivilege SeAuditPrivilege SeImpersonatePrivilege

Security	Audit Success	12548	2015-04-25 10:46:57	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Logon ID: 0x3e7 Privileges: SeAssignPrimaryTokenPrivilege SeTcbPrivilege SeSecurityPrivilege SeTakeOwnershipPrivilege SeLoadDriverPrivilege SeBackupPrivilege SeRestorePrivilege SeDebugPrivilege SeAuditPrivilege SeSystemEnvironmentPrivilege SeImpersonatePrivilege
Security	Audit Success	12548	2015-04-25 10:46:57	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Logon ID: 0x3e7 Privileges: SeAssignPrimaryTokenPrivilege SeTcbPrivilege SeSecurityPrivilege SeTakeOwnershipPrivilege SeLoadDriverPrivilege SeBackupPrivilege SeRestorePrivilege SeDebugPrivilege SeAuditPrivilege SeSystemEnvironmentPrivilege SeImpersonatePrivilege
Security	Audit Success	12548	2015-04-25 10:46:57	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Logon ID: 0x3e7 Privileges: SeAssignPrimaryTokenPrivilege SeTcbPrivilege SeSecurityPrivilege SeTakeOwnershipPrivilege SeLoadDriverPrivilege SeBackupPrivilege SeRestorePrivilege SeDebugPrivilege SeAuditPrivilege SeSystemEnvironmentPrivilege SeImpersonatePrivilege
Security	Audit Success	12548	2015-04-25 10:46:57	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Logon ID: 0x3e7 Privileges: SeAssignPrimaryTokenPrivilege SeTcbPrivilege SeSecurityPrivilege SeTakeOwnershipPrivilege SeLoadDriverPrivilege SeBackupPrivilege SeRestorePrivilege SeDebugPrivilege SeAuditPrivilege SeSystemEnvironmentPrivilege SeImpersonatePrivilege
Security	Audit Success	13568	2015-04-25 10:46:57	Microsoft-Windows-Security-Auditing	4902: The Per-user audit policy table was created. Number of Elements: 0 Policy ID: 0x7459
Security	Audit Success	12292	2015-04-25 10:46:58	Microsoft-Windows-Security-Auditing	5024: The Windows Firewall service started successfully.
Security	Audit Success	12544	2015-04-25 10:46:58	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: LTRANPHD$ Account Domain: WORKGROUP Logon ID: 0x3e7 Logon Type: 5 Impersonation Level: %%1833 New Logon: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Logon ID: 0x3e7 Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x244 Process Name: C:\Windows\System32\services.exe Network Information: Workstation Name: Source Network Address: - Source Port: - Detailed Authentication Information: Logon Process: Advapi Authentication Package: Negotiate Transited Services: - Package Name (NTLM only): - Key Length: 0 This event is generated when a logon session is created. It is generated on the computer that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service such as the Server service, or a local process such as Winlogon.exe or Services.exe. The logon type field indicates the kind of logon that occurred. The most common types are 2 (interactive) and 3 (network). The New Logon fields indicate the account for whom the new logon was created, i.e. the account that was logged on. The network fields indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impersonation level field indicates the extent to which a process in the logon session can impersonate. The authentication information fields provide detailed information about this specific logon request. - Logon GUID is a unique identifier that can be used to correlate this event with a KDC event. - Transited services indicate which intermediate services have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indicates the length of the generated session key. This will be 0 if no session key was requested.
Security	Audit Success	12544	2015-04-25 10:46:58	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-0-0 Account Name: - Account Domain: - Logon ID: 0x0 Logon Type: 3 Impersonation Level: %%1833 New Logon: Security ID: S-1-5-7 Account Name: ANONYMOUS LOGON Account Domain: NT AUTHORITY Logon ID: 0x17f27 Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x0 Process Name: - Network Information: Workstation Name: Source Network Address: - Source Port: - Detailed Authentication Information: Logon Process: NtLmSsp Authentication Package: NTLM Transited Services: - Package Name (NTLM only): NTLM V1 Key Length: 0 This event is generated when a logon session is created. It is generated on the computer that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service such as the Server service, or a local process such as Winlogon.exe or Services.exe. The logon type field indicates the kind of logon that occurred. The most common types are 2 (interactive) and 3 (network). The New Logon fields indicate the account for whom the new logon was created, i.e. the account that was logged on. The network fields indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impersonation level field indicates the extent to which a process in the logon session can impersonate. The authentication information fields provide detailed information about this specific logon request. - Logon GUID is a unique identifier that can be used to correlate this event with a KDC event. - Transited services indicate which intermediate services have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indicates the length of the generated session key. This will be 0 if no session key was requested.
Security	Audit Success	12548	2015-04-25 10:46:58	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Logon ID: 0x3e7 Privileges: SeAssignPrimaryTokenPrivilege SeTcbPrivilege SeSecurityPrivilege SeTakeOwnershipPrivilege SeLoadDriverPrivilege SeBackupPrivilege SeRestorePrivilege SeDebugPrivilege SeAuditPrivilege SeSystemEnvironmentPrivilege SeImpersonatePrivilege
Security	Audit Success	103	2015-04-25	Microsoft-Windows-Eventlog	1100: The event logging service has shut down.

			10:47:04		
Security	Audit Success	12288	2015-04-25 10:48:25	Microsoft-Windows-Security-Auditing	4608: Windows is starting up. This event is logged when LSASS.EXE starts and the auditing subsystem is initialized.
Security	Audit Success	12544	2015-04-25 10:48:25	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-0-0 Account Name: - Account Domain: - Logon ID: 0x0 Logon Type: 0 Impersonation Level: - New Logon: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Logon ID: 0x3e7 Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x4 Process Name: Network Information: Workstation Name: - Source Network Address: - Source Port: - Detailed Authentication Information: Logon Process: - Authentication Package: - Transited Services: - Package Name (NTLM only): - Key Length: 0 This event is generated when a logon session is created. It is generated on the computer that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service such as the Server service, or a local process such as Winlogon.exe or Services.exe. The logon type field indicates the kind of logon that occurred. The most common types are 2 (interactive) and 3 (network). The New Logon fields indicate the account for whom the new logon was created, i.e. the account that was logged on. The network fields indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impersonation level field indicates the extent to which a process in the logon session can impersonate. The authentication information fields provide detailed information about this specific logon request. - Logon GUID is a unique identifier that can be used to correlate this event with a KDC event. - Transited services indicate which intermediate services have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indicates the length of the generated session key. This will be 0 if no session key was requested.
Security	Audit Success	12544	2015-04-25 10:48:25	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: LTRANPHD$ Account Domain: WORKGROUP Logon ID: 0x3e7 Logon Type: 5 Impersonation Level: %%1833 New Logon: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Logon ID: 0x3e7 Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x23c Process Name: C:\Windows\System32\services.exe Network Information: Workstation Name: Source Network Address: - Source Port: - Detailed Authentication Information: Logon Process: Advapi Authentication Package: Negotiate Transited Services: - Package Name (NTLM only): - Key Length: 0 This event is generated when a logon session is created. It is generated on the computer that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service such as the Server service, or a local process such as Winlogon.exe or Services.exe. The logon type field indicates the kind of logon that occurred. The most common types are 2 (interactive) and 3 (network). The New Logon fields indicate the account for whom the new logon was created, i.e. the account that was logged on. The network fields indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impersonation level field indicates the extent to which a process in the logon session can impersonate. The authentication information fields provide detailed information about this specific logon request. - Logon GUID is a unique identifier that can be used to correlate this event with a KDC event. - Transited services indicate which intermediate services have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indicates the length of the generated session key. This will be 0 if no session key was requested.
Security	Audit Success	12544	2015-04-25 10:48:25	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: LTRANPHD$ Account Domain: WORKGROUP Logon ID: 0x3e7 Logon Type: 5 Impersonation Level: %%1833 New Logon: Security ID: S-1-5-20 Account Name: NETWORK SERVICE Account Domain: NT AUTHORITY Logon ID: 0x3e4 Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x23c Process Name: C:\Windows\System32\services.exe Network Information: Workstation Name: Source Network Address: - Source Port: - Detailed Authentication Information: Logon Process: Advapi Authentication Package: Negotiate Transited Services: - Package Name (NTLM only): - Key Length: 0 This event is generated when a logon session is created. It is generated on the computer that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service such as the Server service, or a local process such as Winlogon.exe or Services.exe. The logon type field indicates the kind of logon that occurred. The most common types are 2 (interactive) and 3 (network). The New Logon fields indicate the account for whom the new logon was created, i.e. the account that was logged on. The network fields indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impersonation level field indicates the extent to which a process in the logon session can impersonate. The authentication information fields provide detailed information about this specific logon request. - Logon GUID is a unique identifier that can be used to correlate this event with a KDC event. - Transited services indicate which intermediate services have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indicates the length of the generated session key. This will be 0 if no session key was requested.
Security	Audit Success	12544	2015-04-25 10:48:25	Microsoft-Windows-Security-Auditing	4648: A logon was attempted using explicit credentials. Subject: Security ID: S-1-5-18 Account Name: LTRANPHD$ Account Domain: WORKGROUP Logon ID: 0x3e7 Logon GUID: {00000000-0000-0000-0000-000000000000} Account Whose Credentials Were Used: Account Name: DWM-1 Account Domain: Window Manager Logon GUID: {00000000-0000-0000-0000-000000000000} Target Server: Target Server Name: localhost Additional Information: localhost Process Information: Process ID: 0x20c Process Name: C:\Windows\System32\winlogon.exe Network Information: Network Address: - Port: - This event is generated

					when a process attempts to log on an account by explicitly specifying that account's credentials. This most commonly occurs in batch-type configurations such as scheduled tasks, or when using the RUNAS command.
Security	Audit Success	12544	2015-04-25 10:48:25	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: LTRANPHD$ Account Domain: WORKGROUP Logon ID: 0x3e7 Logon Type: 2 Impersonation Level: %%1833 New Logon: Security ID: S-1-5-90-1 Account Name: DWM-1 Account Domain: Window Manager Logon ID: 0xc32c Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x20c Process Name: C:\Windows\System32\winlogon.exe Network Information: Workstation Name: Source Network Address: - Source Port: - Detailed Authentication Information: Logon Process: Advapi Authentication Package: Negotiate Transited Services: - Package Name (NTLM only): - Key Length: 0 This event is generated when a logon session is created. It is generated on the computer that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service such as the Server service, or a local process such as Winlogon.exe or Services.exe. The logon type field indicates the kind of logon that occurred. The most common types are 2 (interactive) and 3 (network). The New Logon fields indicate the account for whom the new logon was created, i.e. the account that was logged on. The network fields indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impersonation level field indicates the extent to which a process in the logon session can impersonate. The authentication information fields provide detailed information about this specific logon request. - Logon GUID is a unique identifier that can be used to correlate this event with a KDC event. - Transited services indicate which intermediate services have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indicates the length of the generated session key. This will be 0 if no session key was requested.
Security	Audit Success	12544	2015-04-25 10:48:25	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: LTRANPHD$ Account Domain: WORKGROUP Logon ID: 0x3e7 Logon Type: 2 Impersonation Level: %%1833 New Logon: Security ID: S-1-5-90-1 Account Name: DWM-1 Account Domain: Window Manager Logon ID: 0xc342 Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x20c Process Name: C:\Windows\System32\winlogon.exe Network Information: Workstation Name: Source Network Address: - Source Port: - Detailed Authentication Information: Logon Process: Advapi Authentication Package: Negotiate Transited Services: - Package Name (NTLM only): - Key Length: 0 This event is generated when a logon session is created. It is generated on the computer that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service such as the Server service, or a local process such as Winlogon.exe or Services.exe. The logon type field indicates the kind of logon that occurred. The most common types are 2 (interactive) and 3 (network). The New Logon fields indicate the account for whom the new logon was created, i.e. the account that was logged on. The network fields indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impersonation level field indicates the extent to which a process in the logon session can impersonate. The authentication information fields provide detailed information about this specific logon request. - Logon GUID is a unique identifier that can be used to correlate this event with a KDC event. - Transited services indicate which intermediate services have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indicates the length of the generated session key. This will be 0 if no session key was requested.
Security	Audit Success	12544	2015-04-25 10:48:25	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: LTRANPHD$ Account Domain: WORKGROUP Logon ID: 0x3e7 Logon Type: 5 Impersonation Level: %%1833 New Logon: Security ID: S-1-5-19 Account Name: LOCAL SERVICE Account Domain: NT AUTHORITY Logon ID: 0x3e5 Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x23c Process Name: C:\Windows\System32\services.exe Network Information: Workstation Name: Source Network Address: - Source Port: - Detailed Authentication Information: Logon Process: Advapi Authentication Package: Negotiate Transited Services: - Package Name (NTLM only): - Key Length: 0 This event is generated when a logon session is created. It is generated on the computer that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service such as the Server service, or a local process such as Winlogon.exe or Services.exe. The logon type field indicates the kind of logon that occurred. The most common types are 2 (interactive) and 3 (network). The New Logon fields indicate the account for whom the new logon was created, i.e. the account that was logged on. The network fields indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impersonation level field indicates the extent to which a process in the logon session can impersonate. The authentication information fields provide detailed information about this specific logon request. - Logon GUID is a unique identifier that can be used to correlate this event with a KDC event. - Transited services indicate which intermediate services have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indicates the length of the generated session key. This will be 0 if no session key was requested.
					4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: LTRANPHD$ Account Domain: WORKGROUP Logon ID: 0x3e7 Logon Type: 5 Impersonation Level: %%1833 New Logon: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Logon ID: 0x3e7 Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x23c Process Name: C:\Windows\System32\services.exe Network Information: Workstation Name: Source Network Address: - Source Port: - Detailed Authentication Information: Logon Process: Advapi Authentication Package: Negotiate Transited Services: - Package Name (NTLM only): - Key Length: 0 This event is generated when a logon session is created. It is generated on the computer that was accessed. The subject fields indicate the account on the local

Security	Audit Success	12544	2015-04-25 10:48:25	Microsoft-Windows-Security-Auditing	system which requested the logon. This is most commonly a service such as the Server service, or a local process such as Winlogon.exe or Services.exe. The logon type field indicates the kind of logon that occurred. The most common types are 2 (interactive) and 3 (network). The New Logon fields indicate the account for whom the new logon was created, i.e. the account that was logged on. The network fields indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impersonation level field indicates the extent to which a process in the logon session can impersonate. The authentication information fields provide detailed information about this specific logon request. - Logon GUID is a unique identifier that can be used to correlate this event with a KDC event. - Transited services indicate which intermediate services have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indicates the length of the generated session key. This will be 0 if no session key was requested.
Security	Audit Success	12544	2015-04-25 10:48:25	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: LTRANPHD$ Account Domain: WORKGROUP Logon ID: 0x3e7 Logon Type: 5 Impersonation Level: %%1833 New Logon: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Logon ID: 0x3e7 Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x23c Process Name: C:\Windows\System32\services.exe Network Information: Workstation Name: Source Network Address: - Source Port: - Detailed Authentication Information: Logon Process: Advapi Authentication Package: Negotiate Transited Services: - Package Name (NTLM only): - Key Length: 0 This event is generated when a logon session is created. It is generated on the computer that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service such as the Server service, or a local process such as Winlogon.exe or Services.exe. The logon type field indicates the kind of logon that occurred. The most common types are 2 (interactive) and 3 (network). The New Logon fields indicate the account for whom the new logon was created, i.e. the account that was logged on. The network fields indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impersonation level field indicates the extent to which a process in the logon session can impersonate. The authentication information fields provide detailed information about this specific logon request. - Logon GUID is a unique identifier that can be used to correlate this event with a KDC event. - Transited services indicate which intermediate services have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indicates the length of the generated session key. This will be 0 if no session key was requested.
Security	Audit Success	12544	2015-04-25 10:48:25	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: LTRANPHD$ Account Domain: WORKGROUP Logon ID: 0x3e7 Logon Type: 5 Impersonation Level: %%1833 New Logon: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Logon ID: 0x3e7 Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x23c Process Name: C:\Windows\System32\services.exe Network Information: Workstation Name: Source Network Address: - Source Port: - Detailed Authentication Information: Logon Process: Advapi Authentication Package: Negotiate Transited Services: - Package Name (NTLM only): - Key Length: 0 This event is generated when a logon session is created. It is generated on the computer that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service such as the Server service, or a local process such as Winlogon.exe or Services.exe. The logon type field indicates the kind of logon that occurred. The most common types are 2 (interactive) and 3 (network). The New Logon fields indicate the account for whom the new logon was created, i.e. the account that was logged on. The network fields indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impersonation level field indicates the extent to which a process in the logon session can impersonate. The authentication information fields provide detailed information about this specific logon request. - Logon GUID is a unique identifier that can be used to correlate this event with a KDC event. - Transited services indicate which intermediate services have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indicates the length of the generated session key. This will be 0 if no session key was requested.
Security	Audit Success	12548	2015-04-25 10:48:25	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Logon ID: 0x3e7 Privileges: SeAssignPrimaryTokenPrivilege SeTcbPrivilege SeSecurityPrivilege SeTakeOwnershipPrivilege SeLoadDriverPrivilege SeBackupPrivilege SeRestorePrivilege SeDebugPrivilege SeAuditPrivilege SeSystemEnvironmentPrivilege SeImpersonatePrivilege
Security	Audit Success	12548	2015-04-25 10:48:25	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-20 Account Name: NETWORK SERVICE Account Domain: NT AUTHORITY Logon ID: 0x3e4 Privileges: SeAssignPrimaryTokenPrivilege SeAuditPrivilege SeImpersonatePrivilege
Security	Audit Success	12548	2015-04-25 10:48:25	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-90-1 Account Name: DWM-1 Account Domain: Window Manager Logon ID: 0xc32c Privileges: SeAssignPrimaryTokenPrivilege SeAuditPrivilege SeImpersonatePrivilege
Security	Audit Success	12548	2015-04-25 10:48:25	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-90-1 Account Name: DWM-1 Account Domain: Window Manager Logon ID: 0xc342 Privileges: SeAssignPrimaryTokenPrivilege SeAuditPrivilege
Security	Audit Success	12548	2015-04-25 10:48:25	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-19 Account Name: LOCAL SERVICE Account Domain: NT AUTHORITY Logon ID: 0x3e5 Privileges: SeAssignPrimaryTokenPrivilege SeAuditPrivilege SeImpersonatePrivilege
					4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account

Security	Audit Success	12548	2015-04-25 10:48:25	Microsoft-Windows-Security-Auditing	Domain: NT AUTHORITY Logon ID: 0x3e7 Privileges: SeAssignPrimaryTokenPrivilege SeTcbPrivilege SeSecurityPrivilege SeTakeOwnershipPrivilege SeLoadDriverPrivilege SeBackupPrivilege SeRestorePrivilege SeDebugPrivilege SeAuditPrivilege SeSystemEnvironmentPrivilege SeImpersonatePrivilege
Security	Audit Success	12548	2015-04-25 10:48:25	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Logon ID: 0x3e7 Privileges: SeAssignPrimaryTokenPrivilege SeTcbPrivilege SeSecurityPrivilege SeTakeOwnershipPrivilege SeLoadDriverPrivilege SeBackupPrivilege SeRestorePrivilege SeDebugPrivilege SeAuditPrivilege SeSystemEnvironmentPrivilege SeImpersonatePrivilege
Security	Audit Success	12548	2015-04-25 10:48:25	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Logon ID: 0x3e7 Privileges: SeAssignPrimaryTokenPrivilege SeTcbPrivilege SeSecurityPrivilege SeTakeOwnershipPrivilege SeLoadDriverPrivilege SeBackupPrivilege SeRestorePrivilege SeDebugPrivilege SeAuditPrivilege SeSystemEnvironmentPrivilege SeImpersonatePrivilege
Security	Audit Success	13568	2015-04-25 10:48:25	Microsoft-Windows-Security-Auditing	4902: The Per-user audit policy table was created. Number of Elements: 0 Policy ID: 0x742d
Security	Audit Success	12292	2015-04-25 10:48:26	Microsoft-Windows-Security-Auditing	5033: The Windows Firewall Driver started successfully.
Security	Audit Success	12292	2015-04-25 10:48:26	Microsoft-Windows-Security-Auditing	5024: The Windows Firewall service started successfully.
Security	Audit Success	12544	2015-04-25 10:48:26	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: LTRANPHD$ Account Domain: WORKGROUP Logon ID: 0x3e7 Logon Type: 5 Impersonation Level: %%1833 New Logon: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Logon ID: 0x3e7 Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x23c Process Name: C:\Windows\System32\services.exe Network Information: Workstation Name: Source Network Address: - Source Port: - Detailed Authentication Information: Logon Process: Advapi Authentication Package: Negotiate Transited Services: - Package Name (NTLM only): - Key Length: 0 This event is generated when a logon session is created. It is generated on the computer that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service such as the Server service, or a local process such as Winlogon.exe or Services.exe. The logon type field indicates the kind of logon that occurred. The most common types are 2 (interactive) and 3 (network). The New Logon fields indicate the account for whom the new logon was created, i.e. the account that was logged on. The network fields indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impersonation level field indicates the extent to which a process in the logon session can impersonate. The authentication information fields provide detailed information about this specific logon request. - Logon GUID is a unique identifier that can be used to correlate this event with a KDC event. - Transited services indicate which intermediate services have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indicates the length of the generated session key. This will be 0 if no session key was requested.
Security	Audit Success	12544	2015-04-25 10:48:26	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: LTRANPHD$ Account Domain: WORKGROUP Logon ID: 0x3e7 Logon Type: 5 Impersonation Level: %%1833 New Logon: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Logon ID: 0x3e7 Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x23c Process Name: C:\Windows\System32\services.exe Network Information: Workstation Name: Source Network Address: - Source Port: - Detailed Authentication Information: Logon Process: Advapi Authentication Package: Negotiate Transited Services: - Package Name (NTLM only): - Key Length: 0 This event is generated when a logon session is created. It is generated on the computer that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service such as the Server service, or a local process such as Winlogon.exe or Services.exe. The logon type field indicates the kind of logon that occurred. The most common types are 2 (interactive) and 3 (network). The New Logon fields indicate the account for whom the new logon was created, i.e. the account that was logged on. The network fields indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impersonation level field indicates the extent to which a process in the logon session can impersonate. The authentication information fields provide detailed information about this specific logon request. - Logon GUID is a unique identifier that can be used to correlate this event with a KDC event. - Transited services indicate which intermediate services have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indicates the length of the generated session key. This will be 0 if no session key was requested.
					4624: An account was successfully logged on. Subject: Security ID: S-1-0-0 Account Name: - Account Domain: - Logon ID: 0x0 Logon Type: 3 Impersonation Level: %%1833 New Logon: Security ID: S-1-5-7 Account Name: ANONYMOUS LOGON Account Domain: NT AUTHORITY Logon ID: 0x17dd0 Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x0 Process Name: - Network Information: Workstation Name: Source Network Address: - Source Port: - Detailed Authentication Information: Logon Process: NtLmSsp Authentication Package: NTLM Transited Services: - Package Name (NTLM only): NTLM V1 Key Length: 0 This event is generated when a logon session is created. It is generated on the computer that

Security	Audit Success	12544	2015-04-25 10:48:26	Microsoft-Windows-Security-Auditing	was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service such as the Server service, or a local process such as Winlogon.exe or Services.exe. The logon type field indicates the kind of logon that occurred. The most common types are 2 (interactive) and 3 (network). The New Logon fields indicate the account for whom the new logon was created, i.e. the account that was logged on. The network fields indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impersonation level field indicates the extent to which a process in the logon session can impersonate. The authentication information fields provide detailed information about this specific logon request. - Logon GUID is a unique identifier that can be used to correlate this event with a KDC event. - Transited services indicate which intermediate services have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indicates the length of the generated session key. This will be 0 if no session key was requested.
Security	Audit Success	12548	2015-04-25 10:48:26	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Logon ID: 0x3e7 Privileges: SeAssignPrimaryTokenPrivilege SeTcbPrivilege SeSecurityPrivilege SeTakeOwnershipPrivilege SeLoadDriverPrivilege SeBackupPrivilege SeRestorePrivilege SeDebugPrivilege SeAuditPrivilege SeSystemEnvironmentPrivilege SeImpersonatePrivilege
Security	Audit Success	12548	2015-04-25 10:48:26	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Logon ID: 0x3e7 Privileges: SeAssignPrimaryTokenPrivilege SeTcbPrivilege SeSecurityPrivilege SeTakeOwnershipPrivilege SeLoadDriverPrivilege SeBackupPrivilege SeRestorePrivilege SeDebugPrivilege SeAuditPrivilege SeSystemEnvironmentPrivilege SeImpersonatePrivilege
Security	Audit Success	12544	2015-04-25 10:48:30	Microsoft-Windows-Security-Auditing	4648: A logon was attempted using explicit credentials. Subject: Security ID: S-1-5-18 Account Name: LTRANPHD$ Account Domain: WORKGROUP Logon ID: 0x3e7 Logon GUID: {00000000-0000-0000-0000-000000000000} Account Whose Credentials Were Used: Account Name: Liem Account Domain: LTRANPHD Logon GUID: {00000000-0000-0000-0000-000000000000} Target Server: Target Server Name: localhost Additional Information: localhost Process Information: Process ID: 0x20c Process Name: C:\Windows\System32\winlogon.exe Network Information: Network Address: 127.0.0.1 Port: 0 This event is generated when a process attempts to log on an account by explicitly specifying that account's credentials. This most commonly occurs in batch-type configurations such as scheduled tasks, or when using the RUNAS command.
Security	Audit Success	12544	2015-04-25 10:48:30	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: LTRANPHD$ Account Domain: WORKGROUP Logon ID: 0x3e7 Logon Type: 2 Impersonation Level: %%1833 New Logon: Security ID: S-1-5-21-1888849264-3803429180-4108621888-1001 Account Name: Liem Account Domain: LTRANPHD Logon ID: 0x1ba49 Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x20c Process Name: C:\Windows\System32\winlogon.exe Network Information: Workstation Name: LTRANPHD Source Network Address: 127.0.0.1 Source Port: 0 Detailed Authentication Information: Logon Process: User32 Authentication Package: Negotiate Transited Services: - Package Name (NTLM only): - Key Length: 0 This event is generated when a logon session is created. It is generated on the computer that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service such as the Server service, or a local process such as Winlogon.exe or Services.exe. The logon type field indicates the kind of logon that occurred. The most common types are 2 (interactive) and 3 (network). The New Logon fields indicate the account for whom the new logon was created, i.e. the account that was logged on. The network fields indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impersonation level field indicates the extent to which a process in the logon session can impersonate. The authentication information fields provide detailed information about this specific logon request. - Logon GUID is a unique identifier that can be used to correlate this event with a KDC event. - Transited services indicate which intermediate services have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indicates the length of the generated session key. This will be 0 if no session key was requested.
Security	Audit Success	12544	2015-04-25 10:48:30	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: LTRANPHD$ Account Domain: WORKGROUP Logon ID: 0x3e7 Logon Type: 2 Impersonation Level: %%1833 New Logon: Security ID: S-1-5-21-1888849264-3803429180-4108621888-1001 Account Name: Liem Account Domain: LTRANPHD Logon ID: 0x1ba7e Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x20c Process Name: C:\Windows\System32\winlogon.exe Network Information: Workstation Name: LTRANPHD Source Network Address: 127.0.0.1 Source Port: 0 Detailed Authentication Information: Logon Process: User32 Authentication Package: Negotiate Transited Services: - Package Name (NTLM only): - Key Length: 0 This event is generated when a logon session is created. It is generated on the computer that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service such as the Server service, or a local process such as Winlogon.exe or Services.exe. The logon type field indicates the kind of logon that occurred. The most common types are 2 (interactive) and 3 (network). The New Logon fields indicate the account for whom the new logon was created, i.e. the account that was logged on. The network fields indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impersonation level field indicates the extent to which a process in the logon session can impersonate. The authentication information fields provide detailed information about this specific logon request. - Logon GUID is a unique identifier that can be used to correlate this event with a KDC event. - Transited services indicate which intermediate services have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indicates the length of the generated session key. This will be 0 if no session key was requested.

Security	Audit Success	12544	2015-04-25 10:48:30	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: LTRANPHD$ Account Domain: WORKGROUP Logon ID: 0x3e7 Logon Type: 5 Impersonation Level: %%1833 New Logon: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Logon ID: 0x3e7 Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x23c Process Name: C:\Windows\System32\services.exe Network Information: Workstation Name: Source Network Address: - Source Port: - Detailed Authentication Information: Logon Process: Advapi Authentication Package: Negotiate Transited Services: - Package Name (NTLM only): - Key Length: 0 This event is generated when a logon session is created. It is generated on the computer that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service such as the Server service, or a local process such as Winlogon.exe or Services.exe. The logon type field indicates the kind of logon that occurred. The most common types are 2 (interactive) and 3 (network). The New Logon fields indicate the account for whom the new logon was created, i.e. the account that was logged on. The network fields indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impersonation level field indicates the extent to which a process in the logon session can impersonate. The authentication information fields provide detailed information about this specific logon request. - Logon GUID is a unique identifier that can be used to correlate this event with a KDC event. - Transited services indicate which intermediate services have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indicates the length of the generated session key. This will be 0 if no session key was requested.
Security	Audit Success	12548	2015-04-25 10:48:30	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-21-1888849264-3803429180-4108621888-1001 Account Name: Liem Account Domain: LTRANPHD Logon ID: 0x1ba49 Privileges: SeSecurityPrivilege SeTakeOwnershipPrivilege SeLoadDriverPrivilege SeBackupPrivilege SeRestorePrivilege SeDebugPrivilege SeSystemEnvironmentPrivilege SeImpersonatePrivilege
Security	Audit Success	12548	2015-04-25 10:48:30	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Logon ID: 0x3e7 Privileges: SeAssignPrimaryTokenPrivilege SeTcbPrivilege SeSecurityPrivilege SeTakeOwnershipPrivilege SeLoadDriverPrivilege SeBackupPrivilege SeRestorePrivilege SeDebugPrivilege SeAuditPrivilege SeSystemEnvironmentPrivilege SeImpersonatePrivilege
Security	Audit Success	13824	2015-04-25 10:48:32	Microsoft-Windows-Security-Auditing	4797: An attempt was made to query the existence of a blank password for an account. Subject: Security ID: S-1-5-21-1888849264-3803429180-4108621888-1001 Account Name: Liem Account Domain: LTRANPHD Logon ID: 0x1ba7e Additional Information: Caller Workstation: LTRANPHD Target Account Name: Administrator Target Account Domain: LTRANPHD
Security	Audit Success	13824	2015-04-25 10:48:32	Microsoft-Windows-Security-Auditing	4797: An attempt was made to query the existence of a blank password for an account. Subject: Security ID: S-1-5-21-1888849264-3803429180-4108621888-1001 Account Name: Liem Account Domain: LTRANPHD Logon ID: 0x1ba7e Additional Information: Caller Workstation: LTRANPHD Target Account Name: Guest Target Account Domain: LTRANPHD
Security	Audit Success	13824	2015-04-25 10:48:32	Microsoft-Windows-Security-Auditing	4797: An attempt was made to query the existence of a blank password for an account. Subject: Security ID: S-1-5-21-1888849264-3803429180-4108621888-1001 Account Name: Liem Account Domain: LTRANPHD Logon ID: 0x1ba7e Additional Information: Caller Workstation: LTRANPHD Target Account Name: Administrator Target Account Domain: LTRANPHD
Security	Audit Success	13824	2015-04-25 10:48:32	Microsoft-Windows-Security-Auditing	4797: An attempt was made to query the existence of a blank password for an account. Subject: Security ID: S-1-5-21-1888849264-3803429180-4108621888-1001 Account Name: Liem Account Domain: LTRANPHD Logon ID: 0x1ba7e Additional Information: Caller Workstation: LTRANPHD Target Account Name: Guest Target Account Domain: LTRANPHD
Security	Audit Success	13824	2015-04-25 10:48:34	Microsoft-Windows-Security-Auditing	4797: An attempt was made to query the existence of a blank password for an account. Subject: Security ID: S-1-5-19 Account Name: LOCAL SERVICE Account Domain: NT AUTHORITY Logon ID: 0x3e5 Additional Information: Caller Workstation: LTRANPHD Target Account Name: Administrator Target Account Domain: LTRANPHD
Security	Audit Success	13824	2015-04-25 10:48:34	Microsoft-Windows-Security-Auditing	4797: An attempt was made to query the existence of a blank password for an account. Subject: Security ID: S-1-5-19 Account Name: LOCAL SERVICE Account Domain: NT AUTHORITY Logon ID: 0x3e5 Additional Information: Caller Workstation: LTRANPHD Target Account Name: Administrator Target Account Domain: LTRANPHD
Security	Audit Success	13824	2015-04-25 10:48:34	Microsoft-Windows-Security-Auditing	4797: An attempt was made to query the existence of a blank password for an account. Subject: Security ID: S-1-5-19 Account Name: LOCAL SERVICE Account Domain: NT AUTHORITY Logon ID: 0x3e5 Additional Information: Caller Workstation: LTRANPHD Target Account Name: Guest Target Account Domain: LTRANPHD
Security	Audit Success	13824	2015-04-25 10:48:34	Microsoft-Windows-Security-Auditing	4797: An attempt was made to query the existence of a blank password for an account. Subject: Security ID: S-1-5-19 Account Name: LOCAL SERVICE Account Domain: NT AUTHORITY Logon ID: 0x3e5 Additional Information: Caller Workstation: LTRANPHD Target Account Name: Guest Target Account Domain: LTRANPHD
Security	Audit Success	13824	2015-04-25 10:48:34	Microsoft-Windows-Security-Auditing	4797: An attempt was made to query the existence of a blank password for an account. Subject: Security ID: S-1-5-19 Account Name: LOCAL SERVICE Account Domain: NT AUTHORITY Logon ID: 0x3e5 Additional Information: Caller Workstation: LTRANPHD Target Account Name: Liem Target Account Domain: LTRANPHD
Security	Audit Success	13824	2015-04-25 10:48:34	Microsoft-Windows-Security-Auditing	4797: An attempt was made to query the existence of a blank password for an account. Subject: Security ID: S-1-5-19 Account Name: LOCAL SERVICE Account Domain: NT AUTHORITY Logon ID: 0x3e5 Additional Information: Caller Workstation: LTRANPHD Target Account Name: Liem Target Account Domain: LTRANPHD
	Audit		2015-04-	Microsoft-Windows-Security-	4797: An attempt was made to query the existence of a blank password for an account. Subject: Security ID:

Security	Success	13824	25 10:48:34	Auditing	S-1-5-19 Account Name: LOCAL SERVICE Account Domain: NT AUTHORITY Logon ID: 0x3e5 Additional Information: Caller Workstation: LTRANPHD Target Account Name: Liem Target Account Domain: LTRANPHD
Security	Audit Success	13824	2015-04-25 10:48:34	Microsoft-Windows-Security-Auditing	4797: An attempt was made to query the existence of a blank password for an account. Subject: Security ID: S-1-5-19 Account Name: LOCAL SERVICE Account Domain: NT AUTHORITY Logon ID: 0x3e5 Additional Information: Caller Workstation: LTRANPHD Target Account Name: Liem Target Account Domain: LTRANPHD
Security	Audit Success	103	2015-04-25 11:09:29	Microsoft-Windows-Eventlog	1100: The event logging service has shut down.
Security	Audit Success	12545	2015-04-25 11:09:29	Microsoft-Windows-Security-Auditing	4647: User initiated logoff: Subject: Security ID: S-1-5-21-1888849264-3803429180-4108621888-1001 Account Name: Liem Account Domain: LTRANPHD Logon ID: 0x1ba7e This event is generated when a logoff is initiated. No further user-initiated activity can occur. This event can be interpreted as a logoff event.
Security	Audit Success	12288	2015-04-25 11:11:56	Microsoft-Windows-Security-Auditing	4608: Windows is starting up. This event is logged when LSASS.EXE starts and the auditing subsystem is initialized.
Security	Audit Success	12544	2015-04-25 11:11:56	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-0-0 Account Name: - Account Domain: - Logon ID: 0x0 Logon Type: 0 Impersonation Level: - New Logon: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Logon ID: 0x3e7 Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x4 Process Name: Network Information: Workstation Name: - Source Network Address: - Source Port: - Detailed Authentication Information: Logon Process: - Authentication Package: - Transited Services: - Package Name (NTLM only): - Key Length: 0 This event is generated when a logon session is created. It is generated on the computer that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service such as the Server service, or a local process such as Winlogon.exe or Services.exe. The logon type field indicates the kind of logon that occurred. The most common types are 2 (interactive) and 3 (network). The New Logon fields indicate the account for whom the new logon was created, i.e. the account that was logged on. The network fields indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impersonation level field indicates the extent to which a process in the logon session can impersonate. The authentication information fields provide detailed information about this specific logon request. - Logon GUID is a unique identifier that can be used to correlate this event with a KDC event. - Transited services indicate which intermediate services have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indicates the length of the generated session key. This will be 0 if no session key was requested.
Security	Audit Success	12544	2015-04-25 11:11:56	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: LTRANPHD$ Account Domain: WORKGROUP Logon ID: 0x3e7 Logon Type: 5 Impersonation Level: %%1833 New Logon: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Logon ID: 0x3e7 Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x240 Process Name: C:\Windows\System32\services.exe Network Information: Workstation Name: Source Network Address: - Source Port: - Detailed Authentication Information: Logon Process: Advapi Authentication Package: Negotiate Transited Services: - Package Name (NTLM only): - Key Length: 0 This event is generated when a logon session is created. It is generated on the computer that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service such as the Server service, or a local process such as Winlogon.exe or Services.exe. The logon type field indicates the kind of logon that occurred. The most common types are 2 (interactive) and 3 (network). The New Logon fields indicate the account for whom the new logon was created, i.e. the account that was logged on. The network fields indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impersonation level field indicates the extent to which a process in the logon session can impersonate. The authentication information fields provide detailed information about this specific logon request. - Logon GUID is a unique identifier that can be used to correlate this event with a KDC event. - Transited services indicate which intermediate services have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indicates the length of the generated session key. This will be 0 if no session key was requested.
Security	Audit Success	12544	2015-04-25 11:11:56	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: LTRANPHD$ Account Domain: WORKGROUP Logon ID: 0x3e7 Logon Type: 5 Impersonation Level: %%1833 New Logon: Security ID: S-1-5-20 Account Name: NETWORK SERVICE Account Domain: NT AUTHORITY Logon ID: 0x3e4 Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x240 Process Name: C:\Windows\System32\services.exe Network Information: Workstation Name: Source Network Address: - Source Port: - Detailed Authentication Information: Logon Process: Advapi Authentication Package: Negotiate Transited Services: - Package Name (NTLM only): - Key Length: 0 This event is generated when a logon session is created. It is generated on the computer that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service such as the Server service, or a local process such as Winlogon.exe or Services.exe. The logon type field indicates the kind of logon that occurred. The most common types are 2 (interactive) and 3 (network). The New Logon fields indicate the account for whom the new logon was created, i.e. the account that was logged on. The network fields indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impersonation level field indicates the extent to which a process in the logon session can impersonate. The authentication information fields provide detailed information about this specific logon request.

					- Logon GUID is a unique identifier that can be used to correlate this event with a KDC event. - Transited services indicate which intermediate services have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indicates the length of the generated session key. This will be 0 if no session key was requested.
Security	Audit Success	12544	2015-04-25 11:11:56	Microsoft-Windows-Security-Auditing	4648: A logon was attempted using explicit credentials. Subject: Security ID: S-1-5-18 Account Name: LTRANPHD$ Account Domain: WORKGROUP Logon ID: 0x3e7 Logon GUID: {00000000-0000-0000-0000-000000000000} Account Whose Credentials Were Used: Account Name: DWM-1 Account Domain: Window Manager Logon GUID: {00000000-0000-0000-0000-000000000000} Target Server: Target Server Name: localhost Additional Information: localhost Process Information: Process ID: 0x210 Process Name: C:\Windows\System32\winlogon.exe Network Information: Network Address: - Port: - This event is generated when a process attempts to log on an account by explicitly specifying that account's credentials. This most commonly occurs in batch-type configurations such as scheduled tasks, or when using the RUNAS command.
Security	Audit Success	12544	2015-04-25 11:11:56	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: LTRANPHD$ Account Domain: WORKGROUP Logon ID: 0x3e7 Logon Type: 2 Impersonation Level: %%1833 New Logon: Security ID: S-1-5-90-1 Account Name: DWM-1 Account Domain: Window Manager Logon ID: 0xc2ef Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x210 Process Name: C:\Windows\System32\winlogon.exe Network Information: Workstation Name: Source Network Address: - Source Port: - Detailed Authentication Information: Logon Process: Advapi Authentication Package: Negotiate Transited Services: - Package Name (NTLM only): - Key Length: 0 This event is generated when a logon session is created. It is generated on the computer that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service such as the Server service, or a local process such as Winlogon.exe or Services.exe. The logon type field indicates the kind of logon that occurred. The most common types are 2 (interactive) and 3 (network). The New Logon fields indicate the account for whom the new logon was created, i.e. the account that was logged on. The network fields indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impersonation level field indicates the extent to which a process in the logon session can impersonate. The authentication information fields provide detailed information about this specific logon request. - Logon GUID is a unique identifier that can be used to correlate this event with a KDC event. - Transited services indicate which intermediate services have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indicates the length of the generated session key. This will be 0 if no session key was requested.
Security	Audit Success	12544	2015-04-25 11:11:56	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: LTRANPHD$ Account Domain: WORKGROUP Logon ID: 0x3e7 Logon Type: 2 Impersonation Level: %%1833 New Logon: Security ID: S-1-5-90-1 Account Name: DWM-1 Account Domain: Window Manager Logon ID: 0xc30f Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x210 Process Name: C:\Windows\System32\winlogon.exe Network Information: Workstation Name: Source Network Address: - Source Port: - Detailed Authentication Information: Logon Process: Advapi Authentication Package: Negotiate Transited Services: - Package Name (NTLM only): - Key Length: 0 This event is generated when a logon session is created. It is generated on the computer that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service such as the Server service, or a local process such as Winlogon.exe or Services.exe. The logon type field indicates the kind of logon that occurred. The most common types are 2 (interactive) and 3 (network). The New Logon fields indicate the account for whom the new logon was created, i.e. the account that was logged on. The network fields indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impersonation level field indicates the extent to which a process in the logon session can impersonate. The authentication information fields provide detailed information about this specific logon request. - Logon GUID is a unique identifier that can be used to correlate this event with a KDC event. - Transited services indicate which intermediate services have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indicates the length of the generated session key. This will be 0 if no session key was requested.
Security	Audit Success	12544	2015-04-25 11:11:56	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: LTRANPHD$ Account Domain: WORKGROUP Logon ID: 0x3e7 Logon Type: 5 Impersonation Level: %%1833 New Logon: Security ID: S-1-5-19 Account Name: LOCAL SERVICE Account Domain: NT AUTHORITY Logon ID: 0x3e5 Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x240 Process Name: C:\Windows\System32\services.exe Network Information: Workstation Name: Source Network Address: - Source Port: - Detailed Authentication Information: Logon Process: Advapi Authentication Package: Negotiate Transited Services: - Package Name (NTLM only): - Key Length: 0 This event is generated when a logon session is created. It is generated on the computer that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service such as the Server service, or a local process such as Winlogon.exe or Services.exe. The logon type field indicates the kind of logon that occurred. The most common types are 2 (interactive) and 3 (network). The New Logon fields indicate the account for whom the new logon was created, i.e. the account that was logged on. The network fields indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impersonation level field indicates the extent to which a process in the logon session can impersonate. The authentication information fields provide detailed information about this specific logon request. - Logon GUID is a unique identifier that can be used to correlate this event with a KDC event. - Transited services indicate which intermediate services have participated in this logon request. - Package name indicates

					which sub-protocol was used among the NTLM protocols. - Key length indicates the length of the generated session key. This will be 0 if no session key was requested.
Security	Audit Success	12544	2015-04-25 11:11:56	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: LTRANPHD$ Account Domain: WORKGROUP Logon ID: 0x3e7 Logon Type: 5 Impersonation Level: %%1833 New Logon: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Logon ID: 0x3e7 Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x240 Process Name: C:\Windows\System32\services.exe Network Information: Workstation Name: Source Network Address: - Source Port: - Detailed Authentication Information: Logon Process: Advapi Authentication Package: Negotiate Transited Services: - Package Name (NTLM only): - Key Length: 0 This event is generated when a logon session is created. It is generated on the computer that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service such as the Server service, or a local process such as Winlogon.exe or Services.exe. The logon type field indicates the kind of logon that occurred. The most common types are 2 (interactive) and 3 (network). The New Logon fields indicate the account for whom the new logon was created, i.e. the account that was logged on. The network fields indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impersonation level field indicates the extent to which a process in the logon session can impersonate. The authentication information fields provide detailed information about this specific logon request. - Logon GUID is a unique identifier that can be used to correlate this event with a KDC event. - Transited services indicate which intermediate services have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indicates the length of the generated session key. This will be 0 if no session key was requested.
Security	Audit Success	12544	2015-04-25 11:11:56	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: LTRANPHD$ Account Domain: WORKGROUP Logon ID: 0x3e7 Logon Type: 5 Impersonation Level: %%1833 New Logon: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Logon ID: 0x3e7 Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x240 Process Name: C:\Windows\System32\services.exe Network Information: Workstation Name: Source Network Address: - Source Port: - Detailed Authentication Information: Logon Process: Advapi Authentication Package: Negotiate Transited Services: - Package Name (NTLM only): - Key Length: 0 This event is generated when a logon session is created. It is generated on the computer that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service such as the Server service, or a local process such as Winlogon.exe or Services.exe. The logon type field indicates the kind of logon that occurred. The most common types are 2 (interactive) and 3 (network). The New Logon fields indicate the account for whom the new logon was created, i.e. the account that was logged on. The network fields indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impersonation level field indicates the extent to which a process in the logon session can impersonate. The authentication information fields provide detailed information about this specific logon request. - Logon GUID is a unique identifier that can be used to correlate this event with a KDC event. - Transited services indicate which intermediate services have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indicates the length of the generated session key. This will be 0 if no session key was requested.
Security	Audit Success	12544	2015-04-25 11:11:56	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: LTRANPHD$ Account Domain: WORKGROUP Logon ID: 0x3e7 Logon Type: 5 Impersonation Level: %%1833 New Logon: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Logon ID: 0x3e7 Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x240 Process Name: C:\Windows\System32\services.exe Network Information: Workstation Name: Source Network Address: - Source Port: - Detailed Authentication Information: Logon Process: Advapi Authentication Package: Negotiate Transited Services: - Package Name (NTLM only): - Key Length: 0 This event is generated when a logon session is created. It is generated on the computer that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service such as the Server service, or a local process such as Winlogon.exe or Services.exe. The logon type field indicates the kind of logon that occurred. The most common types are 2 (interactive) and 3 (network). The New Logon fields indicate the account for whom the new logon was created, i.e. the account that was logged on. The network fields indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impersonation level field indicates the extent to which a process in the logon session can impersonate. The authentication information fields provide detailed information about this specific logon request. - Logon GUID is a unique identifier that can be used to correlate this event with a KDC event. - Transited services indicate which intermediate services have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indicates the length of the generated session key. This will be 0 if no session key was requested.
Security	Audit Success	12548	2015-04-25 11:11:56	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Logon ID: 0x3e7 Privileges: SeAssignPrimaryTokenPrivilege SeTcbPrivilege SeSecurityPrivilege SeTakeOwnershipPrivilege SeLoadDriverPrivilege SeBackupPrivilege SeRestorePrivilege SeDebugPrivilege SeAuditPrivilege SeSystemEnvironmentPrivilege SeImpersonatePrivilege
Security	Audit Success	12548	2015-04-25 11:11:56	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-20 Account Name: NETWORK SERVICE Account Domain: NT AUTHORITY Logon ID: 0x3e4 Privileges: SeAssignPrimaryTokenPrivilege SeAuditPrivilege SeImpersonatePrivilege

Security	Audit Success	12548	2015-04-25 11:11:56		Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-90-1 Account Name: DWM-1 Account Domain: Window Manager Logon ID: 0xc2ef Privileges: SeAssignPrimaryTokenPrivilege SeAuditPrivilege SeImpersonatePrivilege
Security	Audit Success	12548	2015-04-25 11:11:56		Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-90-1 Account Name: DWM-1 Account Domain: Window Manager Logon ID: 0xc30f Privileges: SeAssignPrimaryTokenPrivilege SeAuditPrivilege
Security	Audit Success	12548	2015-04-25 11:11:56		Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-19 Account Name: LOCAL SERVICE Account Domain: NT AUTHORITY Logon ID: 0x3e5 Privileges: SeAssignPrimaryTokenPrivilege SeAuditPrivilege SeImpersonatePrivilege
Security	Audit Success	12548	2015-04-25 11:11:56		Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Logon ID: 0x3e7 Privileges: SeAssignPrimaryTokenPrivilege SeTcbPrivilege SeSecurityPrivilege SeTakeOwnershipPrivilege SeLoadDriverPrivilege SeBackupPrivilege SeRestorePrivilege SeDebugPrivilege SeAuditPrivilege SeSystemEnvironmentPrivilege SeImpersonatePrivilege
Security	Audit Success	12548	2015-04-25 11:11:56		Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Logon ID: 0x3e7 Privileges: SeAssignPrimaryTokenPrivilege SeTcbPrivilege SeSecurityPrivilege SeTakeOwnershipPrivilege SeLoadDriverPrivilege SeBackupPrivilege SeRestorePrivilege SeDebugPrivilege SeAuditPrivilege SeSystemEnvironmentPrivilege SeImpersonatePrivilege
Security	Audit Success	12548	2015-04-25 11:11:56		Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Logon ID: 0x3e7 Privileges: SeAssignPrimaryTokenPrivilege SeTcbPrivilege SeSecurityPrivilege SeTakeOwnershipPrivilege SeLoadDriverPrivilege SeBackupPrivilege SeRestorePrivilege SeDebugPrivilege SeAuditPrivilege SeSystemEnvironmentPrivilege SeImpersonatePrivilege
Security	Audit Success	13568	2015-04-25 11:11:56		Microsoft-Windows-Security-Auditing	4902: The Per-user audit policy table was created. Number of Elements: 0 Policy ID: 0x7467
Security	Audit Success	12292	2015-04-25 11:11:57		Microsoft-Windows-Security-Auditing	5033: The Windows Firewall Driver started successfully.
Security	Audit Success	12292	2015-04-25 11:11:57		Microsoft-Windows-Security-Auditing	5024: The Windows Firewall service started successfully.
Security	Audit Success	12544	2015-04-25 11:11:57		Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: LTRANPHD$ Account Domain: WORKGROUP Logon ID: 0x3e7 Logon Type: 5 Impersonation Level: %%1833 New Logon: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Logon ID: 0x3e7 Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x240 Process Name: C:\Windows\System32\services.exe Network Information: Workstation Name: Source Network Address: - Source Port: - Detailed Authentication Information: Logon Process: Advapi Authentication Package: Negotiate Transited Services: - Package Name (NTLM only): - Key Length: 0 This event is generated when a logon session is created. It is generated on the computer that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service such as the Server service, or a local process such as Winlogon.exe or Services.exe. The logon type field indicates the kind of logon that occurred. The most common types are 2 (interactive) and 3 (network). The New Logon fields indicate the account for whom the new logon was created, i.e. the account that was logged on. The network fields indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impersonation level field indicates the extent to which a process in the logon session can impersonate. The authentication information fields provide detailed information about this specific logon request. - Logon GUID is a unique identifier that can be used to correlate this event with a KDC event. - Transited services indicate which intermediate services have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indicates the length of the generated session key. This will be 0 if no session key was requested.
Security	Audit Success	12544	2015-04-25 11:11:57		Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: LTRANPHD$ Account Domain: WORKGROUP Logon ID: 0x3e7 Logon Type: 5 Impersonation Level: %%1833 New Logon: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Logon ID: 0x3e7 Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x240 Process Name: C:\Windows\System32\services.exe Network Information: Workstation Name: Source Network Address: - Source Port: - Detailed Authentication Information: Logon Process: Advapi Authentication Package: Negotiate Transited Services: - Package Name (NTLM only): - Key Length: 0 This event is generated when a logon session is created. It is generated on the computer that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service such as the Server service, or a local process such as Winlogon.exe or Services.exe. The logon type field indicates the kind of logon that occurred. The most common types are 2 (interactive) and 3 (network). The New Logon fields indicate the account for whom the new logon was created, i.e. the account that was logged on. The network fields indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impersonation level field indicates the extent to which a process in the logon session can impersonate. The authentication information fields provide detailed information about this specific logon request. - Logon GUID is a unique identifier that can be used to correlate this event with a KDC event. - Transited

					services indicate which intermediate services have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indicates the length of the generated session key. This will be 0 if no session key was requested.
Security	Audit Success	12544	2015-04-25 11:11:57	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-0-0 Account Name: - Account Domain: - Logon ID: 0x0 Logon Type: 3 Impersonation Level: %%1833 New Logon: Security ID: S-1-5-7 Account Name: ANONYMOUS LOGON Account Domain: NT AUTHORITY Logon ID: 0x17fb7 Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x0 Process Name: - Network Information: Workstation Name: Source Network Address: - Source Port: - Detailed Authentication Information: Logon Process: NtLmSsp Authentication Package: NTLM Transited Services: - Package Name (NTLM only): NTLM V1 Key Length: 0 This event is generated when a logon session is created. It is generated on the computer that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service such as the Server service, or a local process such as Winlogon.exe or Services.exe. The logon type field indicates the kind of logon that occurred. The most common types are 2 (interactive) and 3 (network). The New Logon fields indicate the account for whom the new logon was created, i.e. the account that was logged on. The network fields indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impersonation level field indicates the extent to which a process in the logon session can impersonate. The authentication information fields provide detailed information about this specific logon request. - Logon GUID is a unique identifier that can be used to correlate this event with a KDC event. - Transited services indicate which intermediate services have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indicates the length of the generated session key. This will be 0 if no session key was requested.
Security	Audit Success	12548	2015-04-25 11:11:57	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Logon ID: 0x3e7 Privileges: SeAssignPrimaryTokenPrivilege SeTcbPrivilege SeSecurityPrivilege SeTakeOwnershipPrivilege SeLoadDriverPrivilege SeBackupPrivilege SeRestorePrivilege SeDebugPrivilege SeAuditPrivilege SeSystemEnvironmentPrivilege SeImpersonatePrivilege
Security	Audit Success	12548	2015-04-25 11:11:57	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Logon ID: 0x3e7 Privileges: SeAssignPrimaryTokenPrivilege SeTcbPrivilege SeSecurityPrivilege SeTakeOwnershipPrivilege SeLoadDriverPrivilege SeBackupPrivilege SeRestorePrivilege SeDebugPrivilege SeAuditPrivilege SeSystemEnvironmentPrivilege SeImpersonatePrivilege
Security	Audit Success	12544	2015-04-25 11:11:59	Microsoft-Windows-Security-Auditing	4648: A logon was attempted using explicit credentials. Subject: Security ID: S-1-5-18 Account Name: LTRANPHD$ Account Domain: WORKGROUP Logon ID: 0x3e7 Logon GUID: {00000000-0000-0000-0000-000000000000} Account Whose Credentials Were Used: Account Name: Liem Account Domain: LTRANPHD Logon GUID: {00000000-0000-0000-0000-000000000000} Target Server: Target Server Name: localhost Additional Information: localhost Process Information: Process ID: 0x210 Process Name: C:\Windows\System32\winlogon.exe Network Information: Network Address: 127.0.0.1 Port: 0 This event is generated when a process attempts to log on an account by explicitly specifying that account's credentials. This most commonly occurs in batch-type configurations such as scheduled tasks, or when using the RUNAS command.
Security	Audit Success	12544	2015-04-25 11:11:59	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: LTRANPHD$ Account Domain: WORKGROUP Logon ID: 0x3e7 Logon Type: 2 Impersonation Level: %%1833 New Logon: Security ID: S-1-5-21-1888849264-3803429180-4108621888-1001 Account Name: Liem Account Domain: LTRANPHD Logon ID: 0x19644 Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x210 Process Name: C:\Windows\System32\winlogon.exe Network Information: Workstation Name: LTRANPHD Source Network Address: 127.0.0.1 Source Port: 0 Detailed Authentication Information: Logon Process: User32 Authentication Package: Negotiate Transited Services: - Package Name (NTLM only): - Key Length: 0 This event is generated when a logon session is created. It is generated on the computer that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service such as the Server service, or a local process such as Winlogon.exe or Services.exe. The logon type field indicates the kind of logon that occurred. The most common types are 2 (interactive) and 3 (network). The New Logon fields indicate the account for whom the new logon was created, i.e. the account that was logged on. The network fields indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impersonation level field indicates the extent to which a process in the logon session can impersonate. The authentication information fields provide detailed information about this specific logon request. - Logon GUID is a unique identifier that can be used to correlate this event with a KDC event. - Transited services indicate which intermediate services have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indicates the length of the generated session key. This will be 0 if no session key was requested.
					4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: LTRANPHD$ Account Domain: WORKGROUP Logon ID: 0x3e7 Logon Type: 2 Impersonation Level: %%1833 New Logon: Security ID: S-1-5-21-1888849264-3803429180-4108621888-1001 Account Name: Liem Account Domain: LTRANPHD Logon ID: 0x19677 Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x210 Process Name: C:\Windows\System32\winlogon.exe Network Information: Workstation Name: LTRANPHD Source Network Address: 127.0.0.1 Source Port: 0 Detailed Authentication Information: Logon Process: User32 Authentication Package: Negotiate Transited Services: - Package Name (NTLM only): - Key Length: 0 This event is generated when a logon session is created. It is generated on the computer that was accessed. The subject fields indicate the account on the local system which requested the logon. This is
	Audit		2015-04-	Microsoft-Windows-Security-	

Security	Success	12544	25 11:11:59	Auditing	most commonly a service such as the Server service, or a local process such as Winlogon.exe or Services.exe. The logon type field indicates the kind of logon that occurred. The most common types are 2 (interactive) and 3 (network). The New Logon fields indicate the account for whom the new logon was created, i.e. the account that was logged on. The network fields indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impersonation level field indicates the extent to which a process in the logon session can impersonate. The authentication information fields provide detailed information about this specific logon request. - Logon GUID is a unique identifier that can be used to correlate this event with a KDC event. - Transited services indicate which intermediate services have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indicates the length of the generated session key. This will be 0 if no session key was requested.
Security	Audit Success	12548	2015-04-25 11:11:59	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-21-1888849264-3803429180-4108621888-1001 Account Name: Liem Account Domain: LTRANPHD Logon ID: 0x19644 Privileges: SeSecurityPrivilege SeTakeOwnershipPrivilege SeLoadDriverPrivilege SeBackupPrivilege SeRestorePrivilege SeDebugPrivilege SeSystemEnvironmentPrivilege SeImpersonatePrivilege
Security	Audit Success	12544	2015-04-25 11:12:00	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: LTRANPHD$ Account Domain: WORKGROUP Logon ID: 0x3e7 Logon Type: 5 Impersonation Level: %%1833 New Logon: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Logon ID: 0x3e7 Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x240 Process Name: C:\Windows\System32\services.exe Network Information: Workstation Name: Source Network Address: - Source Port: - Detailed Authentication Information: Logon Process: Advapi Authentication Package: Negotiate Transited Services: - Package Name (NTLM only): - Key Length: 0 This event is generated when a logon session is created. It is generated on the computer that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service such as the Server service, or a local process such as Winlogon.exe or Services.exe. The logon type field indicates the kind of logon that occurred. The most common types are 2 (interactive) and 3 (network). The New Logon fields indicate the account for whom the new logon was created, i.e. the account that was logged on. The network fields indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impersonation level field indicates the extent to which a process in the logon session can impersonate. The authentication information fields provide detailed information about this specific logon request. - Logon GUID is a unique identifier that can be used to correlate this event with a KDC event. - Transited services indicate which intermediate services have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indicates the length of the generated session key. This will be 0 if no session key was requested.
Security	Audit Success	12548	2015-04-25 11:12:00	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Logon ID: 0x3e7 Privileges: SeAssignPrimaryTokenPrivilege SeTcbPrivilege SeSecurityPrivilege SeTakeOwnershipPrivilege SeLoadDriverPrivilege SeBackupPrivilege SeRestorePrivilege SeDebugPrivilege SeAuditPrivilege SeSystemEnvironmentPrivilege SeImpersonatePrivilege
Security	Audit Success	13824	2015-04-25 11:12:02	Microsoft-Windows-Security-Auditing	4797: An attempt was made to query the existence of a blank password for an account. Subject: Security ID: S-1-5-21-1888849264-3803429180-4108621888-1001 Account Name: Liem Account Domain: LTRANPHD Logon ID: 0x19677 Additional Information: Caller Workstation: LTRANPHD Target Account Name: Administrator Target Account Domain: LTRANPHD
Security	Audit Success	13824	2015-04-25 11:12:02	Microsoft-Windows-Security-Auditing	4797: An attempt was made to query the existence of a blank password for an account. Subject: Security ID: S-1-5-21-1888849264-3803429180-4108621888-1001 Account Name: Liem Account Domain: LTRANPHD Logon ID: 0x19677 Additional Information: Caller Workstation: LTRANPHD Target Account Name: Guest Target Account Domain: LTRANPHD
Security	Audit Success	13824	2015-04-25 11:12:02	Microsoft-Windows-Security-Auditing	4797: An attempt was made to query the existence of a blank password for an account. Subject: Security ID: S-1-5-21-1888849264-3803429180-4108621888-1001 Account Name: Liem Account Domain: LTRANPHD Logon ID: 0x19677 Additional Information: Caller Workstation: LTRANPHD Target Account Name: Administrator Target Account Domain: LTRANPHD
Security	Audit Success	13824	2015-04-25 11:12:02	Microsoft-Windows-Security-Auditing	4797: An attempt was made to query the existence of a blank password for an account. Subject: Security ID: S-1-5-21-1888849264-3803429180-4108621888-1001 Account Name: Liem Account Domain: LTRANPHD Logon ID: 0x19677 Additional Information: Caller Workstation: LTRANPHD Target Account Name: Guest Target Account Domain: LTRANPHD
Security	Audit Success	13824	2015-04-25 11:12:05	Microsoft-Windows-Security-Auditing	4797: An attempt was made to query the existence of a blank password for an account. Subject: Security ID: S-1-5-19 Account Name: LOCAL SERVICE Account Domain: NT AUTHORITY Logon ID: 0x3e5 Additional Information: Caller Workstation: LTRANPHD Target Account Name: Administrator Target Account Domain: LTRANPHD
Security	Audit Success	13824	2015-04-25 11:12:05	Microsoft-Windows-Security-Auditing	4797: An attempt was made to query the existence of a blank password for an account. Subject: Security ID: S-1-5-19 Account Name: LOCAL SERVICE Account Domain: NT AUTHORITY Logon ID: 0x3e5 Additional Information: Caller Workstation: LTRANPHD Target Account Name: Administrator Target Account Domain: LTRANPHD
Security	Audit Success	13824	2015-04-25 11:12:05	Microsoft-Windows-Security-Auditing	4797: An attempt was made to query the existence of a blank password for an account. Subject: Security ID: S-1-5-19 Account Name: LOCAL SERVICE Account Domain: NT AUTHORITY Logon ID: 0x3e5 Additional Information: Caller Workstation: LTRANPHD Target Account Name: Guest Target Account Domain: LTRANPHD
			2015-04-		4797: An attempt was made to query the existence of a blank password for an account. Subject: Security ID:

Security	Audit Success	13824	25 11:12:05	Microsoft-Windows-Security-Auditing	S-1-5-19 Account Name: LOCAL SERVICE Account Domain: NT AUTHORITY Logon ID: 0x3e5 Additional Information: Caller Workstation: LTRANPHD Target Account Name: Guest Target Account Domain: LTRANPHD
Security	Audit Success	13824	2015-04-25 11:12:05	Microsoft-Windows-Security-Auditing	4797: An attempt was made to query the existence of a blank password for an account. Subject: Security ID: S-1-5-19 Account Name: LOCAL SERVICE Account Domain: NT AUTHORITY Logon ID: 0x3e5 Additional Information: Caller Workstation: LTRANPHD Target Account Name: Liem Target Account Domain: LTRANPHD
Security	Audit Success	13824	2015-04-25 11:12:05	Microsoft-Windows-Security-Auditing	4797: An attempt was made to query the existence of a blank password for an account. Subject: Security ID: S-1-5-19 Account Name: LOCAL SERVICE Account Domain: NT AUTHORITY Logon ID: 0x3e5 Additional Information: Caller Workstation: LTRANPHD Target Account Name: Liem Target Account Domain: LTRANPHD
Security	Audit Success	13824	2015-04-25 11:12:05	Microsoft-Windows-Security-Auditing	4797: An attempt was made to query the existence of a blank password for an account. Subject: Security ID: S-1-5-19 Account Name: LOCAL SERVICE Account Domain: NT AUTHORITY Logon ID: 0x3e5 Additional Information: Caller Workstation: LTRANPHD Target Account Name: Liem Target Account Domain: LTRANPHD
Security	Audit Success	13824	2015-04-25 11:12:05	Microsoft-Windows-Security-Auditing	4797: An attempt was made to query the existence of a blank password for an account. Subject: Security ID: S-1-5-19 Account Name: LOCAL SERVICE Account Domain: NT AUTHORITY Logon ID: 0x3e5 Additional Information: Caller Workstation: LTRANPHD Target Account Name: Liem Target Account Domain: LTRANPHD
Security	Audit Success	12545	2015-04-25 11:12:10	Microsoft-Windows-Security-Auditing	4647: User initiated logoff: Subject: Security ID: S-1-5-21-1888849264-3803429180-4108621888-1001 Account Name: Liem Account Domain: LTRANPHD Logon ID: 0x19677 This event is generated when a logoff is initiated. No further user-initiated activity can occur. This event can be interpreted as a logoff event.
Security	Audit Success	103	2015-04-25 11:12:11	Microsoft-Windows-Eventlog	1100: The event logging service has shut down.
Security	Audit Success	12288	2015-04-25 11:12:22	Microsoft-Windows-Security-Auditing	4608: Windows is starting up. This event is logged when LSASS.EXE starts and the auditing subsystem is initialized.
Security	Audit Success	12292	2015-04-25 11:12:22	Microsoft-Windows-Security-Auditing	5033: The Windows Firewall Driver started successfully.
Security	Audit Success	12544	2015-04-25 11:12:22	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-0-0 Account Name: - Account Domain: - Logon ID: 0x0 Logon Type: 0 Impersonation Level: - New Logon: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Logon ID: 0x3e7 Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x4 Process Name: Network Information: Workstation Name: - Source Network Address: - Source Port: - Detailed Authentication Information: Logon Process: - Authentication Package: - Transited Services: - Package Name (NTLM only): - Key Length: 0 This event is generated when a logon session is created. It is generated on the computer that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service such as the Server service, or a local process such as Winlogon.exe or Services.exe. The logon type field indicates the kind of logon that occurred. The most common types are 2 (interactive) and 3 (network). The New Logon fields indicate the account for whom the new logon was created, i.e. the account that was logged on. The network fields indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impersonation level field indicates the extent to which a process in the logon session can impersonate. The authentication information fields provide detailed information about this specific logon request. - Logon GUID is a unique identifier that can be used to correlate this event with a KDC event. - Transited services indicate which intermediate services have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indicates the length of the generated session key. This will be 0 if no session key was requested.
Security	Audit Success	12544	2015-04-25 11:12:22	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: LTRANPHD$ Account Domain: WORKGROUP Logon ID: 0x3e7 Logon Type: 5 Impersonation Level: %%1833 New Logon: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Logon ID: 0x3e7 Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x240 Process Name: C:\Windows\System32\services.exe Network Information: Workstation Name: Source Network Address: - Source Port: - Detailed Authentication Information: Logon Process: Advapi Authentication Package: Negotiate Transited Services: - Package Name (NTLM only): - Key Length: 0 This event is generated when a logon session is created. It is generated on the computer that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service such as the Server service, or a local process such as Winlogon.exe or Services.exe. The logon type field indicates the kind of logon that occurred. The most common types are 2 (interactive) and 3 (network). The New Logon fields indicate the account for whom the new logon was created, i.e. the account that was logged on. The network fields indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impersonation level field indicates the extent to which a process in the logon session can impersonate. The authentication information fields provide detailed information about this specific logon request. - Logon GUID is a unique identifier that can be used to correlate this event with a KDC event. - Transited services indicate which intermediate services have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indicates the length of the generated session key. This will be 0 if no session key was requested.
					4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: LTRANPHD$

Security	Audit Success	12544	2015-04-25 11:12:22	Microsoft-Windows-Security-Auditing	Account Domain: WORKGROUP Logon ID: 0x3e7 Logon Type: 5 Impersonation Level: %%1833 New Logon: Security ID: S-1-5-20 Account Name: NETWORK SERVICE Account Domain: NT AUTHORITY Logon ID: 0x3e4 Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x240 Process Name: C:\Windows\System32\services.exe Network Information: Workstation Name: Source Network Address: - Source Port: - Detailed Authentication Information: Logon Process: Advapi Authentication Package: Negotiate Transited Services: - Package Name (NTLM only): - Key Length: 0 This event is generated when a logon session is created. It is generated on the computer that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service such as the Server service, or a local process such as Winlogon.exe or Services.exe. The logon type field indicates the kind of logon that occurred. The most common types are 2 (interactive) and 3 (network). The New Logon fields indicate the account for whom the new logon was created, i.e. the account that was logged on. The network fields indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impersonation level field indicates the extent to which a process in the logon session can impersonate. The authentication information fields provide detailed information about this specific logon request. - Logon GUID is a unique identifier that can be used to correlate this event with a KDC event. - Transited services indicate which intermediate services have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indicates the length of the generated session key. This will be 0 if no session key was requested.
Security	Audit Success	12544	2015-04-25 11:12:22	Microsoft-Windows-Security-Auditing	4648: A logon was attempted using explicit credentials. Subject: Security ID: S-1-5-18 Account Name: LTRANPHD$ Account Domain: WORKGROUP Logon ID: 0x3e7 Logon GUID: {00000000-0000-0000-0000-000000000000} Account Whose Credentials Were Used: Account Name: DWM-1 Account Domain: Window Manager Logon GUID: {00000000-0000-0000-0000-000000000000} Target Server: Target Server Name: localhost Additional Information: localhost Process Information: Process ID: 0x210 Process Name: C:\Windows\System32\winlogon.exe Network Information: Network Address: - Port: - This event is generated when a process attempts to log on an account by explicitly specifying that account's credentials. This most commonly occurs in batch-type configurations such as scheduled tasks, or when using the RUNAS command.
Security	Audit Success	12544	2015-04-25 11:12:22	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: LTRANPHD$ Account Domain: WORKGROUP Logon ID: 0x3e7 Logon Type: 2 Impersonation Level: %%1833 New Logon: Security ID: S-1-5-90-1 Account Name: DWM-1 Account Domain: Window Manager Logon ID: 0xc2f8 Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x210 Process Name: C:\Windows\System32\winlogon.exe Network Information: Workstation Name: Source Network Address: - Source Port: - Detailed Authentication Information: Logon Process: Advapi Authentication Package: Negotiate Transited Services: - Package Name (NTLM only): - Key Length: 0 This event is generated when a logon session is created. It is generated on the computer that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service such as the Server service, or a local process such as Winlogon.exe or Services.exe. The logon type field indicates the kind of logon that occurred. The most common types are 2 (interactive) and 3 (network). The New Logon fields indicate the account for whom the new logon was created, i.e. the account that was logged on. The network fields indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impersonation level field indicates the extent to which a process in the logon session can impersonate. The authentication information fields provide detailed information about this specific logon request. - Logon GUID is a unique identifier that can be used to correlate this event with a KDC event. - Transited services indicate which intermediate services have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indicates the length of the generated session key. This will be 0 if no session key was requested.
Security	Audit Success	12544	2015-04-25 11:12:22	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: LTRANPHD$ Account Domain: WORKGROUP Logon ID: 0x3e7 Logon Type: 2 Impersonation Level: %%1833 New Logon: Security ID: S-1-5-90-1 Account Name: DWM-1 Account Domain: Window Manager Logon ID: 0xc316 Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x210 Process Name: C:\Windows\System32\winlogon.exe Network Information: Workstation Name: Source Network Address: - Source Port: - Detailed Authentication Information: Logon Process: Advapi Authentication Package: Negotiate Transited Services: - Package Name (NTLM only): - Key Length: 0 This event is generated when a logon session is created. It is generated on the computer that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service such as the Server service, or a local process such as Winlogon.exe or Services.exe. The logon type field indicates the kind of logon that occurred. The most common types are 2 (interactive) and 3 (network). The New Logon fields indicate the account for whom the new logon was created, i.e. the account that was logged on. The network fields indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impersonation level field indicates the extent to which a process in the logon session can impersonate. The authentication information fields provide detailed information about this specific logon request. - Logon GUID is a unique identifier that can be used to correlate this event with a KDC event. - Transited services indicate which intermediate services have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indicates the length of the generated session key. This will be 0 if no session key was requested.
					4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: LTRANPHD$ Account Domain: WORKGROUP Logon ID: 0x3e7 Logon Type: 5 Impersonation Level: %%1833 New Logon: Security ID: S-1-5-19 Account Name: LOCAL SERVICE Account Domain: NT AUTHORITY Logon ID: 0x3e5 Logon

						GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x240 Process Name: C:\Windows\System32\services.exe Network Information: Workstation Name: Source Network Address: - Source Port: - Detailed Authentication Information: Logon Process: Advapi Authentication Package: Negotiate Transited Services: - Package Name (NTLM only): - Key Length: 0 This event is generated when a logon session is created. It is generated on the computer that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service such as the Server service, or a local process such as Winlogon.exe or Services.exe. The logon type field indicates the kind of logon that occurred. The most common types are 2 (interactive) and 3 (network). The New Logon fields indicate the account for whom the new logon was created, i.e. the account that was logged on. The network fields indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impersonation level field indicates the extent to which a process in the logon session can impersonate. The authentication information fields provide detailed information about this specific logon request. - Logon GUID is a unique identifier that can be used to correlate this event with a KDC event. - Transited services indicate which intermediate services have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indicates the length of the generated session key. This will be 0 if no session key was requested.
Security	Audit Success	12544	2015-04-25 11:12:22		Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: LTRANPHD$ Account Domain: WORKGROUP Logon ID: 0x3e7 Logon Type: 5 Impersonation Level: %%1833 New Logon: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Logon ID: 0x3e7 Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x240 Process Name: C:\Windows\System32\services.exe Network Information: Workstation Name: Source Network Address: - Source Port: - Detailed Authentication Information: Logon Process: Advapi Authentication Package: Negotiate Transited Services: - Package Name (NTLM only): - Key Length: 0 This event is generated when a logon session is created. It is generated on the computer that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service such as the Server service, or a local process such as Winlogon.exe or Services.exe. The logon type field indicates the kind of logon that occurred. The most common types are 2 (interactive) and 3 (network). The New Logon fields indicate the account for whom the new logon was created, i.e. the account that was logged on. The network fields indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impersonation level field indicates the extent to which a process in the logon session can impersonate. The authentication information fields provide detailed information about this specific logon request. - Logon GUID is a unique identifier that can be used to correlate this event with a KDC event. - Transited services indicate which intermediate services have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indicates the length of the generated session key. This will be 0 if no session key was requested.
Security	Audit Success	12544	2015-04-25 11:12:22		Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: LTRANPHD$ Account Domain: WORKGROUP Logon ID: 0x3e7 Logon Type: 5 Impersonation Level: %%1833 New Logon: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Logon ID: 0x3e7 Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x240 Process Name: C:\Windows\System32\services.exe Network Information: Workstation Name: Source Network Address: - Source Port: - Detailed Authentication Information: Logon Process: Advapi Authentication Package: Negotiate Transited Services: - Package Name (NTLM only): - Key Length: 0 This event is generated when a logon session is created. It is generated on the computer that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service such as the Server service, or a local process such as Winlogon.exe or Services.exe. The logon type field indicates the kind of logon that occurred. The most common types are 2 (interactive) and 3 (network). The New Logon fields indicate the account for whom the new logon was created, i.e. the account that was logged on. The network fields indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impersonation level field indicates the extent to which a process in the logon session can impersonate. The authentication information fields provide detailed information about this specific logon request. - Logon GUID is a unique identifier that can be used to correlate this event with a KDC event. - Transited services indicate which intermediate services have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indicates the length of the generated session key. This will be 0 if no session key was requested.
Security	Audit Success	12544	2015-04-25 11:12:22		Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: LTRANPHD$ Account Domain: WORKGROUP Logon ID: 0x3e7 Logon Type: 5 Impersonation Level: %%1833 New Logon: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Logon ID: 0x3e7 Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x240 Process Name: C:\Windows\System32\services.exe Network Information: Workstation Name: Source Network Address: - Source Port: - Detailed Authentication Information: Logon Process: Advapi Authentication Package: Negotiate Transited Services: - Package Name (NTLM only): - Key Length: 0 This event is generated when a logon session is created. It is generated on the computer that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service such as the Server service, or a local process such as Winlogon.exe or Services.exe. The logon type field indicates the kind of logon that occurred. The most common types are 2 (interactive) and 3 (network). The New Logon fields indicate the account for whom the new logon was created, i.e. the account that was logged on. The network fields indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some

					cases. The impersonation level field indicates the extent to which a process in the logon session can impersonate. The authentication information fields provide detailed information about this specific logon request. - Logon GUID is a unique identifier that can be used to correlate this event with a KDC event. - Transited services indicate which intermediate services have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indicates the length of the generated session key. This will be 0 if no session key was requested.
Security	Audit Success	12548	2015-04-25 11:12:22	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Logon ID: 0x3e7 Privileges: SeAssignPrimaryTokenPrivilege SeTcbPrivilege SeSecurityPrivilege SeTakeOwnershipPrivilege SeLoadDriverPrivilege SeBackupPrivilege SeRestorePrivilege SeDebugPrivilege SeAuditPrivilege SeSystemEnvironmentPrivilege SeImpersonatePrivilege
Security	Audit Success	12548	2015-04-25 11:12:22	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-20 Account Name: NETWORK SERVICE Account Domain: NT AUTHORITY Logon ID: 0x3e4 Privileges: SeAssignPrimaryTokenPrivilege SeAuditPrivilege SeImpersonatePrivilege
Security	Audit Success	12548	2015-04-25 11:12:22	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-90-1 Account Name: DWM-1 Account Domain: Window Manager Logon ID: 0xc2f8 Privileges: SeAssignPrimaryTokenPrivilege SeAuditPrivilege SeImpersonatePrivilege
Security	Audit Success	12548	2015-04-25 11:12:22	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-90-1 Account Name: DWM-1 Account Domain: Window Manager Logon ID: 0xc316 Privileges: SeAssignPrimaryTokenPrivilege SeAuditPrivilege
Security	Audit Success	12548	2015-04-25 11:12:22	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-19 Account Name: LOCAL SERVICE Account Domain: NT AUTHORITY Logon ID: 0x3e5 Privileges: SeAssignPrimaryTokenPrivilege SeAuditPrivilege SeImpersonatePrivilege
Security	Audit Success	12548	2015-04-25 11:12:22	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Logon ID: 0x3e7 Privileges: SeAssignPrimaryTokenPrivilege SeTcbPrivilege SeSecurityPrivilege SeTakeOwnershipPrivilege SeLoadDriverPrivilege SeBackupPrivilege SeRestorePrivilege SeDebugPrivilege SeAuditPrivilege SeSystemEnvironmentPrivilege SeImpersonatePrivilege
Security	Audit Success	12548	2015-04-25 11:12:22	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Logon ID: 0x3e7 Privileges: SeAssignPrimaryTokenPrivilege SeTcbPrivilege SeSecurityPrivilege SeTakeOwnershipPrivilege SeLoadDriverPrivilege SeBackupPrivilege SeRestorePrivilege SeDebugPrivilege SeAuditPrivilege SeSystemEnvironmentPrivilege SeImpersonatePrivilege
Security	Audit Success	12548	2015-04-25 11:12:22	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Logon ID: 0x3e7 Privileges: SeAssignPrimaryTokenPrivilege SeTcbPrivilege SeSecurityPrivilege SeTakeOwnershipPrivilege SeLoadDriverPrivilege SeBackupPrivilege SeRestorePrivilege SeDebugPrivilege SeAuditPrivilege SeSystemEnvironmentPrivilege SeImpersonatePrivilege
Security	Audit Success	13568	2015-04-25 11:12:22	Microsoft-Windows-Security-Auditing	4902: The Per-user audit policy table was created. Number of Elements: 0 Policy ID: 0x73ff
Security	Audit Success	12292	2015-04-25 11:12:23	Microsoft-Windows-Security-Auditing	5024: The Windows Firewall service started successfully.
Security	Audit Success	12544	2015-04-25 11:12:23	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: LTRANPHD$ Account Domain: WORKGROUP Logon ID: 0x3e7 Logon Type: 5 Impersonation Level: %%1833 New Logon: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Logon ID: 0x3e7 Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x240 Process Name: C:\Windows\System32\services.exe Network Information: Workstation Name: Source Network Address: - Source Port: - Detailed Authentication Information: Logon Process: Advapi Authentication Package: Negotiate Transited Services: - Package Name (NTLM only): - Key Length: 0 This event is generated when a logon session is created. It is generated on the computer that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service such as the Server service, or a local process such as Winlogon.exe or Services.exe. The logon type field indicates the kind of logon that occurred. The most common types are 2 (interactive) and 3 (network). The New Logon fields indicate the account for whom the new logon was created, i.e. the account that was logged on. The network fields indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impersonation level field indicates the extent to which a process in the logon session can impersonate. The authentication information fields provide detailed information about this specific logon request. - Logon GUID is a unique identifier that can be used to correlate this event with a KDC event. - Transited services indicate which intermediate services have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indicates the length of the generated session key. This will be 0 if no session key was requested.
					4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: LTRANPHD$ Account Domain: WORKGROUP Logon ID: 0x3e7 Logon Type: 5 Impersonation Level: %%1833 New Logon: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Logon ID: 0x3e7 Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x240 Process Name: C:\Windows\System32\services.exe Network Information: Workstation Name: Source Network Address: - Source Port: - Detailed Authentication Information: Logon Process: Advapi Authentication Package: Negotiate Transited

Security	Audit Success	12544	2015-04-25 11:12:23	Microsoft-Windows-Security-Auditing	Services: - Package Name (NTLM only): - Key Length: 0 This event is generated when a logon session is created. It is generated on the computer that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service such as the Server service, or a local process such as Winlogon.exe or Services.exe. The logon type field indicates the kind of logon that occurred. The most common types are 2 (interactive) and 3 (network). The New Logon fields indicate the account for whom the new logon was created, i.e. the account that was logged on. The network fields indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impersonation level field indicates the extent to which a process in the logon session can impersonate. The authentication information fields provide detailed information about this specific logon request. - Logon GUID is a unique identifier that can be used to correlate this event with a KDC event. - Transited services indicate which intermediate services have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indicates the length of the generated session key. This will be 0 if no session key was requested.
Security	Audit Success	12544	2015-04-25 11:12:23	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-0-0 Account Name: - Account Domain: - Logon ID: 0x0 Logon Type: 3 Impersonation Level: %%1833 New Logon: Security ID: S-1-5-7 Account Name: ANONYMOUS LOGON Account Domain: NT AUTHORITY Logon ID: 0x15e9c Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x0 Process Name: - Network Information: Workstation Name: Source Network Address: - Source Port: - Detailed Authentication Information: Logon Process: NtLmSsp Authentication Package: NTLM Transited Services: - Package Name (NTLM only): NTLM V1 Key Length: 0 This event is generated when a logon session is created. It is generated on the computer that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service such as the Server service, or a local process such as Winlogon.exe or Services.exe. The logon type field indicates the kind of logon that occurred. The most common types are 2 (interactive) and 3 (network). The New Logon fields indicate the account for whom the new logon was created, i.e. the account that was logged on. The network fields indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impersonation level field indicates the extent to which a process in the logon session can impersonate. The authentication information fields provide detailed information about this specific logon request. - Logon GUID is a unique identifier that can be used to correlate this event with a KDC event. - Transited services indicate which intermediate services have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indicates the length of the generated session key. This will be 0 if no session key was requested.
Security	Audit Success	12548	2015-04-25 11:12:23	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Logon ID: 0x3e7 Privileges: SeAssignPrimaryTokenPrivilege SeTcbPrivilege SeSecurityPrivilege SeTakeOwnershipPrivilege SeLoadDriverPrivilege SeBackupPrivilege SeRestorePrivilege SeDebugPrivilege SeAuditPrivilege SeSystemEnvironmentPrivilege SeImpersonatePrivilege
Security	Audit Success	12548	2015-04-25 11:12:23	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Logon ID: 0x3e7 Privileges: SeAssignPrimaryTokenPrivilege SeTcbPrivilege SeSecurityPrivilege SeTakeOwnershipPrivilege SeLoadDriverPrivilege SeBackupPrivilege SeRestorePrivilege SeDebugPrivilege SeAuditPrivilege SeSystemEnvironmentPrivilege SeImpersonatePrivilege
Security	Audit Success	12544	2015-04-25 11:12:25	Microsoft-Windows-Security-Auditing	4648: A logon was attempted using explicit credentials. Subject: Security ID: S-1-5-18 Account Name: LTRANPHD$ Account Domain: WORKGROUP Logon ID: 0x3e7 Logon GUID: {00000000-0000-0000-0000-000000000000} Account Whose Credentials Were Used: Account Name: Liem Account Domain: LTRANPHD Logon GUID: {00000000-0000-0000-0000-000000000000} Target Server: Target Server Name: localhost Additional Information: localhost Process Information: Process ID: 0x210 Process Name: C:\Windows\System32\winlogon.exe Network Information: Network Address: 127.0.0.1 Port: 0 This event is generated when a process attempts to log on an account by explicitly specifying that account's credentials. This most commonly occurs in batch-type configurations such as scheduled tasks, or when using the RUNAS command.
Security	Audit Success	12544	2015-04-25 11:12:25	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: LTRANPHD$ Account Domain: WORKGROUP Logon ID: 0x3e7 Logon Type: 2 Impersonation Level: %%1833 New Logon: Security ID: S-1-5-21-1888849264-3803429180-4108621888-1001 Account Name: Liem Account Domain: LTRANPHD Logon ID: 0x1a2ae Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x210 Process Name: C:\Windows\System32\winlogon.exe Network Information: Workstation Name: LTRANPHD Source Network Address: 127.0.0.1 Source Port: 0 Detailed Authentication Information: Logon Process: User32 Authentication Package: Negotiate Transited Services: - Package Name (NTLM only): - Key Length: 0 This event is generated when a logon session is created. It is generated on the computer that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service such as the Server service, or a local process such as Winlogon.exe or Services.exe. The logon type field indicates the kind of logon that occurred. The most common types are 2 (interactive) and 3 (network). The New Logon fields indicate the account for whom the new logon was created, i.e. the account that was logged on. The network fields indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impersonation level field indicates the extent to which a process in the logon session can impersonate. The authentication information fields provide detailed information about this specific logon request. - Logon GUID is a unique identifier that can be used to correlate this event with a KDC event. - Transited services indicate which intermediate services have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length

					indicates the length of the generated session key. This will be 0 if no session key was requested.
Security	Audit Success	12544	2015-04-25 11:12:25	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: LTRANPHD$ Account Domain: WORKGROUP Logon ID: 0x3e7 Logon Type: 2 Impersonation Level: %%1833 New Logon: Security ID: S-1-5-21-1888849264-3803429180-4108621888-1001 Account Name: Liem Account Domain: LTRANPHD Logon ID: 0x1a2df Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x210 Process Name: C:\Windows\System32\winlogon.exe Network Information: Workstation Name: LTRANPHD Source Network Address: 127.0.0.1 Source Port: 0 Detailed Authentication Information: Logon Process: User32 Authentication Package: Negotiate Transited Services: - Package Name (NTLM only): - Key Length: 0 This event is generated when a logon session is created. It is generated on the computer that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service such as the Server service, or a local process such as Winlogon.exe or Services.exe. The logon type field indicates the kind of logon that occurred. The most common types are 2 (interactive) and 3 (network). The New Logon fields indicate the account for whom the new logon was created, i.e. the account that was logged on. The network fields indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impersonation level field indicates the extent to which a process in the logon session can impersonate. The authentication information fields provide detailed information about this specific logon request. - Logon GUID is a unique identifier that can be used to correlate this event with a KDC event. - Transited services indicate which intermediate services have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indicates the length of the generated session key. This will be 0 if no session key was requested.
Security	Audit Success	12548	2015-04-25 11:12:25	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-21-1888849264-3803429180-4108621888-1001 Account Name: Liem Account Domain: LTRANPHD Logon ID: 0x1a2ae Privileges: SeSecurityPrivilege SeTakeOwnershipPrivilege SeLoadDriverPrivilege SeBackupPrivilege SeRestorePrivilege SeDebugPrivilege SeSystemEnvironmentPrivilege SeImpersonatePrivilege
Security	Audit Success	12544	2015-04-25 11:12:26	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: LTRANPHD$ Account Domain: WORKGROUP Logon ID: 0x3e7 Logon Type: 5 Impersonation Level: %%1833 New Logon: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Logon ID: 0x3e7 Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x240 Process Name: C:\Windows\System32\services.exe Network Information: Workstation Name: Source Network Address: - Source Port: - Detailed Authentication Information: Logon Process: Advapi Authentication Package: Negotiate Transited Services: - Package Name (NTLM only): - Key Length: 0 This event is generated when a logon session is created. It is generated on the computer that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service such as the Server service, or a local process such as Winlogon.exe or Services.exe. The logon type field indicates the kind of logon that occurred. The most common types are 2 (interactive) and 3 (network). The New Logon fields indicate the account for whom the new logon was created, i.e. the account that was logged on. The network fields indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impersonation level field indicates the extent to which a process in the logon session can impersonate. The authentication information fields provide detailed information about this specific logon request. - Logon GUID is a unique identifier that can be used to correlate this event with a KDC event. - Transited services indicate which intermediate services have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indicates the length of the generated session key. This will be 0 if no session key was requested.
Security	Audit Success	12548	2015-04-25 11:12:26	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Logon ID: 0x3e7 Privileges: SeAssignPrimaryTokenPrivilege SeTcbPrivilege SeSecurityPrivilege SeTakeOwnershipPrivilege SeLoadDriverPrivilege SeBackupPrivilege SeRestorePrivilege SeDebugPrivilege SeAuditPrivilege SeSystemEnvironmentPrivilege SeImpersonatePrivilege
Security	Audit Success	13824	2015-04-25 11:12:28	Microsoft-Windows-Security-Auditing	4797: An attempt was made to query the existence of a blank password for an account. Subject: Security ID: S-1-5-21-1888849264-3803429180-4108621888-1001 Account Name: Liem Account Domain: LTRANPHD Logon ID: 0x1a2df Additional Information: Caller Workstation: LTRANPHD Target Account Name: Administrator Target Account Domain: LTRANPHD
Security	Audit Success	13824	2015-04-25 11:12:28	Microsoft-Windows-Security-Auditing	4797: An attempt was made to query the existence of a blank password for an account. Subject: Security ID: S-1-5-21-1888849264-3803429180-4108621888-1001 Account Name: Liem Account Domain: LTRANPHD Logon ID: 0x1a2df Additional Information: Caller Workstation: LTRANPHD Target Account Name: Guest Target Account Domain: LTRANPHD
Security	Audit Success	13824	2015-04-25 11:12:28	Microsoft-Windows-Security-Auditing	4797: An attempt was made to query the existence of a blank password for an account. Subject: Security ID: S-1-5-21-1888849264-3803429180-4108621888-1001 Account Name: Liem Account Domain: LTRANPHD Logon ID: 0x1a2df Additional Information: Caller Workstation: LTRANPHD Target Account Name: Administrator Target Account Domain: LTRANPHD
Security	Audit Success	13824	2015-04-25 11:12:28	Microsoft-Windows-Security-Auditing	4797: An attempt was made to query the existence of a blank password for an account. Subject: Security ID: S-1-5-21-1888849264-3803429180-4108621888-1001 Account Name: Liem Account Domain: LTRANPHD Logon ID: 0x1a2df Additional Information: Caller Workstation: LTRANPHD Target Account Name: Guest Target Account Domain: LTRANPHD
Security	Audit	13824	2015-04-25	Microsoft-Windows-Security-	4797: An attempt was made to query the existence of a blank password for an account. Subject: Security ID: S-1-5-19 Account Name: LOCAL SERVICE Account Domain: NT AUTHORITY Logon ID: 0x3e5 Additional

	Success		11:12:30	Auditing	Information: Caller Workstation: LTRANPHD Target Account Name: Administrator Target Account Domain: LTRANPHD
Security	Audit Success	13824	2015-04-25 11:12:30	Microsoft-Windows-Security-Auditing	4797: An attempt was made to query the existence of a blank password for an account. Subject: Security ID: S-1-5-19 Account Name: LOCAL SERVICE Account Domain: NT AUTHORITY Logon ID: 0x3e5 Additional Information: Caller Workstation: LTRANPHD Target Account Name: Administrator Target Account Domain: LTRANPHD
Security	Audit Success	13824	2015-04-25 11:12:30	Microsoft-Windows-Security-Auditing	4797: An attempt was made to query the existence of a blank password for an account. Subject: Security ID: S-1-5-19 Account Name: LOCAL SERVICE Account Domain: NT AUTHORITY Logon ID: 0x3e5 Additional Information: Caller Workstation: LTRANPHD Target Account Name: Guest Target Account Domain: LTRANPHD
Security	Audit Success	13824	2015-04-25 11:12:30	Microsoft-Windows-Security-Auditing	4797: An attempt was made to query the existence of a blank password for an account. Subject: Security ID: S-1-5-19 Account Name: LOCAL SERVICE Account Domain: NT AUTHORITY Logon ID: 0x3e5 Additional Information: Caller Workstation: LTRANPHD Target Account Name: Guest Target Account Domain: LTRANPHD
Security	Audit Success	13824	2015-04-25 11:12:30	Microsoft-Windows-Security-Auditing	4797: An attempt was made to query the existence of a blank password for an account. Subject: Security ID: S-1-5-19 Account Name: LOCAL SERVICE Account Domain: NT AUTHORITY Logon ID: 0x3e5 Additional Information: Caller Workstation: LTRANPHD Target Account Name: Liem Target Account Domain: LTRANPHD
Security	Audit Success	13824	2015-04-25 11:12:30	Microsoft-Windows-Security-Auditing	4797: An attempt was made to query the existence of a blank password for an account. Subject: Security ID: S-1-5-19 Account Name: LOCAL SERVICE Account Domain: NT AUTHORITY Logon ID: 0x3e5 Additional Information: Caller Workstation: LTRANPHD Target Account Name: Liem Target Account Domain: LTRANPHD
Security	Audit Success	13824	2015-04-25 11:12:30	Microsoft-Windows-Security-Auditing	4797: An attempt was made to query the existence of a blank password for an account. Subject: Security ID: S-1-5-19 Account Name: LOCAL SERVICE Account Domain: NT AUTHORITY Logon ID: 0x3e5 Additional Information: Caller Workstation: LTRANPHD Target Account Name: Liem Target Account Domain: LTRANPHD
Security	Audit Success	13824	2015-04-25 11:12:30	Microsoft-Windows-Security-Auditing	4797: An attempt was made to query the existence of a blank password for an account. Subject: Security ID: S-1-5-19 Account Name: LOCAL SERVICE Account Domain: NT AUTHORITY Logon ID: 0x3e5 Additional Information: Caller Workstation: LTRANPHD Target Account Name: Liem Target Account Domain: LTRANPHD
Security	Audit Success	12544	2015-04-25 11:31:28	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: LTRANPHD$ Account Domain: WORKGROUP Logon ID: 0x3e7 Logon Type: 5 Impersonation Level: %%1833 New Logon: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Logon ID: 0x3e7 Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x240 Process Name: C:\Windows\System32\services.exe Network Information: Workstation Name: Source Network Address: - Source Port: - Detailed Authentication Information: Logon Process: Advapi Authentication Package: Negotiate Transited Services: - Package Name (NTLM only): - Key Length: 0 This event is generated when a logon session is created. It is generated on the computer that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service such as the Server service, or a local process such as Winlogon.exe or Services.exe. The logon type field indicates the kind of logon that occurred. The most common types are 2 (interactive) and 3 (network). The New Logon fields indicate the account for whom the new logon was created, i.e. the account that was logged on. The network fields indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impersonation level field indicates the extent to which a process in the logon session can impersonate. The authentication information fields provide detailed information about this specific logon request. - Logon GUID is a unique identifier that can be used to correlate this event with a KDC event. - Transited services indicate which intermediate services have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indicates the length of the generated session key. This will be 0 if no session key was requested.
Security	Audit Success	12548	2015-04-25 11:31:28	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Logon ID: 0x3e7 Privileges: SeAssignPrimaryTokenPrivilege SeTcbPrivilege SeSecurityPrivilege SeTakeOwnershipPrivilege SeLoadDriverPrivilege SeBackupPrivilege SeRestorePrivilege SeDebugPrivilege SeAuditPrivilege SeSystemEnvironmentPrivilege SeImpersonatePrivilege
Security	Audit Success	12288	2015-04-25 15:32:49	Microsoft-Windows-Security-Auditing	4608: Windows is starting up. This event is logged when LSASS.EXE starts and the auditing subsystem is initialized.
Security	Audit Success	12544	2015-04-25 15:32:49	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-0-0 Account Name: - Account Domain: - Logon ID: 0x0 Logon Type: 0 Impersonation Level: - New Logon: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Logon ID: 0x3e7 Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x4 Process Name: Network Information: Workstation Name: - Source Network Address: - Source Port: - Detailed Authentication Information: Logon Process: - Authentication Package: - Transited Services: - Package Name (NTLM only): - Key Length: 0 This event is generated when a logon session is created. It is generated on the computer that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service such as the Server service, or a local process such as Winlogon.exe or Services.exe. The logon type field indicates the kind of logon that occurred. The most common types are 2 (interactive) and 3 (network). The New Logon fields indicate the account for whom the new logon was created, i.e. the account that was logged on. The network fields indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impersonation level field indicates the extent to which a process in the logon session can impersonate. The authentication information fields provide detailed information about this specific logon request. - Logon GUID is a unique identifier that can be used to correlate this event

					with a KDC event. - Transited services indicate which intermediate services have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indicates the length of the generated session key. This will be 0 if no session key was requested.
Security	Audit Success	12544	2015-04-25 15:32:49	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: LTRANPHD$ Account Domain: WORKGROUP Logon ID: 0x3e7 Logon Type: 5 Impersonation Level: %%1833 New Logon: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Logon ID: 0x3e7 Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x234 Process Name: C:\Windows\System32\services.exe Network Information: Workstation Name: Source Network Address: - Source Port: - Detailed Authentication Information: Logon Process: Advapi Authentication Package: Negotiate Transited Services: - Package Name (NTLM only): - Key Length: 0 This event is generated when a logon session is created. It is generated on the computer that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service such as the Server service, or a local process such as Winlogon.exe or Services.exe. The logon type field indicates the kind of logon that occurred. The most common types are 2 (interactive) and 3 (network). The New Logon fields indicate the account for whom the new logon was created, i.e. the account that was logged on. The network fields indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impersonation level field indicates the extent to which a process in the logon session can impersonate. The authentication information fields provide detailed information about this specific logon request. - Logon GUID is a unique identifier that can be used to correlate this event with a KDC event. - Transited services indicate which intermediate services have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indicates the length of the generated session key. This will be 0 if no session key was requested.
Security	Audit Success	12544	2015-04-25 15:32:49	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: LTRANPHD$ Account Domain: WORKGROUP Logon ID: 0x3e7 Logon Type: 5 Impersonation Level: %%1833 New Logon: Security ID: S-1-5-20 Account Name: NETWORK SERVICE Account Domain: NT AUTHORITY Logon ID: 0x3e4 Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x234 Process Name: C:\Windows\System32\services.exe Network Information: Workstation Name: Source Network Address: - Source Port: - Detailed Authentication Information: Logon Process: Advapi Authentication Package: Negotiate Transited Services: - Package Name (NTLM only): - Key Length: 0 This event is generated when a logon session is created. It is generated on the computer that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service such as the Server service, or a local process such as Winlogon.exe or Services.exe. The logon type field indicates the kind of logon that occurred. The most common types are 2 (interactive) and 3 (network). The New Logon fields indicate the account for whom the new logon was created, i.e. the account that was logged on. The network fields indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impersonation level field indicates the extent to which a process in the logon session can impersonate. The authentication information fields provide detailed information about this specific logon request. - Logon GUID is a unique identifier that can be used to correlate this event with a KDC event. - Transited services indicate which intermediate services have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indicates the length of the generated session key. This will be 0 if no session key was requested.
Security	Audit Success	12544	2015-04-25 15:32:49	Microsoft-Windows-Security-Auditing	4648: A logon was attempted using explicit credentials. Subject: Security ID: S-1-5-18 Account Name: LTRANPHD$ Account Domain: WORKGROUP Logon ID: 0x3e7 Logon GUID: {00000000-0000-0000-0000-000000000000} Account Whose Credentials Were Used: Account Name: DWM-1 Account Domain: Window Manager Logon GUID: {00000000-0000-0000-0000-000000000000} Target Server: Target Server Name: localhost Additional Information: localhost Process Information: Process ID: 0x20c Process Name: C:\Windows\System32\winlogon.exe Network Information: Network Address: - Port: - This event is generated when a process attempts to log on an account by explicitly specifying that account's credentials. This most commonly occurs in batch-type configurations such as scheduled tasks, or when using the RUNAS command.
Security	Audit Success	12544	2015-04-25 15:32:49	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: LTRANPHD$ Account Domain: WORKGROUP Logon ID: 0x3e7 Logon Type: 2 Impersonation Level: %%1833 New Logon: Security ID: S-1-5-90-1 Account Name: DWM-1 Account Domain: Window Manager Logon ID: 0xebd6 Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x20c Process Name: C:\Windows\System32\winlogon.exe Network Information: Workstation Name: Source Network Address: - Source Port: - Detailed Authentication Information: Logon Process: Advapi Authentication Package: Negotiate Transited Services: - Package Name (NTLM only): - Key Length: 0 This event is generated when a logon session is created. It is generated on the computer that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service such as the Server service, or a local process such as Winlogon.exe or Services.exe. The logon type field indicates the kind of logon that occurred. The most common types are 2 (interactive) and 3 (network). The New Logon fields indicate the account for whom the new logon was created, i.e. the account that was logged on. The network fields indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impersonation level field indicates the extent to which a process in the logon session can impersonate. The authentication information fields provide detailed information about this specific logon request. - Logon GUID is a unique identifier that can be used to correlate this event with a KDC event. - Transited services indicate which intermediate services have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indicates the length of the generated

					session key. This will be 0 if no session key was requested.
Security	Audit Success	12544	2015-04-25 15:32:49	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: LTRANPHD$ Account Domain: WORKGROUP Logon ID: 0x3e7 Logon Type: 2 Impersonation Level: %%1833 New Logon: Security ID: S-1-5-90-1 Account Name: DWM-1 Account Domain: Window Manager Logon ID: 0xec09 Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x20c Process Name: C:\Windows\System32\winlogon.exe Network Information: Workstation Name: Source Network Address: - Source Port: - Detailed Authentication Information: Logon Process: Advapi Authentication Package: Negotiate Transited Services: - Package Name (NTLM only): - Key Length: 0 This event is generated when a logon session is created. It is generated on the computer that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service such as the Server service, or a local process such as Winlogon.exe or Services.exe. The logon type field indicates the kind of logon that occurred. The most common types are 2 (interactive) and 3 (network). The New Logon fields indicate the account for whom the new logon was created, i.e. the account that was logged on. The network fields indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impersonation level field indicates the extent to which a process in the logon session can impersonate. The authentication information fields provide detailed information about this specific logon request. - Logon GUID is a unique identifier that can be used to correlate this event with a KDC event. - Transited services indicate which intermediate services have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indicates the length of the generated session key. This will be 0 if no session key was requested.
Security	Audit Success	12544	2015-04-25 15:32:49	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: LTRANPHD$ Account Domain: WORKGROUP Logon ID: 0x3e7 Logon Type: 5 Impersonation Level: %%1833 New Logon: Security ID: S-1-5-19 Account Name: LOCAL SERVICE Account Domain: NT AUTHORITY Logon ID: 0x3e5 Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x234 Process Name: C:\Windows\System32\services.exe Network Information: Workstation Name: Source Network Address: - Source Port: - Detailed Authentication Information: Logon Process: Advapi Authentication Package: Negotiate Transited Services: - Package Name (NTLM only): - Key Length: 0 This event is generated when a logon session is created. It is generated on the computer that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service such as the Server service, or a local process such as Winlogon.exe or Services.exe. The logon type field indicates the kind of logon that occurred. The most common types are 2 (interactive) and 3 (network). The New Logon fields indicate the account for whom the new logon was created, i.e. the account that was logged on. The network fields indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impersonation level field indicates the extent to which a process in the logon session can impersonate. The authentication information fields provide detailed information about this specific logon request. - Logon GUID is a unique identifier that can be used to correlate this event with a KDC event. - Transited services indicate which intermediate services have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indicates the length of the generated session key. This will be 0 if no session key was requested.
Security	Audit Success	12544	2015-04-25 15:32:49	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: LTRANPHD$ Account Domain: WORKGROUP Logon ID: 0x3e7 Logon Type: 5 Impersonation Level: %%1833 New Logon: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Logon ID: 0x3e7 Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x234 Process Name: C:\Windows\System32\services.exe Network Information: Workstation Name: Source Network Address: - Source Port: - Detailed Authentication Information: Logon Process: Advapi Authentication Package: Negotiate Transited Services: - Package Name (NTLM only): - Key Length: 0 This event is generated when a logon session is created. It is generated on the computer that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service such as the Server service, or a local process such as Winlogon.exe or Services.exe. The logon type field indicates the kind of logon that occurred. The most common types are 2 (interactive) and 3 (network). The New Logon fields indicate the account for whom the new logon was created, i.e. the account that was logged on. The network fields indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impersonation level field indicates the extent to which a process in the logon session can impersonate. The authentication information fields provide detailed information about this specific logon request. - Logon GUID is a unique identifier that can be used to correlate this event with a KDC event. - Transited services indicate which intermediate services have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indicates the length of the generated session key. This will be 0 if no session key was requested.
			2015-04-		4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: LTRANPHD$ Account Domain: WORKGROUP Logon ID: 0x3e7 Logon Type: 5 Impersonation Level: %%1833 New Logon: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Logon ID: 0x3e7 Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x234 Process Name: C:\Windows\System32\services.exe Network Information: Workstation Name: Source Network Address: - Source Port: - Detailed Authentication Information: Logon Process: Advapi Authentication Package: Negotiate Transited Services: - Package Name (NTLM only): - Key Length: 0 This event is generated when a logon session is created. It is generated on the computer that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service such as the Server service, or a local

Security	Audit Success	12544	25 15:32:49	Microsoft-Windows-Security-Auditing	process such as Winlogon.exe or Services.exe. The logon type field indicates the kind of logon that occurred. The most common types are 2 (interactive) and 3 (network). The New Logon fields indicate the account for whom the new logon was created, i.e. the account that was logged on. The network fields indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impersonation level field indicates the extent to which a process in the logon session can impersonate. The authentication information fields provide detailed information about this specific logon request. - Logon GUID is a unique identifier that can be used to correlate this event with a KDC event. - Transited services indicate which intermediate services have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indicates the length of the generated session key. This will be 0 if no session key was requested.
Security	Audit Success	12544	2015-04-25 15:32:49	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: LTRANPHD$ Account Domain: WORKGROUP Logon ID: 0x3e7 Logon Type: 5 Impersonation Level: %%1833 New Logon: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Logon ID: 0x3e7 Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x234 Process Name: C:\Windows\System32\services.exe Network Information: Workstation Name: Source Network Address: - Source Port: - Detailed Authentication Information: Logon Process: Advapi Authentication Package: Negotiate Transited Services: - Package Name (NTLM only): - Key Length: 0 This event is generated when a logon session is created. It is generated on the computer that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service such as the Server service, or a local process such as Winlogon.exe or Services.exe. The logon type field indicates the kind of logon that occurred. The most common types are 2 (interactive) and 3 (network). The New Logon fields indicate the account for whom the new logon was created, i.e. the account that was logged on. The network fields indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impersonation level field indicates the extent to which a process in the logon session can impersonate. The authentication information fields provide detailed information about this specific logon request. - Logon GUID is a unique identifier that can be used to correlate this event with a KDC event. - Transited services indicate which intermediate services have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indicates the length of the generated session key. This will be 0 if no session key was requested.
Security	Audit Success	12548	2015-04-25 15:32:49	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Logon ID: 0x3e7 Privileges: SeAssignPrimaryTokenPrivilege SeTcbPrivilege SeSecurityPrivilege SeTakeOwnershipPrivilege SeLoadDriverPrivilege SeBackupPrivilege SeRestorePrivilege SeDebugPrivilege SeAuditPrivilege SeSystemEnvironmentPrivilege SeImpersonatePrivilege
Security	Audit Success	12548	2015-04-25 15:32:49	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-20 Account Name: NETWORK SERVICE Account Domain: NT AUTHORITY Logon ID: 0x3e4 Privileges: SeAssignPrimaryTokenPrivilege SeAuditPrivilege SeImpersonatePrivilege
Security	Audit Success	12548	2015-04-25 15:32:49	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-90-1 Account Name: DWM-1 Account Domain: Window Manager Logon ID: 0xebd6 Privileges: SeAssignPrimaryTokenPrivilege SeAuditPrivilege SeImpersonatePrivilege
Security	Audit Success	12548	2015-04-25 15:32:49	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-90-1 Account Name: DWM-1 Account Domain: Window Manager Logon ID: 0xec09 Privileges: SeAssignPrimaryTokenPrivilege SeAuditPrivilege
Security	Audit Success	12548	2015-04-25 15:32:49	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-19 Account Name: LOCAL SERVICE Account Domain: NT AUTHORITY Logon ID: 0x3e5 Privileges: SeAssignPrimaryTokenPrivilege SeAuditPrivilege SeImpersonatePrivilege
Security	Audit Success	12548	2015-04-25 15:32:49	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Logon ID: 0x3e7 Privileges: SeAssignPrimaryTokenPrivilege SeTcbPrivilege SeSecurityPrivilege SeTakeOwnershipPrivilege SeLoadDriverPrivilege SeBackupPrivilege SeRestorePrivilege SeDebugPrivilege SeAuditPrivilege SeSystemEnvironmentPrivilege SeImpersonatePrivilege
Security	Audit Success	12548	2015-04-25 15:32:49	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Logon ID: 0x3e7 Privileges: SeAssignPrimaryTokenPrivilege SeTcbPrivilege SeSecurityPrivilege SeTakeOwnershipPrivilege SeLoadDriverPrivilege SeBackupPrivilege SeRestorePrivilege SeDebugPrivilege SeAuditPrivilege SeSystemEnvironmentPrivilege SeImpersonatePrivilege
Security	Audit Success	12548	2015-04-25 15:32:49	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Logon ID: 0x3e7 Privileges: SeAssignPrimaryTokenPrivilege SeTcbPrivilege SeSecurityPrivilege SeTakeOwnershipPrivilege SeLoadDriverPrivilege SeBackupPrivilege SeRestorePrivilege SeDebugPrivilege SeAuditPrivilege SeSystemEnvironmentPrivilege SeImpersonatePrivilege
Security	Audit Success	13568	2015-04-25 15:32:49	Microsoft-Windows-Security-Auditing	4902: The Per-user audit policy table was created. Number of Elements: 0 Policy ID: 0x9b73
					4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: LTRANPHD$ Account Domain: WORKGROUP Logon ID: 0x3e7 Logon Type: 5 Impersonation Level: %%1833 New Logon: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Logon ID: 0x3e7 Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x234 Process Name:

Security	Audit Success	12544	2015-04-25 15:32:50	Microsoft-Windows-Security-Auditing	C:\Windows\System32\services.exe Network Information: Workstation Name: Source Network Address: - Source Port: - Detailed Authentication Information: Logon Process: Advapi Authentication Package: Negotiate Transited Services: - Package Name (NTLM only): - Key Length: 0 This event is generated when a logon session is created. It is generated on the computer that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service such as the Server service, or a local process such as Winlogon.exe or Services.exe. The logon type field indicates the kind of logon that occurred. The most common types are 2 (interactive) and 3 (network). The New Logon fields indicate the account for whom the new logon was created, i.e. the account that was logged on. The network fields indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impersonation level field indicates the extent to which a process in the logon session can impersonate. The authentication information fields provide detailed information about this specific logon request. - Logon GUID is a unique identifier that can be used to correlate this event with a KDC event. - Transited services indicate which intermediate services have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indicates the length of the generated session key. This will be 0 if no session key was requested.
Security	Audit Success	12548	2015-04-25 15:32:50	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Logon ID: 0x3e7 Privileges: SeAssignPrimaryTokenPrivilege SeTcbPrivilege SeSecurityPrivilege SeTakeOwnershipPrivilege SeLoadDriverPrivilege SeBackupPrivilege SeRestorePrivilege SeDebugPrivilege SeAuditPrivilege SeSystemEnvironmentPrivilege SeImpersonatePrivilege
Security	Audit Success	12292	2015-04-25 15:32:51	Microsoft-Windows-Security-Auditing	5033: The Windows Firewall Driver started successfully.
Security	Audit Success	12544	2015-04-25 15:32:51	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: LTRANPHD$ Account Domain: WORKGROUP Logon ID: 0x3e7 Logon Type: 5 Impersonation Level: %%1833 New Logon: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Logon ID: 0x3e7 Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x234 Process Name: C:\Windows\System32\services.exe Network Information: Workstation Name: Source Network Address: - Source Port: - Detailed Authentication Information: Logon Process: Advapi Authentication Package: Negotiate Transited Services: - Package Name (NTLM only): - Key Length: 0 This event is generated when a logon session is created. It is generated on the computer that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service such as the Server service, or a local process such as Winlogon.exe or Services.exe. The logon type field indicates the kind of logon that occurred. The most common types are 2 (interactive) and 3 (network). The New Logon fields indicate the account for whom the new logon was created, i.e. the account that was logged on. The network fields indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impersonation level field indicates the extent to which a process in the logon session can impersonate. The authentication information fields provide detailed information about this specific logon request. - Logon GUID is a unique identifier that can be used to correlate this event with a KDC event. - Transited services indicate which intermediate services have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indicates the length of the generated session key. This will be 0 if no session key was requested.
Security	Audit Success	12548	2015-04-25 15:32:51	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Logon ID: 0x3e7 Privileges: SeAssignPrimaryTokenPrivilege SeTcbPrivilege SeSecurityPrivilege SeTakeOwnershipPrivilege SeLoadDriverPrivilege SeBackupPrivilege SeRestorePrivilege SeDebugPrivilege SeAuditPrivilege SeSystemEnvironmentPrivilege SeImpersonatePrivilege
Security	Audit Success	12292	2015-04-25 15:32:52	Microsoft-Windows-Security-Auditing	5024: The Windows Firewall service started successfully.
Security	Audit Success	12544	2015-04-25 15:32:52	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: LTRANPHD$ Account Domain: WORKGROUP Logon ID: 0x3e7 Logon Type: 5 Impersonation Level: %%1833 New Logon: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Logon ID: 0x3e7 Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x234 Process Name: C:\Windows\System32\services.exe Network Information: Workstation Name: Source Network Address: - Source Port: - Detailed Authentication Information: Logon Process: Advapi Authentication Package: Negotiate Transited Services: - Package Name (NTLM only): - Key Length: 0 This event is generated when a logon session is created. It is generated on the computer that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service such as the Server service, or a local process such as Winlogon.exe or Services.exe. The logon type field indicates the kind of logon that occurred. The most common types are 2 (interactive) and 3 (network). The New Logon fields indicate the account for whom the new logon was created, i.e. the account that was logged on. The network fields indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impersonation level field indicates the extent to which a process in the logon session can impersonate. The authentication information fields provide detailed information about this specific logon request. - Logon GUID is a unique identifier that can be used to correlate this event with a KDC event. - Transited services indicate which intermediate services have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indicates the length of the generated

					session key. This will be 0 if no session key was requested.
Security	Audit Success	12544	2015-04-25 15:32:52	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-0-0 Account Name: - Account Domain: - Logon ID: 0x0 Logon Type: 3 Impersonation Level: %%1833 New Logon: Security ID: S-1-5-7 Account Name: ANONYMOUS LOGON Account Domain: NT AUTHORITY Logon ID: 0x1ae73 Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x0 Process Name: - Network Information: Workstation Name: Source Network Address: - Source Port: - Detailed Authentication Information: Logon Process: NtLmSsp Authentication Package: NTLM Transited Services: - Package Name (NTLM only): NTLM V1 Key Length: 0 This event is generated when a logon session is created. It is generated on the computer that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service such as the Server service, or a local process such as Winlogon.exe or Services.exe. The logon type field indicates the kind of logon that occurred. The most common types are 2 (interactive) and 3 (network). The New Logon fields indicate the account for whom the new logon was created, i.e. the account that was logged on. The network fields indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impersonation level field indicates the extent to which a process in the logon session can impersonate. The authentication information fields provide detailed information about this specific logon request. - Logon GUID is a unique identifier that can be used to correlate this event with a KDC event. - Transited services indicate which intermediate services have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indicates the length of the generated session key. This will be 0 if no session key was requested.
Security	Audit Success	12548	2015-04-25 15:32:52	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Logon ID: 0x3e7 Privileges: SeAssignPrimaryTokenPrivilege SeTcbPrivilege SeSecurityPrivilege SeTakeOwnershipPrivilege SeLoadDriverPrivilege SeBackupPrivilege SeRestorePrivilege SeDebugPrivilege SeAuditPrivilege SeSystemEnvironmentPrivilege SeImpersonatePrivilege
Security	Audit Success	12544	2015-04-25 15:32:55	Microsoft-Windows-Security-Auditing	4648: A logon was attempted using explicit credentials. Subject: Security ID: S-1-5-18 Account Name: LTRANPHD$ Account Domain: WORKGROUP Logon ID: 0x3e7 Logon GUID: {00000000-0000-0000-0000-000000000000} Account Whose Credentials Were Used: Account Name: Liem Account Domain: LTRANPHD Logon GUID: {00000000-0000-0000-0000-000000000000} Target Server: Target Server Name: localhost Additional Information: localhost Process Information: Process ID: 0x20c Process Name: C:\Windows\System32\winlogon.exe Network Information: Network Address: 127.0.0.1 Port: 0 This event is generated when a process attempts to log on an account by explicitly specifying that account's credentials. This most commonly occurs in batch-type configurations such as scheduled tasks, or when using the RUNAS command.
Security	Audit Success	12544	2015-04-25 15:32:55	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: LTRANPHD$ Account Domain: WORKGROUP Logon ID: 0x3e7 Logon Type: 2 Impersonation Level: %%1833 New Logon: Security ID: S-1-5-21-1888849264-3803429180-4108621888-1001 Account Name: Liem Account Domain: LTRANPHD Logon ID: 0x1e83a Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x20c Process Name: C:\Windows\System32\winlogon.exe Network Information: Workstation Name: LTRANPHD Source Network Address: 127.0.0.1 Source Port: 0 Detailed Authentication Information: Logon Process: User32 Authentication Package: Negotiate Transited Services: - Package Name (NTLM only): - Key Length: 0 This event is generated when a logon session is created. It is generated on the computer that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service such as the Server service, or a local process such as Winlogon.exe or Services.exe. The logon type field indicates the kind of logon that occurred. The most common types are 2 (interactive) and 3 (network). The New Logon fields indicate the account for whom the new logon was created, i.e. the account that was logged on. The network fields indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impersonation level field indicates the extent to which a process in the logon session can impersonate. The authentication information fields provide detailed information about this specific logon request. - Logon GUID is a unique identifier that can be used to correlate this event with a KDC event. - Transited services indicate which intermediate services have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indicates the length of the generated session key. This will be 0 if no session key was requested.
Security	Audit Success	12544	2015-04-25 15:32:55	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: LTRANPHD$ Account Domain: WORKGROUP Logon ID: 0x3e7 Logon Type: 2 Impersonation Level: %%1833 New Logon: Security ID: S-1-5-21-1888849264-3803429180-4108621888-1001 Account Name: Liem Account Domain: LTRANPHD Logon ID: 0x1e86a Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x20c Process Name: C:\Windows\System32\winlogon.exe Network Information: Workstation Name: LTRANPHD Source Network Address: 127.0.0.1 Source Port: 0 Detailed Authentication Information: Logon Process: User32 Authentication Package: Negotiate Transited Services: - Package Name (NTLM only): - Key Length: 0 This event is generated when a logon session is created. It is generated on the computer that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service such as the Server service, or a local process such as Winlogon.exe or Services.exe. The logon type field indicates the kind of logon that occurred. The most common types are 2 (interactive) and 3 (network). The New Logon fields indicate the account for whom the new logon was created, i.e. the account that was logged on. The network fields indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impersonation level field indicates the extent to which a process in the logon session can impersonate. The authentication information fields provide detailed

					information about this specific logon request. - Logon GUID is a unique identifier that can be used to correlate this event with a KDC event. - Transited services indicate which intermediate services have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indicates the length of the generated session key. This will be 0 if no session key was requested.
Security	Audit Success	12544	2015-04-25 15:32:55	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: LTRANPHD$ Account Domain: WORKGROUP Logon ID: 0x3e7 Logon Type: 5 Impersonation Level: %%1833 New Logon: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Logon ID: 0x3e7 Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x234 Process Name: C:\Windows\System32\services.exe Network Information: Workstation Name: Source Network Address: - Source Port: - Detailed Authentication Information: Logon Process: Advapi Authentication Package: Negotiate Transited Services: - Package Name (NTLM only): - Key Length: 0 This event is generated when a logon session is created. It is generated on the computer that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service such as the Server service, or a local process such as Winlogon.exe or Services.exe. The logon type field indicates the kind of logon that occurred. The most common types are 2 (interactive) and 3 (network). The New Logon fields indicate the account for whom the new logon was created, i.e. the account that was logged on. The network fields indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impersonation level field indicates the extent to which a process in the logon session can impersonate. The authentication information fields provide detailed information about this specific logon request. - Logon GUID is a unique identifier that can be used to correlate this event with a KDC event. - Transited services indicate which intermediate services have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indicates the length of the generated session key. This will be 0 if no session key was requested.
Security	Audit Success	12548	2015-04-25 15:32:55	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-21-1888849264-3803429180-4108621888-1001 Account Name: Liem Account Domain: LTRANPHD Logon ID: 0x1e83a Privileges: SeSecurityPrivilege SeTakeOwnershipPrivilege SeLoadDriverPrivilege SeBackupPrivilege SeRestorePrivilege SeDebugPrivilege SeSystemEnvironmentPrivilege SeImpersonatePrivilege
Security	Audit Success	12548	2015-04-25 15:32:55	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Logon ID: 0x3e7 Privileges: SeAssignPrimaryTokenPrivilege SeTcbPrivilege SeSecurityPrivilege SeTakeOwnershipPrivilege SeLoadDriverPrivilege SeBackupPrivilege SeRestorePrivilege SeDebugPrivilege SeAuditPrivilege SeSystemEnvironmentPrivilege SeImpersonatePrivilege
Security	Audit Success	13824	2015-04-25 15:32:57	Microsoft-Windows-Security-Auditing	4797: An attempt was made to query the existence of a blank password for an account. Subject: Security ID: S-1-5-21-1888849264-3803429180-4108621888-1001 Account Name: Liem Account Domain: LTRANPHD Logon ID: 0x1e86a Additional Information: Caller Workstation: LTRANPHD Target Account Name: Administrator Target Account Domain: LTRANPHD
Security	Audit Success	13824	2015-04-25 15:32:57	Microsoft-Windows-Security-Auditing	4797: An attempt was made to query the existence of a blank password for an account. Subject: Security ID: S-1-5-21-1888849264-3803429180-4108621888-1001 Account Name: Liem Account Domain: LTRANPHD Logon ID: 0x1e86a Additional Information: Caller Workstation: LTRANPHD Target Account Name: Guest Target Account Domain: LTRANPHD
Security	Audit Success	13824	2015-04-25 15:32:57	Microsoft-Windows-Security-Auditing	4797: An attempt was made to query the existence of a blank password for an account. Subject: Security ID: S-1-5-21-1888849264-3803429180-4108621888-1001 Account Name: Liem Account Domain: LTRANPHD Logon ID: 0x1e86a Additional Information: Caller Workstation: LTRANPHD Target Account Name: Administrator Target Account Domain: LTRANPHD
Security	Audit Success	13824	2015-04-25 15:32:57	Microsoft-Windows-Security-Auditing	4797: An attempt was made to query the existence of a blank password for an account. Subject: Security ID: S-1-5-21-1888849264-3803429180-4108621888-1001 Account Name: Liem Account Domain: LTRANPHD Logon ID: 0x1e86a Additional Information: Caller Workstation: LTRANPHD Target Account Name: Guest Target Account Domain: LTRANPHD
Security	Audit Success	13824	2015-04-25 15:32:59	Microsoft-Windows-Security-Auditing	4797: An attempt was made to query the existence of a blank password for an account. Subject: Security ID: S-1-5-19 Account Name: LOCAL SERVICE Account Domain: NT AUTHORITY Logon ID: 0x3e5 Additional Information: Caller Workstation: LTRANPHD Target Account Name: Administrator Target Account Domain: LTRANPHD
Security	Audit Success	13824	2015-04-25 15:32:59	Microsoft-Windows-Security-Auditing	4797: An attempt was made to query the existence of a blank password for an account. Subject: Security ID: S-1-5-19 Account Name: LOCAL SERVICE Account Domain: NT AUTHORITY Logon ID: 0x3e5 Additional Information: Caller Workstation: LTRANPHD Target Account Name: Administrator Target Account Domain: LTRANPHD
Security	Audit Success	13824	2015-04-25 15:32:59	Microsoft-Windows-Security-Auditing	4797: An attempt was made to query the existence of a blank password for an account. Subject: Security ID: S-1-5-19 Account Name: LOCAL SERVICE Account Domain: NT AUTHORITY Logon ID: 0x3e5 Additional Information: Caller Workstation: LTRANPHD Target Account Name: Guest Target Account Domain: LTRANPHD
Security	Audit Success	13824	2015-04-25 15:32:59	Microsoft-Windows-Security-Auditing	4797: An attempt was made to query the existence of a blank password for an account. Subject: Security ID: S-1-5-19 Account Name: LOCAL SERVICE Account Domain: NT AUTHORITY Logon ID: 0x3e5 Additional Information: Caller Workstation: LTRANPHD Target Account Name: Guest Target Account Domain: LTRANPHD
Security	Audit Success	13824	2015-04-25 15:32:59	Microsoft-Windows-Security-Auditing	4797: An attempt was made to query the existence of a blank password for an account. Subject: Security ID: S-1-5-19 Account Name: LOCAL SERVICE Account Domain: NT AUTHORITY Logon ID: 0x3e5 Additional Information: Caller Workstation: LTRANPHD Target Account Name: Liem Target Account Domain: LTRANPHD

Security	Audit Success	13824	2015-04-25 15:32:59	Microsoft-Windows-Security-Auditing	4797: An attempt was made to query the existence of a blank password for an account. Subject: Security ID: S-1-5-19 Account Name: LOCAL SERVICE Account Domain: NT AUTHORITY Logon ID: 0x3e5 Additional Information: Caller Workstation: LTRANPHD Target Account Name: Liem Target Account Domain: LTRANPHD
Security	Audit Success	13824	2015-04-25 15:32:59	Microsoft-Windows-Security-Auditing	4797: An attempt was made to query the existence of a blank password for an account. Subject: Security ID: S-1-5-19 Account Name: LOCAL SERVICE Account Domain: NT AUTHORITY Logon ID: 0x3e5 Additional Information: Caller Workstation: LTRANPHD Target Account Name: Liem Target Account Domain: LTRANPHD
Security	Audit Success	13824	2015-04-25 15:32:59	Microsoft-Windows-Security-Auditing	4797: An attempt was made to query the existence of a blank password for an account. Subject: Security ID: S-1-5-19 Account Name: LOCAL SERVICE Account Domain: NT AUTHORITY Logon ID: 0x3e5 Additional Information: Caller Workstation: LTRANPHD Target Account Name: Liem Target Account Domain: LTRANPHD
Security	Audit Success	12288	2015-04-25 16:03:00	Microsoft-Windows-Security-Auditing	4608: Windows is starting up. This event is logged when LSASS.EXE starts and the auditing subsystem is initialized.
Security	Audit Success	12544	2015-04-25 16:03:00	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-0-0 Account Name: - Account Domain: - Logon ID: 0x0 Logon Type: 0 Impersonation Level: - New Logon: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Logon ID: 0x3e7 Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x4 Process Name: Network Information: Workstation Name: - Source Network Address: - Source Port: - Detailed Authentication Information: Logon Process: - Authentication Package: - Transited Services: - Package Name (NTLM only): - Key Length: 0 This event is generated when a logon session is created. It is generated on the computer that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service such as the Server service, or a local process such as Winlogon.exe or Services.exe. The logon type field indicates the kind of logon that occurred. The most common types are 2 (interactive) and 3 (network). The New Logon fields indicate the account for whom the new logon was created, i.e. the account that was logged on. The network fields indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impersonation level field indicates the extent to which a process in the logon session can impersonate. The authentication information fields provide detailed information about this specific logon request. - Logon GUID is a unique identifier that can be used to correlate this event with a KDC event. - Transited services indicate which intermediate services have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indicates the length of the generated session key. This will be 0 if no session key was requested.
Security	Audit Success	12544	2015-04-25 16:03:00	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: LTRANPHD$ Account Domain: WORKGROUP Logon ID: 0x3e7 Logon Type: 5 Impersonation Level: %%1833 New Logon: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Logon ID: 0x3e7 Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x238 Process Name: C:\Windows\System32\services.exe Network Information: Workstation Name: Source Network Address: - Source Port: - Detailed Authentication Information: Logon Process: Advapi Authentication Package: Negotiate Transited Services: - Package Name (NTLM only): - Key Length: 0 This event is generated when a logon session is created. It is generated on the computer that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service such as the Server service, or a local process such as Winlogon.exe or Services.exe. The logon type field indicates the kind of logon that occurred. The most common types are 2 (interactive) and 3 (network). The New Logon fields indicate the account for whom the new logon was created, i.e. the account that was logged on. The network fields indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impersonation level field indicates the extent to which a process in the logon session can impersonate. The authentication information fields provide detailed information about this specific logon request. - Logon GUID is a unique identifier that can be used to correlate this event with a KDC event. - Transited services indicate which intermediate services have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indicates the length of the generated session key. This will be 0 if no session key was requested.
Security	Audit Success	12544	2015-04-25 16:03:00	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: LTRANPHD$ Account Domain: WORKGROUP Logon ID: 0x3e7 Logon Type: 5 Impersonation Level: %%1833 New Logon: Security ID: S-1-5-20 Account Name: NETWORK SERVICE Account Domain: NT AUTHORITY Logon ID: 0x3e4 Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x238 Process Name: C:\Windows\System32\services.exe Network Information: Workstation Name: Source Network Address: - Source Port: - Detailed Authentication Information: Logon Process: Advapi Authentication Package: Negotiate Transited Services: - Package Name (NTLM only): - Key Length: 0 This event is generated when a logon session is created. It is generated on the computer that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service such as the Server service, or a local process such as Winlogon.exe or Services.exe. The logon type field indicates the kind of logon that occurred. The most common types are 2 (interactive) and 3 (network). The New Logon fields indicate the account for whom the new logon was created, i.e. the account that was logged on. The network fields indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impersonation level field indicates the extent to which a process in the logon session can impersonate. The authentication information fields provide detailed information about this specific logon request. - Logon GUID is a unique identifier that can be used to correlate this event with a KDC event. - Transited services indicate which intermediate services have participated in this logon request. - Package name indicates

					which sub-protocol was used among the NTLM protocols. - Key length indicates the length of the generated session key. This will be 0 if no session key was requested.
Security	Audit Success	12544	2015-04-25 16:03:00	Microsoft-Windows-Security-Auditing	4648: A logon was attempted using explicit credentials. Subject: Security ID: S-1-5-18 Account Name: LTRANPHD$ Account Domain: WORKGROUP Logon ID: 0x3e7 Logon GUID: {00000000-0000-0000-0000-000000000000} Account Whose Credentials Were Used: Account Name: DWM-1 Account Domain: Window Manager Logon GUID: {00000000-0000-0000-0000-000000000000} Target Server: Target Server Name: localhost Additional Information: localhost Process Information: Process ID: 0x21c Process Name: C:\Windows\System32\winlogon.exe Network Information: Network Address: - Port: - This event is generated when a process attempts to log on an account by explicitly specifying that account's credentials. This most commonly occurs in batch-type configurations such as scheduled tasks, or when using the RUNAS command.
Security	Audit Success	12544	2015-04-25 16:03:00	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: LTRANPHD$ Account Domain: WORKGROUP Logon ID: 0x3e7 Logon Type: 2 Impersonation Level: %%1833 New Logon: Security ID: S-1-5-90-1 Account Name: DWM-1 Account Domain: Window Manager Logon ID: 0xfe38 Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x21c Process Name: C:\Windows\System32\winlogon.exe Network Information: Workstation Name: Source Network Address: - Source Port: - Detailed Authentication Information: Logon Process: Advapi Authentication Package: Negotiate Transited Services: - Package Name (NTLM only): - Key Length: 0 This event is generated when a logon session is created. It is generated on the computer that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service such as the Server service, or a local process such as Winlogon.exe or Services.exe. The logon type field indicates the kind of logon that occurred. The most common types are 2 (interactive) and 3 (network). The New Logon fields indicate the account for whom the new logon was created, i.e. the account that was logged on. The network fields indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impersonation level field indicates the extent to which a process in the logon session can impersonate. The authentication information fields provide detailed information about this specific logon request. - Logon GUID is a unique identifier that can be used to correlate this event with a KDC event. - Transited services indicate which intermediate services have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indicates the length of the generated session key. This will be 0 if no session key was requested.
Security	Audit Success	12544	2015-04-25 16:03:00	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: LTRANPHD$ Account Domain: WORKGROUP Logon ID: 0x3e7 Logon Type: 2 Impersonation Level: %%1833 New Logon: Security ID: S-1-5-90-1 Account Name: DWM-1 Account Domain: Window Manager Logon ID: 0xfe55 Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x21c Process Name: C:\Windows\System32\winlogon.exe Network Information: Workstation Name: Source Network Address: - Source Port: - Detailed Authentication Information: Logon Process: Advapi Authentication Package: Negotiate Transited Services: - Package Name (NTLM only): - Key Length: 0 This event is generated when a logon session is created. It is generated on the computer that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service such as the Server service, or a local process such as Winlogon.exe or Services.exe. The logon type field indicates the kind of logon that occurred. The most common types are 2 (interactive) and 3 (network). The New Logon fields indicate the account for whom the new logon was created, i.e. the account that was logged on. The network fields indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impersonation level field indicates the extent to which a process in the logon session can impersonate. The authentication information fields provide detailed information about this specific logon request. - Logon GUID is a unique identifier that can be used to correlate this event with a KDC event. - Transited services indicate which intermediate services have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indicates the length of the generated session key. This will be 0 if no session key was requested.
Security	Audit Success	12544	2015-04-25 16:03:00	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: LTRANPHD$ Account Domain: WORKGROUP Logon ID: 0x3e7 Logon Type: 5 Impersonation Level: %%1833 New Logon: Security ID: S-1-5-19 Account Name: LOCAL SERVICE Account Domain: NT AUTHORITY Logon ID: 0x3e5 Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x238 Process Name: C:\Windows\System32\services.exe Network Information: Workstation Name: Source Network Address: - Source Port: - Detailed Authentication Information: Logon Process: Advapi Authentication Package: Negotiate Transited Services: - Package Name (NTLM only): - Key Length: 0 This event is generated when a logon session is created. It is generated on the computer that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service such as the Server service, or a local process such as Winlogon.exe or Services.exe. The logon type field indicates the kind of logon that occurred. The most common types are 2 (interactive) and 3 (network). The New Logon fields indicate the account for whom the new logon was created, i.e. the account that was logged on. The network fields indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impersonation level field indicates the extent to which a process in the logon session can impersonate. The authentication information fields provide detailed information about this specific logon request. - Logon GUID is a unique identifier that can be used to correlate this event with a KDC event. - Transited services indicate which intermediate services have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indicates the length of the generated session key. This will be 0 if no session key was requested.

Security	Audit Success	12544	2015-04-25 16:03:00	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: LTRANPHD$ Account Domain: WORKGROUP Logon ID: 0x3e7 Logon Type: 5 Impersonation Level: %%1833 New Logon: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Logon ID: 0x3e7 Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x238 Process Name: C:\Windows\System32\services.exe Network Information: Workstation Name: Source Network Address: - Source Port: - Detailed Authentication Information: Logon Process: Advapi Authentication Package: Negotiate Transited Services: - Package Name (NTLM only): - Key Length: 0 This event is generated when a logon session is created. It is generated on the computer that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service such as the Server service, or a local process such as Winlogon.exe or Services.exe. The logon type field indicates the kind of logon that occurred. The most common types are 2 (interactive) and 3 (network). The New Logon fields indicate the account for whom the new logon was created, i.e. the account that was logged on. The network fields indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impersonation level field indicates the extent to which a process in the logon session can impersonate. The authentication information fields provide detailed information about this specific logon request. - Logon GUID is a unique identifier that can be used to correlate this event with a KDC event. - Transited services indicate which intermediate services have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indicates the length of the generated session key. This will be 0 if no session key was requested.
Security	Audit Success	12544	2015-04-25 16:03:00	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: LTRANPHD$ Account Domain: WORKGROUP Logon ID: 0x3e7 Logon Type: 5 Impersonation Level: %%1833 New Logon: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Logon ID: 0x3e7 Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x238 Process Name: C:\Windows\System32\services.exe Network Information: Workstation Name: Source Network Address: - Source Port: - Detailed Authentication Information: Logon Process: Advapi Authentication Package: Negotiate Transited Services: - Package Name (NTLM only): - Key Length: 0 This event is generated when a logon session is created. It is generated on the computer that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service such as the Server service, or a local process such as Winlogon.exe or Services.exe. The logon type field indicates the kind of logon that occurred. The most common types are 2 (interactive) and 3 (network). The New Logon fields indicate the account for whom the new logon was created, i.e. the account that was logged on. The network fields indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impersonation level field indicates the extent to which a process in the logon session can impersonate. The authentication information fields provide detailed information about this specific logon request. - Logon GUID is a unique identifier that can be used to correlate this event with a KDC event. - Transited services indicate which intermediate services have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indicates the length of the generated session key. This will be 0 if no session key was requested.
Security	Audit Success	12548	2015-04-25 16:03:00	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Logon ID: 0x3e7 Privileges: SeAssignPrimaryTokenPrivilege SeTcbPrivilege SeSecurityPrivilege SeTakeOwnershipPrivilege SeLoadDriverPrivilege SeBackupPrivilege SeRestorePrivilege SeDebugPrivilege SeAuditPrivilege SeSystemEnvironmentPrivilege SeImpersonatePrivilege
Security	Audit Success	12548	2015-04-25 16:03:00	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-20 Account Name: NETWORK SERVICE Account Domain: NT AUTHORITY Logon ID: 0x3e4 Privileges: SeAssignPrimaryTokenPrivilege SeAuditPrivilege SeImpersonatePrivilege
Security	Audit Success	12548	2015-04-25 16:03:00	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-90-1 Account Name: DWM-1 Account Domain: Window Manager Logon ID: 0xfe38 Privileges: SeAssignPrimaryTokenPrivilege SeAuditPrivilege SeImpersonatePrivilege
Security	Audit Success	12548	2015-04-25 16:03:00	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-90-1 Account Name: DWM-1 Account Domain: Window Manager Logon ID: 0xfe55 Privileges: SeAssignPrimaryTokenPrivilege SeAuditPrivilege
Security	Audit Success	12548	2015-04-25 16:03:00	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-19 Account Name: LOCAL SERVICE Account Domain: NT AUTHORITY Logon ID: 0x3e5 Privileges: SeAssignPrimaryTokenPrivilege SeAuditPrivilege SeImpersonatePrivilege
Security	Audit Success	12548	2015-04-25 16:03:00	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Logon ID: 0x3e7 Privileges: SeAssignPrimaryTokenPrivilege SeTcbPrivilege SeSecurityPrivilege SeTakeOwnershipPrivilege SeLoadDriverPrivilege SeBackupPrivilege SeRestorePrivilege SeDebugPrivilege SeAuditPrivilege SeSystemEnvironmentPrivilege SeImpersonatePrivilege
Security	Audit Success	12548	2015-04-25 16:03:00	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Logon ID: 0x3e7 Privileges: SeAssignPrimaryTokenPrivilege SeTcbPrivilege SeSecurityPrivilege SeTakeOwnershipPrivilege SeLoadDriverPrivilege SeBackupPrivilege SeRestorePrivilege SeDebugPrivilege SeAuditPrivilege SeSystemEnvironmentPrivilege SeImpersonatePrivilege
Security	Audit Success	13568	2015-04-25 16:03:00	Microsoft-Windows-Security-Auditing	4902: The Per-user audit policy table was created. Number of Elements: 0 Policy ID: 0xa615

Security	Audit Success	12544	2015-04-25 16:03:01	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: LTRANPHD$ Account Domain: WORKGROUP Logon ID: 0x3e7 Logon Type: 5 Impersonation Level: %%1833 New Logon: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Logon ID: 0x3e7 Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x238 Process Name: C:\Windows\System32\services.exe Network Information: Workstation Name: Source Network Address: - Source Port: - Detailed Authentication Information: Logon Process: Advapi Authentication Package: Negotiate Transited Services: - Package Name (NTLM only): - Key Length: 0 This event is generated when a logon session is created. It is generated on the computer that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service such as the Server service, or a local process such as Winlogon.exe or Services.exe. The logon type field indicates the kind of logon that occurred. The most common types are 2 (interactive) and 3 (network). The New Logon fields indicate the account for whom the new logon was created, i.e. the account that was logged on. The network fields indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impersonation level field indicates the extent to which a process in the logon session can impersonate. The authentication information fields provide detailed information about this specific logon request. - Logon GUID is a unique identifier that can be used to correlate this event with a KDC event. - Transited services indicate which intermediate services have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indicates the length of the generated session key. This will be 0 if no session key was requested.
Security	Audit Success	12548	2015-04-25 16:03:01	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Logon ID: 0x3e7 Privileges: SeAssignPrimaryTokenPrivilege SeTcbPrivilege SeSecurityPrivilege SeTakeOwnershipPrivilege SeLoadDriverPrivilege SeBackupPrivilege SeRestorePrivilege SeDebugPrivilege SeAuditPrivilege SeSystemEnvironmentPrivilege SeImpersonatePrivilege
Security	Audit Success	12292	2015-04-25 16:03:02	Microsoft-Windows-Security-Auditing	5033: The Windows Firewall Driver started successfully.
Security	Audit Success	12292	2015-04-25 16:03:02	Microsoft-Windows-Security-Auditing	5024: The Windows Firewall service started successfully.
Security	Audit Success	12544	2015-04-25 16:03:02	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: LTRANPHD$ Account Domain: WORKGROUP Logon ID: 0x3e7 Logon Type: 5 Impersonation Level: %%1833 New Logon: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Logon ID: 0x3e7 Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x238 Process Name: C:\Windows\System32\services.exe Network Information: Workstation Name: Source Network Address: - Source Port: - Detailed Authentication Information: Logon Process: Advapi Authentication Package: Negotiate Transited Services: - Package Name (NTLM only): - Key Length: 0 This event is generated when a logon session is created. It is generated on the computer that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service such as the Server service, or a local process such as Winlogon.exe or Services.exe. The logon type field indicates the kind of logon that occurred. The most common types are 2 (interactive) and 3 (network). The New Logon fields indicate the account for whom the new logon was created, i.e. the account that was logged on. The network fields indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impersonation level field indicates the extent to which a process in the logon session can impersonate. The authentication information fields provide detailed information about this specific logon request. - Logon GUID is a unique identifier that can be used to correlate this event with a KDC event. - Transited services indicate which intermediate services have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indicates the length of the generated session key. This will be 0 if no session key was requested.
Security	Audit Success	12544	2015-04-25 16:03:02	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: LTRANPHD$ Account Domain: WORKGROUP Logon ID: 0x3e7 Logon Type: 5 Impersonation Level: %%1833 New Logon: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Logon ID: 0x3e7 Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x238 Process Name: C:\Windows\System32\services.exe Network Information: Workstation Name: Source Network Address: - Source Port: - Detailed Authentication Information: Logon Process: Advapi Authentication Package: Negotiate Transited Services: - Package Name (NTLM only): - Key Length: 0 This event is generated when a logon session is created. It is generated on the computer that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service such as the Server service, or a local process such as Winlogon.exe or Services.exe. The logon type field indicates the kind of logon that occurred. The most common types are 2 (interactive) and 3 (network). The New Logon fields indicate the account for whom the new logon was created, i.e. the account that was logged on. The network fields indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impersonation level field indicates the extent to which a process in the logon session can impersonate. The authentication information fields provide detailed information about this specific logon request. - Logon GUID is a unique identifier that can be used to correlate this event with a KDC event. - Transited services indicate which intermediate services have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indicates the length of the generated

					session key. This will be 0 if no session key was requested.
Security	Audit Success	12544	2015-04-25 16:03:02	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-0-0 Account Name: - Account Domain: - Logon ID: 0x0 Logon Type: 3 Impersonation Level: %%1833 New Logon: Security ID: S-1-5-7 Account Name: ANONYMOUS LOGON Account Domain: NT AUTHORITY Logon ID: 0x1a52b Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x0 Process Name: - Network Information: Workstation Name: Source Network Address: - Source Port: - Detailed Authentication Information: Logon Process: NtLmSsp Authentication Package: NTLM Transited Services: - Package Name (NTLM only): NTLM V1 Key Length: 0 This event is generated when a logon session is created. It is generated on the computer that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service such as the Server service, or a local process such as Winlogon.exe or Services.exe. The logon type field indicates the kind of logon that occurred. The most common types are 2 (interactive) and 3 (network). The New Logon fields indicate the account for whom the new logon was created, i.e. the account that was logged on. The network fields indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impersonation level field indicates the extent to which a process in the logon session can impersonate. The authentication information fields provide detailed information about this specific logon request. - Logon GUID is a unique identifier that can be used to correlate this event with a KDC event. - Transited services indicate which intermediate services have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indicates the length of the generated session key. This will be 0 if no session key was requested.
Security	Audit Success	12548	2015-04-25 16:03:02	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Logon ID: 0x3e7 Privileges: SeAssignPrimaryTokenPrivilege SeTcbPrivilege SeSecurityPrivilege SeTakeOwnershipPrivilege SeLoadDriverPrivilege SeBackupPrivilege SeRestorePrivilege SeDebugPrivilege SeAuditPrivilege SeSystemEnvironmentPrivilege SeImpersonatePrivilege
Security	Audit Success	12548	2015-04-25 16:03:02	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Logon ID: 0x3e7 Privileges: SeAssignPrimaryTokenPrivilege SeTcbPrivilege SeSecurityPrivilege SeTakeOwnershipPrivilege SeLoadDriverPrivilege SeBackupPrivilege SeRestorePrivilege SeDebugPrivilege SeAuditPrivilege SeSystemEnvironmentPrivilege SeImpersonatePrivilege
Security	Audit Success	12544	2015-04-25 16:03:04	Microsoft-Windows-Security-Auditing	4648: A logon was attempted using explicit credentials. Subject: Security ID: S-1-5-18 Account Name: LTRANPHD$ Account Domain: WORKGROUP Logon ID: 0x3e7 Logon GUID: {00000000-0000-0000-0000-000000000000} Account Whose Credentials Were Used: Account Name: Liem Account Domain: LTRANPHD Logon GUID: {00000000-0000-0000-0000-000000000000} Target Server: Target Server Name: localhost Additional Information: localhost Process Information: Process ID: 0x21c Process Name: C:\Windows\System32\winlogon.exe Network Information: Network Address: 127.0.0.1 Port: 0 This event is generated when a process attempts to log on an account by explicitly specifying that account's credentials. This most commonly occurs in batch-type configurations such as scheduled tasks, or when using the RUNAS command.
Security	Audit Success	12544	2015-04-25 16:03:04	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: LTRANPHD$ Account Domain: WORKGROUP Logon ID: 0x3e7 Logon Type: 2 Impersonation Level: %%1833 New Logon: Security ID: S-1-5-21-1888849264-3803429180-4108621888-1001 Account Name: Liem Account Domain: LTRANPHD Logon ID: 0x1c23e Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x21c Process Name: C:\Windows\System32\winlogon.exe Network Information: Workstation Name: LTRANPHD Source Network Address: 127.0.0.1 Source Port: 0 Detailed Authentication Information: Logon Process: User32 Authentication Package: Negotiate Transited Services: - Package Name (NTLM only): - Key Length: 0 This event is generated when a logon session is created. It is generated on the computer that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service such as the Server service, or a local process such as Winlogon.exe or Services.exe. The logon type field indicates the kind of logon that occurred. The most common types are 2 (interactive) and 3 (network). The New Logon fields indicate the account for whom the new logon was created, i.e. the account that was logged on. The network fields indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impersonation level field indicates the extent to which a process in the logon session can impersonate. The authentication information fields provide detailed information about this specific logon request. - Logon GUID is a unique identifier that can be used to correlate this event with a KDC event. - Transited services indicate which intermediate services have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indicates the length of the generated session key. This will be 0 if no session key was requested.
Security	Audit Success	12544	2015-04-25 16:03:04	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: LTRANPHD$ Account Domain: WORKGROUP Logon ID: 0x3e7 Logon Type: 2 Impersonation Level: %%1833 New Logon: Security ID: S-1-5-21-1888849264-3803429180-4108621888-1001 Account Name: Liem Account Domain: LTRANPHD Logon ID: 0x1c271 Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x21c Process Name: C:\Windows\System32\winlogon.exe Network Information: Workstation Name: LTRANPHD Source Network Address: 127.0.0.1 Source Port: 0 Detailed Authentication Information: Logon Process: User32 Authentication Package: Negotiate Transited Services: - Package Name (NTLM only): - Key Length: 0 This event is generated when a logon session is created. It is generated on the computer that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service such as the Server service, or a local process such as Winlogon.exe or Services.exe. The logon type field indicates the kind of logon that occurred. The most common types are 2 (interactive) and 3

					(network). The New Logon fields indicate the account for whom the new logon was created, i.e. the account that was logged on. The network fields indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impersonation level field indicates the extent to which a process in the logon session can impersonate. The authentication information fields provide detailed information about this specific logon request. - Logon GUID is a unique identifier that can be used to correlate this event with a KDC event. - Transited services indicate which intermediate services have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indicates the length of the generated session key. This will be 0 if no session key was requested.
Security	Audit Success	12548	2015-04-25 16:03:04	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-21-1888849264-3803429180-4108621888-1001 Account Name: Liem Account Domain: LTRANPHD Logon ID: 0x1c23e Privileges: SeSecurityPrivilege SeTakeOwnershipPrivilege SeLoadDriverPrivilege SeBackupPrivilege SeRestorePrivilege SeDebugPrivilege SeSystemEnvironmentPrivilege SeImpersonatePrivilege
Security	Audit Success	12544	2015-04-25 16:03:06	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: LTRANPHD$ Account Domain: WORKGROUP Logon ID: 0x3e7 Logon Type: 5 Impersonation Level: %%1833 New Logon: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Logon ID: 0x3e7 Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x238 Process Name: C:\Windows\System32\services.exe Network Information: Workstation Name: Source Network Address: - Source Port: - Detailed Authentication Information: Logon Process: Advapi Authentication Package: Negotiate Transited Services: - Package Name (NTLM only): - Key Length: 0 This event is generated when a logon session is created. It is generated on the computer that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service such as the Server service, or a local process such as Winlogon.exe or Services.exe. The logon type field indicates the kind of logon that occurred. The most common types are 2 (interactive) and 3 (network). The New Logon fields indicate the account for whom the new logon was created, i.e. the account that was logged on. The network fields indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impersonation level field indicates the extent to which a process in the logon session can impersonate. The authentication information fields provide detailed information about this specific logon request. - Logon GUID is a unique identifier that can be used to correlate this event with a KDC event. - Transited services indicate which intermediate services have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indicates the length of the generated session key. This will be 0 if no session key was requested.
Security	Audit Success	12548	2015-04-25 16:03:06	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Logon ID: 0x3e7 Privileges: SeAssignPrimaryTokenPrivilege SeTcbPrivilege SeSecurityPrivilege SeTakeOwnershipPrivilege SeLoadDriverPrivilege SeBackupPrivilege SeRestorePrivilege SeDebugPrivilege SeAuditPrivilege SeSystemEnvironmentPrivilege SeImpersonatePrivilege
Security	Audit Success	13824	2015-04-25 16:03:08	Microsoft-Windows-Security-Auditing	4797: An attempt was made to query the existence of a blank password for an account. Subject: Security ID: S-1-5-19 Account Name: LOCAL SERVICE Account Domain: NT AUTHORITY Logon ID: 0x3e5 Additional Information: Caller Workstation: LTRANPHD Target Account Name: Administrator Target Account Domain: LTRANPHD
Security	Audit Success	13824	2015-04-25 16:03:08	Microsoft-Windows-Security-Auditing	4797: An attempt was made to query the existence of a blank password for an account. Subject: Security ID: S-1-5-19 Account Name: LOCAL SERVICE Account Domain: NT AUTHORITY Logon ID: 0x3e5 Additional Information: Caller Workstation: LTRANPHD Target Account Name: Guest Target Account Domain: LTRANPHD
Security	Audit Success	13824	2015-04-25 16:03:08	Microsoft-Windows-Security-Auditing	4797: An attempt was made to query the existence of a blank password for an account. Subject: Security ID: S-1-5-19 Account Name: LOCAL SERVICE Account Domain: NT AUTHORITY Logon ID: 0x3e5 Additional Information: Caller Workstation: LTRANPHD Target Account Name: Administrator Target Account Domain: LTRANPHD
Security	Audit Success	13824	2015-04-25 16:03:08	Microsoft-Windows-Security-Auditing	4797: An attempt was made to query the existence of a blank password for an account. Subject: Security ID: S-1-5-19 Account Name: LOCAL SERVICE Account Domain: NT AUTHORITY Logon ID: 0x3e5 Additional Information: Caller Workstation: LTRANPHD Target Account Name: Liem Target Account Domain: LTRANPHD
Security	Audit Success	13824	2015-04-25 16:03:08	Microsoft-Windows-Security-Auditing	4797: An attempt was made to query the existence of a blank password for an account. Subject: Security ID: S-1-5-19 Account Name: LOCAL SERVICE Account Domain: NT AUTHORITY Logon ID: 0x3e5 Additional Information: Caller Workstation: LTRANPHD Target Account Name: Guest Target Account Domain: LTRANPHD
Security	Audit Success	13824	2015-04-25 16:03:08	Microsoft-Windows-Security-Auditing	4797: An attempt was made to query the existence of a blank password for an account. Subject: Security ID: S-1-5-19 Account Name: LOCAL SERVICE Account Domain: NT AUTHORITY Logon ID: 0x3e5 Additional Information: Caller Workstation: LTRANPHD Target Account Name: Liem Target Account Domain: LTRANPHD
Security	Audit Success	13824	2015-04-25 16:03:08	Microsoft-Windows-Security-Auditing	4797: An attempt was made to query the existence of a blank password for an account. Subject: Security ID: S-1-5-19 Account Name: LOCAL SERVICE Account Domain: NT AUTHORITY Logon ID: 0x3e5 Additional Information: Caller Workstation: LTRANPHD Target Account Name: Liem Target Account Domain: LTRANPHD
Security	Audit Success	13824	2015-04-25 16:03:08	Microsoft-Windows-Security-Auditing	4797: An attempt was made to query the existence of a blank password for an account. Subject: Security ID: S-1-5-19 Account Name: LOCAL SERVICE Account Domain: NT AUTHORITY Logon ID: 0x3e5 Additional Information: Caller Workstation: LTRANPHD Target Account Name: Liem Target Account Domain: LTRANPHD
Security	Audit Success	13824	2015-04-25 16:03:09	Microsoft-Windows-Security-Auditing	4797: An attempt was made to query the existence of a blank password for an account. Subject: Security ID: S-1-5-21-1888849264-3803429180-4108621888-1001 Account Name: Liem Account Domain: LTRANPHD Logon ID: 0x1c271 Additional Information: Caller Workstation: LTRANPHD Target Account Name: Administrator Target Account Domain: LTRANPHD

Security	Audit Success	13824	2015-04-25 16:03:09	Microsoft-Windows-Security-Auditing	4797: An attempt was made to query the existence of a blank password for an account. Subject: Security ID: S-1-5-21-1888849264-3803429180-4108621888-1001 Account Name: Liem Account Domain: LTRANPHD Logon ID: 0x1c271 Additional Information: Caller Workstation: LTRANPHD Target Account Name: Guest Target Account Domain: LTRANPHD
Security	Audit Success	13824	2015-04-25 16:03:09	Microsoft-Windows-Security-Auditing	4797: An attempt was made to query the existence of a blank password for an account. Subject: Security ID: S-1-5-21-1888849264-3803429180-4108621888-1001 Account Name: Liem Account Domain: LTRANPHD Logon ID: 0x1c271 Additional Information: Caller Workstation: LTRANPHD Target Account Name: Administrator Target Account Domain: LTRANPHD
Security	Audit Success	13824	2015-04-25 16:03:09	Microsoft-Windows-Security-Auditing	4797: An attempt was made to query the existence of a blank password for an account. Subject: Security ID: S-1-5-21-1888849264-3803429180-4108621888-1001 Account Name: Liem Account Domain: LTRANPHD Logon ID: 0x1c271 Additional Information: Caller Workstation: LTRANPHD Target Account Name: Guest Target Account Domain: LTRANPHD
Security	Audit Success	12544	2015-04-25 16:13:26	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: LTRANPHD$ Account Domain: WORKGROUP Logon ID: 0x3e7 Logon Type: 5 Impersonation Level: %%1833 New Logon: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Logon ID: 0x3e7 Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x238 Process Name: C:\Windows\System32\services.exe Network Information: Workstation Name: Source Network Address: - Source Port: - Detailed Authentication Information: Logon Process: Advapi Authentication Package: Negotiate Transited Services: - Package Name (NTLM only): - Key Length: 0 This event is generated when a logon session is created. It is generated on the computer that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service such as the Server service, or a local process such as Winlogon.exe or Services.exe. The logon type field indicates the kind of logon that occurred. The most common types are 2 (interactive) and 3 (network). The New Logon fields indicate the account for whom the new logon was created, i.e. the account that was logged on. The network fields indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impersonation level field indicates the extent to which a process in the logon session can impersonate. The authentication information fields provide detailed information about this specific logon request. - Logon GUID is a unique identifier that can be used to correlate this event with a KDC event. - Transited services indicate which intermediate services have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indicates the length of the generated session key. This will be 0 if no session key was requested.
Security	Audit Success	12548	2015-04-25 16:13:26	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Logon ID: 0x3e7 Privileges: SeAssignPrimaryTokenPrivilege SeTcbPrivilege SeSecurityPrivilege SeTakeOwnershipPrivilege SeLoadDriverPrivilege SeBackupPrivilege SeRestorePrivilege SeDebugPrivilege SeAuditPrivilege SeSystemEnvironmentPrivilege SeImpersonatePrivilege
Security	Audit Success	12288	2015-04-25 17:13:20	Microsoft-Windows-Security-Auditing	4608: Windows is starting up. This event is logged when LSASS.EXE starts and the auditing subsystem is initialized.
Security	Audit Success	12544	2015-04-25 17:13:20	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-0-0 Account Name: - Account Domain: - Logon ID: 0x0 Logon Type: 0 Impersonation Level: - New Logon: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Logon ID: 0x3e7 Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x4 Process Name: Network Information: Workstation Name: - Source Network Address: - Source Port: - Detailed Authentication Information: Logon Process: - Authentication Package: - Transited Services: - Package Name (NTLM only): - Key Length: 0 This event is generated when a logon session is created. It is generated on the computer that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service such as the Server service, or a local process such as Winlogon.exe or Services.exe. The logon type field indicates the kind of logon that occurred. The most common types are 2 (interactive) and 3 (network). The New Logon fields indicate the account for whom the new logon was created, i.e. the account that was logged on. The network fields indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impersonation level field indicates the extent to which a process in the logon session can impersonate. The authentication information fields provide detailed information about this specific logon request. - Logon GUID is a unique identifier that can be used to correlate this event with a KDC event. - Transited services indicate which intermediate services have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indicates the length of the generated session key. This will be 0 if no session key was requested.
Security	Audit	12544	2015-04-25	Microsoft-Windows-Security-	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: LTRANPHD$ Account Domain: WORKGROUP Logon ID: 0x3e7 Logon Type: 5 Impersonation Level: %%1833 New Logon: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Logon ID: 0x3e7 Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x234 Process Name: C:\Windows\System32\services.exe Network Information: Workstation Name: Source Network Address: - Source Port: - Detailed Authentication Information: Logon Process: Advapi Authentication Package: Negotiate Transited Services: - Package Name (NTLM only): - Key Length: 0 This event is generated when a logon session is created. It is generated on the computer that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service such as the Server service, or a local process such as Winlogon.exe or Services.exe. The logon type field indicates the kind of logon that occurred.

	Success		17:13:20	Auditing	The most common types are 2 (interactive) and 3 (network). The New Logon fields indicate the account for whom the new logon was created, i.e. the account that was logged on. The network fields indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impersonation level field indicates the extent to which a process in the logon session can impersonate. The authentication information fields provide detailed information about this specific logon request. - Logon GUID is a unique identifier that can be used to correlate this event with a KDC event. - Transited services indicate which intermediate services have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indicates the length of the generated session key. This will be 0 if no session key was requested.
Security	Audit Success	12544	2015-04-25 17:13:20	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: LTRANPHD$ Account Domain: WORKGROUP Logon ID: 0x3e7 Logon Type: 5 Impersonation Level: %%1833 New Logon: Security ID: S-1-5-20 Account Name: NETWORK SERVICE Account Domain: NT AUTHORITY Logon ID: 0x3e4 Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x234 Process Name: C:\Windows\System32\services.exe Network Information: Workstation Name: Source Network Address: - Source Port: - Detailed Authentication Information: Logon Process: Advapi Authentication Package: Negotiate Transited Services: - Package Name (NTLM only): - Key Length: 0 This event is generated when a logon session is created. It is generated on the computer that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service such as the Server service, or a local process such as Winlogon.exe or Services.exe. The logon type field indicates the kind of logon that occurred. The most common types are 2 (interactive) and 3 (network). The New Logon fields indicate the account for whom the new logon was created, i.e. the account that was logged on. The network fields indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impersonation level field indicates the extent to which a process in the logon session can impersonate. The authentication information fields provide detailed information about this specific logon request. - Logon GUID is a unique identifier that can be used to correlate this event with a KDC event. - Transited services indicate which intermediate services have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indicates the length of the generated session key. This will be 0 if no session key was requested.
Security	Audit Success	12544	2015-04-25 17:13:20	Microsoft-Windows-Security-Auditing	4648: A logon was attempted using explicit credentials. Subject: Security ID: S-1-5-18 Account Name: LTRANPHD$ Account Domain: WORKGROUP Logon ID: 0x3e7 Logon GUID: {00000000-0000-0000-0000-000000000000} Account Whose Credentials Were Used: Account Name: DWM-1 Account Domain: Window Manager Logon GUID: {00000000-0000-0000-0000-000000000000} Target Server: Target Server Name: localhost Additional Information: localhost Process Information: Process ID: 0x20c Process Name: C:\Windows\System32\winlogon.exe Network Information: Network Address: - Port: - This event is generated when a process attempts to log on an account by explicitly specifying that account's credentials. This most commonly occurs in batch-type configurations such as scheduled tasks, or when using the RUNAS command.
Security	Audit Success	12544	2015-04-25 17:13:20	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: LTRANPHD$ Account Domain: WORKGROUP Logon ID: 0x3e7 Logon Type: 2 Impersonation Level: %%1833 New Logon: Security ID: S-1-5-90-1 Account Name: DWM-1 Account Domain: Window Manager Logon ID: 0xdfd1 Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x20c Process Name: C:\Windows\System32\winlogon.exe Network Information: Workstation Name: Source Network Address: - Source Port: - Detailed Authentication Information: Logon Process: Advapi Authentication Package: Negotiate Transited Services: - Package Name (NTLM only): - Key Length: 0 This event is generated when a logon session is created. It is generated on the computer that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service such as the Server service, or a local process such as Winlogon.exe or Services.exe. The logon type field indicates the kind of logon that occurred. The most common types are 2 (interactive) and 3 (network). The New Logon fields indicate the account for whom the new logon was created, i.e. the account that was logged on. The network fields indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impersonation level field indicates the extent to which a process in the logon session can impersonate. The authentication information fields provide detailed information about this specific logon request. - Logon GUID is a unique identifier that can be used to correlate this event with a KDC event. - Transited services indicate which intermediate services have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indicates the length of the generated session key. This will be 0 if no session key was requested.
Security	Audit Success	12544	2015-04-25 17:13:20	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: LTRANPHD$ Account Domain: WORKGROUP Logon ID: 0x3e7 Logon Type: 2 Impersonation Level: %%1833 New Logon: Security ID: S-1-5-90-1 Account Name: DWM-1 Account Domain: Window Manager Logon ID: 0xdfe9 Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x20c Process Name: C:\Windows\System32\winlogon.exe Network Information: Workstation Name: Source Network Address: - Source Port: - Detailed Authentication Information: Logon Process: Advapi Authentication Package: Negotiate Transited Services: - Package Name (NTLM only): - Key Length: 0 This event is generated when a logon session is created. It is generated on the computer that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service such as the Server service, or a local process such as Winlogon.exe or Services.exe. The logon type field indicates the kind of logon that occurred. The most common types are 2 (interactive) and 3 (network). The New Logon fields indicate the account for

					whom the new logon was created, i.e. the account that was logged on. The network fields indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impersonation level field indicates the extent to which a process in the logon session can impersonate. The authentication information fields provide detailed information about this specific logon request. - Logon GUID is a unique identifier that can be used to correlate this event with a KDC event. - Transited services indicate which intermediate services have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indicates the length of the generated session key. This will be 0 if no session key was requested.
Security	Audit Success	12544	2015-04-25 17:13:20	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: LTRANPHD$ Account Domain: WORKGROUP Logon ID: 0x3e7 Logon Type: 5 Impersonation Level: %%1833 New Logon: Security ID: S-1-5-19 Account Name: LOCAL SERVICE Account Domain: NT AUTHORITY Logon ID: 0x3e5 Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x234 Process Name: C:\Windows\System32\services.exe Network Information: Workstation Name: Source Network Address: - Source Port: - Detailed Authentication Information: Logon Process: Advapi Authentication Package: Negotiate Transited Services: - Package Name (NTLM only): - Key Length: 0 This event is generated when a logon session is created. It is generated on the computer that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service such as the Server service, or a local process such as Winlogon.exe or Services.exe. The logon type field indicates the kind of logon that occurred. The most common types are 2 (interactive) and 3 (network). The New Logon fields indicate the account for whom the new logon was created, i.e. the account that was logged on. The network fields indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impersonation level field indicates the extent to which a process in the logon session can impersonate. The authentication information fields provide detailed information about this specific logon request. - Logon GUID is a unique identifier that can be used to correlate this event with a KDC event. - Transited services indicate which intermediate services have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indicates the length of the generated session key. This will be 0 if no session key was requested.
Security	Audit Success	12544	2015-04-25 17:13:20	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: LTRANPHD$ Account Domain: WORKGROUP Logon ID: 0x3e7 Logon Type: 5 Impersonation Level: %%1833 New Logon: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Logon ID: 0x3e7 Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x234 Process Name: C:\Windows\System32\services.exe Network Information: Workstation Name: Source Network Address: - Source Port: - Detailed Authentication Information: Logon Process: Advapi Authentication Package: Negotiate Transited Services: - Package Name (NTLM only): - Key Length: 0 This event is generated when a logon session is created. It is generated on the computer that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service such as the Server service, or a local process such as Winlogon.exe or Services.exe. The logon type field indicates the kind of logon that occurred. The most common types are 2 (interactive) and 3 (network). The New Logon fields indicate the account for whom the new logon was created, i.e. the account that was logged on. The network fields indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impersonation level field indicates the extent to which a process in the logon session can impersonate. The authentication information fields provide detailed information about this specific logon request. - Logon GUID is a unique identifier that can be used to correlate this event with a KDC event. - Transited services indicate which intermediate services have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indicates the length of the generated session key. This will be 0 if no session key was requested.
Security	Audit Success	12544	2015-04-25 17:13:20	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: LTRANPHD$ Account Domain: WORKGROUP Logon ID: 0x3e7 Logon Type: 5 Impersonation Level: %%1833 New Logon: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Logon ID: 0x3e7 Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x234 Process Name: C:\Windows\System32\services.exe Network Information: Workstation Name: Source Network Address: - Source Port: - Detailed Authentication Information: Logon Process: Advapi Authentication Package: Negotiate Transited Services: - Package Name (NTLM only): - Key Length: 0 This event is generated when a logon session is created. It is generated on the computer that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service such as the Server service, or a local process such as Winlogon.exe or Services.exe. The logon type field indicates the kind of logon that occurred. The most common types are 2 (interactive) and 3 (network). The New Logon fields indicate the account for whom the new logon was created, i.e. the account that was logged on. The network fields indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impersonation level field indicates the extent to which a process in the logon session can impersonate. The authentication information fields provide detailed information about this specific logon request. - Logon GUID is a unique identifier that can be used to correlate this event with a KDC event. - Transited services indicate which intermediate services have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indicates the length of the generated session key. This will be 0 if no session key was requested.
	Audit		2015-04-	Microsoft-Windows-Security-	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Logon ID: 0x3e7 Privileges: SeAssignPrimaryTokenPrivilege SeTcbPrivilege

Security	Success	12548	25 17:13:20	Auditing	SeSecurityPrivilege SeTakeOwnershipPrivilege SeLoadDriverPrivilege SeBackupPrivilege SeRestorePrivilege SeDebugPrivilege SeAuditPrivilege SeSystemEnvironmentPrivilege SeImpersonatePrivilege
Security	Audit Success	12548	2015-04-25 17:13:20	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-20 Account Name: NETWORK SERVICE Account Domain: NT AUTHORITY Logon ID: 0x3e4 Privileges: SeAssignPrimaryTokenPrivilege SeAuditPrivilege SeImpersonatePrivilege
Security	Audit Success	12548	2015-04-25 17:13:20	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-90-1 Account Name: DWM-1 Account Domain: Window Manager Logon ID: 0xdfd1 Privileges: SeAssignPrimaryTokenPrivilege SeAuditPrivilege SeImpersonatePrivilege
Security	Audit Success	12548	2015-04-25 17:13:20	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-90-1 Account Name: DWM-1 Account Domain: Window Manager Logon ID: 0xdfe9 Privileges: SeAssignPrimaryTokenPrivilege SeAuditPrivilege
Security	Audit Success	12548	2015-04-25 17:13:20	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-19 Account Name: LOCAL SERVICE Account Domain: NT AUTHORITY Logon ID: 0x3e5 Privileges: SeAssignPrimaryTokenPrivilege SeAuditPrivilege SeImpersonatePrivilege
Security	Audit Success	12548	2015-04-25 17:13:20	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Logon ID: 0x3e7 Privileges: SeAssignPrimaryTokenPrivilege SeTcbPrivilege SeSecurityPrivilege SeTakeOwnershipPrivilege SeLoadDriverPrivilege SeBackupPrivilege SeRestorePrivilege SeDebugPrivilege SeAuditPrivilege SeSystemEnvironmentPrivilege SeImpersonatePrivilege
Security	Audit Success	12548	2015-04-25 17:13:20	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Logon ID: 0x3e7 Privileges: SeAssignPrimaryTokenPrivilege SeTcbPrivilege SeSecurityPrivilege SeTakeOwnershipPrivilege SeLoadDriverPrivilege SeBackupPrivilege SeRestorePrivilege SeDebugPrivilege SeAuditPrivilege SeSystemEnvironmentPrivilege SeImpersonatePrivilege
Security	Audit Success	13568	2015-04-25 17:13:20	Microsoft-Windows-Security-Auditing	4902: The Per-user audit policy table was created. Number of Elements: 0 Policy ID: 0x8f89
Security	Audit Success	12544	2015-04-25 17:13:21	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: LTRANPHD$ Account Domain: WORKGROUP Logon ID: 0x3e7 Logon Type: 5 Impersonation Level: %%1833 New Logon: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Logon ID: 0x3e7 Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x234 Process Name: C:\Windows\System32\services.exe Network Information: Workstation Name: Source Network Address: - Source Port: - Detailed Authentication Information: Logon Process: Advapi Authentication Package: Negotiate Transited Services: - Package Name (NTLM only): - Key Length: 0 This event is generated when a logon session is created. It is generated on the computer that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service such as the Server service, or a local process such as Winlogon.exe or Services.exe. The logon type field indicates the kind of logon that occurred. The most common types are 2 (interactive) and 3 (network). The New Logon fields indicate the account for whom the new logon was created, i.e. the account that was logged on. The network fields indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impersonation level field indicates the extent to which a process in the logon session can impersonate. The authentication information fields provide detailed information about this specific logon request. - Logon GUID is a unique identifier that can be used to correlate this event with a KDC event. - Transited services indicate which intermediate services have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indicates the length of the generated session key. This will be 0 if no session key was requested.
Security	Audit Success	12548	2015-04-25 17:13:21	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Logon ID: 0x3e7 Privileges: SeAssignPrimaryTokenPrivilege SeTcbPrivilege SeSecurityPrivilege SeTakeOwnershipPrivilege SeLoadDriverPrivilege SeBackupPrivilege SeRestorePrivilege SeDebugPrivilege SeAuditPrivilege SeSystemEnvironmentPrivilege SeImpersonatePrivilege
Security	Audit Success	12544	2015-04-25 17:13:22	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: LTRANPHD$ Account Domain: WORKGROUP Logon ID: 0x3e7 Logon Type: 5 Impersonation Level: %%1833 New Logon: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Logon ID: 0x3e7 Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x234 Process Name: C:\Windows\System32\services.exe Network Information: Workstation Name: Source Network Address: - Source Port: - Detailed Authentication Information: Logon Process: Advapi Authentication Package: Negotiate Transited Services: - Package Name (NTLM only): - Key Length: 0 This event is generated when a logon session is created. It is generated on the computer that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service such as the Server service, or a local process such as Winlogon.exe or Services.exe. The logon type field indicates the kind of logon that occurred. The most common types are 2 (interactive) and 3 (network). The New Logon fields indicate the account for whom the new logon was created, i.e. the account that was logged on. The network fields indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impersonation level field indicates the extent to which a process in the logon session can impersonate. The authentication information fields provide detailed information about this specific logon request. - Logon GUID is a unique identifier that can be used to correlate this event with a KDC event. - Transited services indicate which intermediate services have participated in this logon request. - Package name indicates

					which sub-protocol was used among the NTLM protocols. - Key length indicates the length of the generated session key. This will be 0 if no session key was requested.
Security	Audit Success	12548	2015-04-25 17:13:22	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Logon ID: 0x3e7 Privileges: SeAssignPrimaryTokenPrivilege SeTcbPrivilege SeSecurityPrivilege SeTakeOwnershipPrivilege SeLoadDriverPrivilege SeBackupPrivilege SeRestorePrivilege SeDebugPrivilege SeAuditPrivilege SeSystemEnvironmentPrivilege SeImpersonatePrivilege
Security	Audit Success	12292	2015-04-25 17:13:23	Microsoft-Windows-Security-Auditing	5033: The Windows Firewall Driver started successfully.
Security	Audit Success	12544	2015-04-25 17:13:23	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: LTRANPHD$ Account Domain: WORKGROUP Logon ID: 0x3e7 Logon Type: 5 Impersonation Level: %%1833 New Logon: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Logon ID: 0x3e7 Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x234 Process Name: C:\Windows\System32\services.exe Network Information: Workstation Name: Source Network Address: - Source Port: - Detailed Authentication Information: Logon Process: Advapi Authentication Package: Negotiate Transited Services: - Package Name (NTLM only): - Key Length: 0 This event is generated when a logon session is created. It is generated on the computer that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service such as the Server service, or a local process such as Winlogon.exe or Services.exe. The logon type field indicates the kind of logon that occurred. The most common types are 2 (interactive) and 3 (network). The New Logon fields indicate the account for whom the new logon was created, i.e. the account that was logged on. The network fields indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impersonation level field indicates the extent to which a process in the logon session can impersonate. The authentication information fields provide detailed information about this specific logon request. - Logon GUID is a unique identifier that can be used to correlate this event with a KDC event. - Transited services indicate which intermediate services have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indicates the length of the generated session key. This will be 0 if no session key was requested.
Security	Audit Success	12548	2015-04-25 17:13:23	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Logon ID: 0x3e7 Privileges: SeAssignPrimaryTokenPrivilege SeTcbPrivilege SeSecurityPrivilege SeTakeOwnershipPrivilege SeLoadDriverPrivilege SeBackupPrivilege SeRestorePrivilege SeDebugPrivilege SeAuditPrivilege SeSystemEnvironmentPrivilege SeImpersonatePrivilege
Security	Audit Success	12292	2015-04-25 17:13:24	Microsoft-Windows-Security-Auditing	5024: The Windows Firewall service started successfully.
Security	Audit Success	12544	2015-04-25 17:13:24	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: LTRANPHD$ Account Domain: WORKGROUP Logon ID: 0x3e7 Logon Type: 5 Impersonation Level: %%1833 New Logon: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Logon ID: 0x3e7 Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x234 Process Name: C:\Windows\System32\services.exe Network Information: Workstation Name: Source Network Address: - Source Port: - Detailed Authentication Information: Logon Process: Advapi Authentication Package: Negotiate Transited Services: - Package Name (NTLM only): - Key Length: 0 This event is generated when a logon session is created. It is generated on the computer that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service such as the Server service, or a local process such as Winlogon.exe or Services.exe. The logon type field indicates the kind of logon that occurred. The most common types are 2 (interactive) and 3 (network). The New Logon fields indicate the account for whom the new logon was created, i.e. the account that was logged on. The network fields indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impersonation level field indicates the extent to which a process in the logon session can impersonate. The authentication information fields provide detailed information about this specific logon request. - Logon GUID is a unique identifier that can be used to correlate this event with a KDC event. - Transited services indicate which intermediate services have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indicates the length of the generated session key. This will be 0 if no session key was requested.
Security	Audit Success	12544	2015-04-25 17:13:24	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-0-0 Account Name: - Account Domain: - Logon ID: 0x0 Logon Type: 3 Impersonation Level: %%1833 New Logon: Security ID: S-1-5-7 Account Name: ANONYMOUS LOGON Account Domain: NT AUTHORITY Logon ID: 0x19dab Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x0 Process Name: - Network Information: Workstation Name: Source Network Address: - Source Port: - Detailed Authentication Information: Logon Process: NtLmSsp Authentication Package: NTLM Transited Services: - Package Name (NTLM only): NTLM V1 Key Length: 0 This event is generated when a logon session is created. It is generated on the computer that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service such as the Server service, or a local process such as Winlogon.exe or Services.exe. The logon type field indicates the kind of logon that occurred. The most common types are 2 (interactive) and 3 (network). The New Logon fields indicate the account for whom the new logon was created, i.e. the account that was logged on. The network fields indicate where a remote logon request originated. Workstation name is

					not always available and may be left blank in some cases. The impersonation level field indicates the extent to which a process in the logon session can impersonate. The authentication information fields provide detailed information about this specific logon request. - Logon GUID is a unique identifier that can be used to correlate this event with a KDC event. - Transited services indicate which intermediate services have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indicates the length of the generated session key. This will be 0 if no session key was requested.
Security	Audit Success	12548	2015-04-25 17:13:24	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Logon ID: 0x3e7 Privileges: SeAssignPrimaryTokenPrivilege SeTcbPrivilege SeSecurityPrivilege SeTakeOwnershipPrivilege SeLoadDriverPrivilege SeBackupPrivilege SeRestorePrivilege SeDebugPrivilege SeAuditPrivilege SeSystemEnvironmentPrivilege SeImpersonatePrivilege
Security	Audit Success	12544	2015-04-25 17:13:34	Microsoft-Windows-Security-Auditing	4648: A logon was attempted using explicit credentials. Subject: Security ID: S-1-5-18 Account Name: LTRANPHD$ Account Domain: WORKGROUP Logon ID: 0x3e7 Logon GUID: {00000000-0000-0000-0000-000000000000} Account Whose Credentials Were Used: Account Name: Liem Account Domain: LTRANPHD Logon GUID: {00000000-0000-0000-0000-000000000000} Target Server: Target Server Name: localhost Additional Information: localhost Process Information: Process ID: 0x20c Process Name: C:\Windows\System32\winlogon.exe Network Information: Network Address: 127.0.0.1 Port: 0 This event is generated when a process attempts to log on an account by explicitly specifying that account's credentials. This most commonly occurs in batch-type configurations such as scheduled tasks, or when using the RUNAS command.
Security	Audit Success	12544	2015-04-25 17:13:34	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: LTRANPHD$ Account Domain: WORKGROUP Logon ID: 0x3e7 Logon Type: 2 Impersonation Level: %%1833 New Logon: Security ID: S-1-5-21-1888849264-3803429180-4108621888-1001 Account Name: Liem Account Domain: LTRANPHD Logon ID: 0x23997 Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x20c Process Name: C:\Windows\System32\winlogon.exe Network Information: Workstation Name: LTRANPHD Source Network Address: 127.0.0.1 Source Port: 0 Detailed Authentication Information: Logon Process: User32 Authentication Package: Negotiate Transited Services: - Package Name (NTLM only): - Key Length: 0 This event is generated when a logon session is created. It is generated on the computer that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service such as the Server service, or a local process such as Winlogon.exe or Services.exe. The logon type field indicates the kind of logon that occurred. The most common types are 2 (interactive) and 3 (network). The New Logon fields indicate the account for whom the new logon was created, i.e. the account that was logged on. The network fields indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impersonation level field indicates the extent to which a process in the logon session can impersonate. The authentication information fields provide detailed information about this specific logon request. - Logon GUID is a unique identifier that can be used to correlate this event with a KDC event. - Transited services indicate which intermediate services have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indicates the length of the generated session key. This will be 0 if no session key was requested.
Security	Audit Success	12544	2015-04-25 17:13:34	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: LTRANPHD$ Account Domain: WORKGROUP Logon ID: 0x3e7 Logon Type: 2 Impersonation Level: %%1833 New Logon: Security ID: S-1-5-21-1888849264-3803429180-4108621888-1001 Account Name: Liem Account Domain: LTRANPHD Logon ID: 0x239f7 Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x20c Process Name: C:\Windows\System32\winlogon.exe Network Information: Workstation Name: LTRANPHD Source Network Address: 127.0.0.1 Source Port: 0 Detailed Authentication Information: Logon Process: User32 Authentication Package: Negotiate Transited Services: - Package Name (NTLM only): - Key Length: 0 This event is generated when a logon session is created. It is generated on the computer that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service such as the Server service, or a local process such as Winlogon.exe or Services.exe. The logon type field indicates the kind of logon that occurred. The most common types are 2 (interactive) and 3 (network). The New Logon fields indicate the account for whom the new logon was created, i.e. the account that was logged on. The network fields indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impersonation level field indicates the extent to which a process in the logon session can impersonate. The authentication information fields provide detailed information about this specific logon request. - Logon GUID is a unique identifier that can be used to correlate this event with a KDC event. - Transited services indicate which intermediate services have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indicates the length of the generated session key. This will be 0 if no session key was requested.
	Audit		2015-04-	Microsoft-Windows-Security-	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: LTRANPHD$ Account Domain: WORKGROUP Logon ID: 0x3e7 Logon Type: 5 Impersonation Level: %%1833 New Logon: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Logon ID: 0x3e7 Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x234 Process Name: C:\Windows\System32\services.exe Network Information: Workstation Name: Source Network Address: - Source Port: - Detailed Authentication Information: Logon Process: Advapi Authentication Package: Negotiate Transited Services: - Package Name (NTLM only): - Key Length: 0 This event is generated when a logon session is created. It is generated on the computer that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service such as the Server service, or a local

Security	Success	12544	25 17:13:34	Auditing	process such as Winlogon.exe or Services.exe. The logon type field indicates the kind of logon that occurred. The most common types are 2 (interactive) and 3 (network). The New Logon fields indicate the account for whom the new logon was created, i.e. the account that was logged on. The network fields indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impersonation level field indicates the extent to which a process in the logon session can impersonate. The authentication information fields provide detailed information about this specific logon request. - Logon GUID is a unique identifier that can be used to correlate this event with a KDC event. - Transited services indicate which intermediate services have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indicates the length of the generated session key. This will be 0 if no session key was requested.
Security	Audit Success	12548	2015-04-25 17:13:34	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-21-1888849264-3803429180-4108621888-1001 Account Name: Liem Account Domain: LTRANPHD Logon ID: 0x23997 Privileges: SeSecurityPrivilege SeTakeOwnershipPrivilege SeLoadDriverPrivilege SeBackupPrivilege SeRestorePrivilege SeDebugPrivilege SeSystemEnvironmentPrivilege SeImpersonatePrivilege
Security	Audit Success	12548	2015-04-25 17:13:34	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Logon ID: 0x3e7 Privileges: SeAssignPrimaryTokenPrivilege SeTcbPrivilege SeSecurityPrivilege SeTakeOwnershipPrivilege SeLoadDriverPrivilege SeBackupPrivilege SeRestorePrivilege SeDebugPrivilege SeAuditPrivilege SeSystemEnvironmentPrivilege SeImpersonatePrivilege
Security	Audit Success	13824	2015-04-25 17:13:35	Microsoft-Windows-Security-Auditing	4797: An attempt was made to query the existence of a blank password for an account. Subject: Security ID: S-1-5-19 Account Name: LOCAL SERVICE Account Domain: NT AUTHORITY Logon ID: 0x3e5 Additional Information: Caller Workstation: LTRANPHD Target Account Name: Administrator Target Account Domain: LTRANPHD
Security	Audit Success	13824	2015-04-25 17:13:35	Microsoft-Windows-Security-Auditing	4797: An attempt was made to query the existence of a blank password for an account. Subject: Security ID: S-1-5-19 Account Name: LOCAL SERVICE Account Domain: NT AUTHORITY Logon ID: 0x3e5 Additional Information: Caller Workstation: LTRANPHD Target Account Name: Guest Target Account Domain: LTRANPHD
Security	Audit Success	13824	2015-04-25 17:13:35	Microsoft-Windows-Security-Auditing	4797: An attempt was made to query the existence of a blank password for an account. Subject: Security ID: S-1-5-19 Account Name: LOCAL SERVICE Account Domain: NT AUTHORITY Logon ID: 0x3e5 Additional Information: Caller Workstation: LTRANPHD Target Account Name: Liem Target Account Domain: LTRANPHD
Security	Audit Success	13824	2015-04-25 17:13:35	Microsoft-Windows-Security-Auditing	4797: An attempt was made to query the existence of a blank password for an account. Subject: Security ID: S-1-5-19 Account Name: LOCAL SERVICE Account Domain: NT AUTHORITY Logon ID: 0x3e5 Additional Information: Caller Workstation: LTRANPHD Target Account Name: Liem Target Account Domain: LTRANPHD
Security	Audit Success	13824	2015-04-25 17:13:35	Microsoft-Windows-Security-Auditing	4797: An attempt was made to query the existence of a blank password for an account. Subject: Security ID: S-1-5-19 Account Name: LOCAL SERVICE Account Domain: NT AUTHORITY Logon ID: 0x3e5 Additional Information: Caller Workstation: LTRANPHD Target Account Name: Administrator Target Account Domain: LTRANPHD
Security	Audit Success	13824	2015-04-25 17:13:35	Microsoft-Windows-Security-Auditing	4797: An attempt was made to query the existence of a blank password for an account. Subject: Security ID: S-1-5-19 Account Name: LOCAL SERVICE Account Domain: NT AUTHORITY Logon ID: 0x3e5 Additional Information: Caller Workstation: LTRANPHD Target Account Name: Guest Target Account Domain: LTRANPHD
Security	Audit Success	13824	2015-04-25 17:13:35	Microsoft-Windows-Security-Auditing	4797: An attempt was made to query the existence of a blank password for an account. Subject: Security ID: S-1-5-19 Account Name: LOCAL SERVICE Account Domain: NT AUTHORITY Logon ID: 0x3e5 Additional Information: Caller Workstation: LTRANPHD Target Account Name: Liem Target Account Domain: LTRANPHD
Security	Audit Success	13824	2015-04-25 17:13:35	Microsoft-Windows-Security-Auditing	4797: An attempt was made to query the existence of a blank password for an account. Subject: Security ID: S-1-5-19 Account Name: LOCAL SERVICE Account Domain: NT AUTHORITY Logon ID: 0x3e5 Additional Information: Caller Workstation: LTRANPHD Target Account Name: Administrator Target Account Domain: LTRANPHD
Security	Audit Success	13824	2015-04-25 17:13:35	Microsoft-Windows-Security-Auditing	4797: An attempt was made to query the existence of a blank password for an account. Subject: Security ID: S-1-5-19 Account Name: LOCAL SERVICE Account Domain: NT AUTHORITY Logon ID: 0x3e5 Additional Information: Caller Workstation: LTRANPHD Target Account Name: Liem Target Account Domain: LTRANPHD
Security	Audit Success	13824	2015-04-25 17:13:35	Microsoft-Windows-Security-Auditing	4797: An attempt was made to query the existence of a blank password for an account. Subject: Security ID: S-1-5-19 Account Name: LOCAL SERVICE Account Domain: NT AUTHORITY Logon ID: 0x3e5 Additional Information: Caller Workstation: LTRANPHD Target Account Name: Administrator Target Account Domain: LTRANPHD
Security	Audit Success	13824	2015-04-25 17:13:35	Microsoft-Windows-Security-Auditing	4797: An attempt was made to query the existence of a blank password for an account. Subject: Security ID: S-1-5-19 Account Name: LOCAL SERVICE Account Domain: NT AUTHORITY Logon ID: 0x3e5 Additional Information: Caller Workstation: LTRANPHD Target Account Name: Guest Target Account Domain: LTRANPHD
Security	Audit Success	13824	2015-04-25 17:13:35	Microsoft-Windows-Security-Auditing	4797: An attempt was made to query the existence of a blank password for an account. Subject: Security ID: S-1-5-19 Account Name: LOCAL SERVICE Account Domain: NT AUTHORITY Logon ID: 0x3e5 Additional Information: Caller Workstation: LTRANPHD Target Account Name: Liem Target Account Domain: LTRANPHD
Security	Audit Success	13824	2015-04-25 17:13:35	Microsoft-Windows-Security-Auditing	4797: An attempt was made to query the existence of a blank password for an account. Subject: Security ID: S-1-5-19 Account Name: LOCAL SERVICE Account Domain: NT AUTHORITY Logon ID: 0x3e5 Additional Information: Caller Workstation: LTRANPHD Target Account Name: Liem Target Account Domain: LTRANPHD
Security	Audit Success	13824	2015-04-25	Microsoft-Windows-Security-Auditing	4797: An attempt was made to query the existence of a blank password for an account. Subject: Security ID: S-1-5-19 Account Name: LOCAL SERVICE Account Domain: NT AUTHORITY Logon ID: 0x3e5 Additional Information: Caller Workstation: LTRANPHD Target Account Name: Administrator Target Account Domain:

			17:13:35		LTRANPHD
Security	Audit Success	13824	2015-04-25 17:13:35	Microsoft-Windows-Security-Auditing	4797: An attempt was made to query the existence of a blank password for an account. Subject: Security ID: S-1-5-19 Account Name: LOCAL SERVICE Account Domain: NT AUTHORITY Logon ID: 0x3e5 Additional Information: Caller Workstation: LTRANPHD Target Account Name: Guest Target Account Domain: LTRANPHD
Security	Audit Success	13824	2015-04-25 17:13:35	Microsoft-Windows-Security-Auditing	4797: An attempt was made to query the existence of a blank password for an account. Subject: Security ID: S-1-5-19 Account Name: LOCAL SERVICE Account Domain: NT AUTHORITY Logon ID: 0x3e5 Additional Information: Caller Workstation: LTRANPHD Target Account Name: Liem Target Account Domain: LTRANPHD
Security	Audit Success	13824	2015-04-25 17:13:35	Microsoft-Windows-Security-Auditing	4797: An attempt was made to query the existence of a blank password for an account. Subject: Security ID: S-1-5-19 Account Name: LOCAL SERVICE Account Domain: NT AUTHORITY Logon ID: 0x3e5 Additional Information: Caller Workstation: LTRANPHD Target Account Name: Liem Target Account Domain: LTRANPHD
Security	Audit Success	13824	2015-04-25 17:13:36	Microsoft-Windows-Security-Auditing	4797: An attempt was made to query the existence of a blank password for an account. Subject: Security ID: S-1-5-21-1888849264-3803429180-4108621888-1001 Account Name: Liem Account Domain: LTRANPHD Logon ID: 0x239f7 Additional Information: Caller Workstation: LTRANPHD Target Account Name: Administrator Target Account Domain: LTRANPHD
Security	Audit Success	13824	2015-04-25 17:13:36	Microsoft-Windows-Security-Auditing	4797: An attempt was made to query the existence of a blank password for an account. Subject: Security ID: S-1-5-21-1888849264-3803429180-4108621888-1001 Account Name: Liem Account Domain: LTRANPHD Logon ID: 0x239f7 Additional Information: Caller Workstation: LTRANPHD Target Account Name: Guest Target Account Domain: LTRANPHD
Security	Audit Success	13824	2015-04-25 17:13:36	Microsoft-Windows-Security-Auditing	4797: An attempt was made to query the existence of a blank password for an account. Subject: Security ID: S-1-5-21-1888849264-3803429180-4108621888-1001 Account Name: Liem Account Domain: LTRANPHD Logon ID: 0x239f7 Additional Information: Caller Workstation: LTRANPHD Target Account Name: Administrator Target Account Domain: LTRANPHD
Security	Audit Success	13824	2015-04-25 17:13:36	Microsoft-Windows-Security-Auditing	4797: An attempt was made to query the existence of a blank password for an account. Subject: Security ID: S-1-5-21-1888849264-3803429180-4108621888-1001 Account Name: Liem Account Domain: LTRANPHD Logon ID: 0x239f7 Additional Information: Caller Workstation: LTRANPHD Target Account Name: Guest Target Account Domain: LTRANPHD
Security	Audit Success	12544	2015-04-25 17:23:30	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: LTRANPHD$ Account Domain: WORKGROUP Logon ID: 0x3e7 Logon Type: 5 Impersonation Level: %%1833 New Logon: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Logon ID: 0x3e7 Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x234 Process Name: C:\Windows\System32\services.exe Network Information: Workstation Name: Source Network Address: - Source Port: - Detailed Authentication Information: Logon Process: Advapi Authentication Package: Negotiate Transited Services: - Package Name (NTLM only): - Key Length: 0 This event is generated when a logon session is created. It is generated on the computer that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service such as the Server service, or a local process such as Winlogon.exe or Services.exe. The logon type field indicates the kind of logon that occurred. The most common types are 2 (interactive) and 3 (network). The New Logon fields indicate the account for whom the new logon was created, i.e. the account that was logged on. The network fields indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impersonation level field indicates the extent to which a process in the logon session can impersonate. The authentication information fields provide detailed information about this specific logon request. - Logon GUID is a unique identifier that can be used to correlate this event with a KDC event. - Transited services indicate which intermediate services have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indicates the length of the generated session key. This will be 0 if no session key was requested.
Security	Audit Success	12548	2015-04-25 17:23:30	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Logon ID: 0x3e7 Privileges: SeAssignPrimaryTokenPrivilege SeTcbPrivilege SeSecurityPrivilege SeTakeOwnershipPrivilege SeLoadDriverPrivilege SeBackupPrivilege SeRestorePrivilege SeDebugPrivilege SeAuditPrivilege SeSystemEnvironmentPrivilege SeImpersonatePrivilege
Security	Audit Success	12288	2015-04-25 17:49:43	Microsoft-Windows-Security-Auditing	4608: Windows is starting up. This event is logged when LSASS.EXE starts and the auditing subsystem is initialized.
Security	Audit Success	12544	2015-04-25 17:49:43	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-0-0 Account Name: - Account Domain: - Logon ID: 0x0 Logon Type: 0 Impersonation Level: - New Logon: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Logon ID: 0x3e7 Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x4 Process Name: Network Information: Workstation Name: - Source Network Address: - Source Port: - Detailed Authentication Information: Logon Process: - Authentication Package: - Transited Services: - Package Name (NTLM only): - Key Length: 0 This event is generated when a logon session is created. It is generated on the computer that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service such as the Server service, or a local process such as Winlogon.exe or Services.exe. The logon type field indicates the kind of logon that occurred. The most common types are 2 (interactive) and 3 (network). The New Logon fields indicate the account for whom the new logon was created, i.e. the account that was logged on. The network fields indicate where a remote logon request originated. Workstation name is not always

					available and may be left blank in some cases. The impersonation level field indicates the extent to which a process in the logon session can impersonate. The authentication information fields provide detailed information about this specific logon request. - Logon GUID is a unique identifier that can be used to correlate this event with a KDC event. - Transited services indicate which intermediate services have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indicates the length of the generated session key. This will be 0 if no session key was requested.
Security	Audit Success	12544	2015-04-25 17:49:43	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: LTRANPHD$ Account Domain: WORKGROUP Logon ID: 0x3e7 Logon Type: 5 Impersonation Level: %%1833 New Logon: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Logon ID: 0x3e7 Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x230 Process Name: C:\Windows\System32\services.exe Network Information: Workstation Name: Source Network Address: - Source Port: - Detailed Authentication Information: Logon Process: Advapi Authentication Package: Negotiate Transited Services: - Package Name (NTLM only): - Key Length: 0 This event is generated when a logon session is created. It is generated on the computer that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service such as the Server service, or a local process such as Winlogon.exe or Services.exe. The logon type field indicates the kind of logon that occurred. The most common types are 2 (interactive) and 3 (network). The New Logon fields indicate the account for whom the new logon was created, i.e. the account that was logged on. The network fields indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impersonation level field indicates the extent to which a process in the logon session can impersonate. The authentication information fields provide detailed information about this specific logon request. - Logon GUID is a unique identifier that can be used to correlate this event with a KDC event. - Transited services indicate which intermediate services have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indicates the length of the generated session key. This will be 0 if no session key was requested.
Security	Audit Success	12544	2015-04-25 17:49:43	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: LTRANPHD$ Account Domain: WORKGROUP Logon ID: 0x3e7 Logon Type: 5 Impersonation Level: %%1833 New Logon: Security ID: S-1-5-20 Account Name: NETWORK SERVICE Account Domain: NT AUTHORITY Logon ID: 0x3e4 Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x230 Process Name: C:\Windows\System32\services.exe Network Information: Workstation Name: Source Network Address: - Source Port: - Detailed Authentication Information: Logon Process: Advapi Authentication Package: Negotiate Transited Services: - Package Name (NTLM only): - Key Length: 0 This event is generated when a logon session is created. It is generated on the computer that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service such as the Server service, or a local process such as Winlogon.exe or Services.exe. The logon type field indicates the kind of logon that occurred. The most common types are 2 (interactive) and 3 (network). The New Logon fields indicate the account for whom the new logon was created, i.e. the account that was logged on. The network fields indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impersonation level field indicates the extent to which a process in the logon session can impersonate. The authentication information fields provide detailed information about this specific logon request. - Logon GUID is a unique identifier that can be used to correlate this event with a KDC event. - Transited services indicate which intermediate services have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indicates the length of the generated session key. This will be 0 if no session key was requested.
Security	Audit Success	12544	2015-04-25 17:49:43	Microsoft-Windows-Security-Auditing	4648: A logon was attempted using explicit credentials. Subject: Security ID: S-1-5-18 Account Name: LTRANPHD$ Account Domain: WORKGROUP Logon ID: 0x3e7 Logon GUID: {00000000-0000-0000-0000-000000000000} Account Whose Credentials Were Used: Account Name: DWM-1 Account Domain: Window Manager Logon GUID: {00000000-0000-0000-0000-000000000000} Target Server: Target Server Name: localhost Additional Information: localhost Process Information: Process ID: 0x208 Process Name: C:\Windows\System32\winlogon.exe Network Information: Network Address: - Port: - This event is generated when a process attempts to log on an account by explicitly specifying that account's credentials. This most commonly occurs in batch-type configurations such as scheduled tasks, or when using the RUNAS command.
Security	Audit Success	12544	2015-04-25 17:49:43	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: LTRANPHD$ Account Domain: WORKGROUP Logon ID: 0x3e7 Logon Type: 2 Impersonation Level: %%1833 New Logon: Security ID: S-1-5-90-1 Account Name: DWM-1 Account Domain: Window Manager Logon ID: 0xf05f Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x208 Process Name: C:\Windows\System32\winlogon.exe Network Information: Workstation Name: Source Network Address: - Source Port: - Detailed Authentication Information: Logon Process: Advapi Authentication Package: Negotiate Transited Services: - Package Name (NTLM only): - Key Length: 0 This event is generated when a logon session is created. It is generated on the computer that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service such as the Server service, or a local process such as Winlogon.exe or Services.exe. The logon type field indicates the kind of logon that occurred. The most common types are 2 (interactive) and 3 (network). The New Logon fields indicate the account for whom the new logon was created, i.e. the account that was logged on. The network fields indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impersonation level field indicates the extent to which a process in the logon session can impersonate. The authentication information fields provide detailed information about this specific logon request.

					- Logon GUID is a unique identifier that can be used to correlate this event with a KDC event. - Transited services indicate which intermediate services have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indicates the length of the generated session key. This will be 0 if no session key was requested.
Security	Audit Success	12544	2015-04-25 17:49:43	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: LTRANPHD$ Account Domain: WORKGROUP Logon ID: 0x3e7 Logon Type: 2 Impersonation Level: %%1833 New Logon: Security ID: S-1-5-90-1 Account Name: DWM-1 Account Domain: Window Manager Logon ID: 0xf079 Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x208 Process Name: C:\Windows\System32\winlogon.exe Network Information: Workstation Name: Source Network Address: - Source Port: - Detailed Authentication Information: Logon Process: Advapi Authentication Package: Negotiate Transited Services: - Package Name (NTLM only): - Key Length: 0 This event is generated when a logon session is created. It is generated on the computer that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service such as the Server service, or a local process such as Winlogon.exe or Services.exe. The logon type field indicates the kind of logon that occurred. The most common types are 2 (interactive) and 3 (network). The New Logon fields indicate the account for whom the new logon was created, i.e. the account that was logged on. The network fields indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impersonation level field indicates the extent to which a process in the logon session can impersonate. The authentication information fields provide detailed information about this specific logon request. - Logon GUID is a unique identifier that can be used to correlate this event with a KDC event. - Transited services indicate which intermediate services have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indicates the length of the generated session key. This will be 0 if no session key was requested.
Security	Audit Success	12544	2015-04-25 17:49:43	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: LTRANPHD$ Account Domain: WORKGROUP Logon ID: 0x3e7 Logon Type: 5 Impersonation Level: %%1833 New Logon: Security ID: S-1-5-19 Account Name: LOCAL SERVICE Account Domain: NT AUTHORITY Logon ID: 0x3e5 Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x230 Process Name: C:\Windows\System32\services.exe Network Information: Workstation Name: Source Network Address: - Source Port: - Detailed Authentication Information: Logon Process: Advapi Authentication Package: Negotiate Transited Services: - Package Name (NTLM only): - Key Length: 0 This event is generated when a logon session is created. It is generated on the computer that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service such as the Server service, or a local process such as Winlogon.exe or Services.exe. The logon type field indicates the kind of logon that occurred. The most common types are 2 (interactive) and 3 (network). The New Logon fields indicate the account for whom the new logon was created, i.e. the account that was logged on. The network fields indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impersonation level field indicates the extent to which a process in the logon session can impersonate. The authentication information fields provide detailed information about this specific logon request. - Logon GUID is a unique identifier that can be used to correlate this event with a KDC event. - Transited services indicate which intermediate services have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indicates the length of the generated session key. This will be 0 if no session key was requested.
Security	Audit Success	12544	2015-04-25 17:49:43	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: LTRANPHD$ Account Domain: WORKGROUP Logon ID: 0x3e7 Logon Type: 5 Impersonation Level: %%1833 New Logon: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Logon ID: 0x3e7 Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x230 Process Name: C:\Windows\System32\services.exe Network Information: Workstation Name: Source Network Address: - Source Port: - Detailed Authentication Information: Logon Process: Advapi Authentication Package: Negotiate Transited Services: - Package Name (NTLM only): - Key Length: 0 This event is generated when a logon session is created. It is generated on the computer that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service such as the Server service, or a local process such as Winlogon.exe or Services.exe. The logon type field indicates the kind of logon that occurred. The most common types are 2 (interactive) and 3 (network). The New Logon fields indicate the account for whom the new logon was created, i.e. the account that was logged on. The network fields indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impersonation level field indicates the extent to which a process in the logon session can impersonate. The authentication information fields provide detailed information about this specific logon request. - Logon GUID is a unique identifier that can be used to correlate this event with a KDC event. - Transited services indicate which intermediate services have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indicates the length of the generated session key. This will be 0 if no session key was requested.
					4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: LTRANPHD$ Account Domain: WORKGROUP Logon ID: 0x3e7 Logon Type: 5 Impersonation Level: %%1833 New Logon: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Logon ID: 0x3e7 Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x230 Process Name: C:\Windows\System32\services.exe Network Information: Workstation Name: Source Network Address: - Source Port: - Detailed Authentication Information: Logon Process: Advapi Authentication Package: Negotiate Transited

Security	Audit Success	12544	2015-04-25 17:49:43		Microsoft-Windows-Security-Auditing	Services: - Package Name (NTLM only): - Key Length: 0 This event is generated when a logon session is created. It is generated on the computer that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service such as the Server service, or a local process such as Winlogon.exe or Services.exe. The logon type field indicates the kind of logon that occurred. The most common types are 2 (interactive) and 3 (network). The New Logon fields indicate the account for whom the new logon was created, i.e. the account that was logged on. The network fields indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impersonation level field indicates the extent to which a process in the logon session can impersonate. The authentication information fields provide detailed information about this specific logon request. - Logon GUID is a unique identifier that can be used to correlate this event with a KDC event. - Transited services indicate which intermediate services have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indicates the length of the generated session key. This will be 0 if no session key was requested.
Security	Audit Success	12544	2015-04-25 17:49:43		Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: LTRANPHD$ Account Domain: WORKGROUP Logon ID: 0x3e7 Logon Type: 5 Impersonation Level: %%1833 New Logon: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Logon ID: 0x3e7 Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x230 Process Name: C:\Windows\System32\services.exe Network Information: Workstation Name: Source Network Address: - Source Port: - Detailed Authentication Information: Logon Process: Advapi Authentication Package: Negotiate Transited Services: - Package Name (NTLM only): - Key Length: 0 This event is generated when a logon session is created. It is generated on the computer that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service such as the Server service, or a local process such as Winlogon.exe or Services.exe. The logon type field indicates the kind of logon that occurred. The most common types are 2 (interactive) and 3 (network). The New Logon fields indicate the account for whom the new logon was created, i.e. the account that was logged on. The network fields indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impersonation level field indicates the extent to which a process in the logon session can impersonate. The authentication information fields provide detailed information about this specific logon request. - Logon GUID is a unique identifier that can be used to correlate this event with a KDC event. - Transited services indicate which intermediate services have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indicates the length of the generated session key. This will be 0 if no session key was requested.
Security	Audit Success	12548	2015-04-25 17:49:43		Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Logon ID: 0x3e7 Privileges: SeAssignPrimaryTokenPrivilege SeTcbPrivilege SeSecurityPrivilege SeTakeOwnershipPrivilege SeLoadDriverPrivilege SeBackupPrivilege SeRestorePrivilege SeDebugPrivilege SeAuditPrivilege SeSystemEnvironmentPrivilege SeImpersonatePrivilege
Security	Audit Success	12548	2015-04-25 17:49:43		Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-20 Account Name: NETWORK SERVICE Account Domain: NT AUTHORITY Logon ID: 0x3e4 Privileges: SeAssignPrimaryTokenPrivilege SeAuditPrivilege SeImpersonatePrivilege
Security	Audit Success	12548	2015-04-25 17:49:43		Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-90-1 Account Name: DWM-1 Account Domain: Window Manager Logon ID: 0xf05f Privileges: SeAssignPrimaryTokenPrivilege SeAuditPrivilege SeImpersonatePrivilege
Security	Audit Success	12548	2015-04-25 17:49:43		Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-90-1 Account Name: DWM-1 Account Domain: Window Manager Logon ID: 0xf079 Privileges: SeAssignPrimaryTokenPrivilege SeAuditPrivilege
Security	Audit Success	12548	2015-04-25 17:49:43		Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-19 Account Name: LOCAL SERVICE Account Domain: NT AUTHORITY Logon ID: 0x3e5 Privileges: SeAssignPrimaryTokenPrivilege SeAuditPrivilege SeImpersonatePrivilege
Security	Audit Success	12548	2015-04-25 17:49:43		Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Logon ID: 0x3e7 Privileges: SeAssignPrimaryTokenPrivilege SeTcbPrivilege SeSecurityPrivilege SeTakeOwnershipPrivilege SeLoadDriverPrivilege SeBackupPrivilege SeRestorePrivilege SeDebugPrivilege SeAuditPrivilege SeSystemEnvironmentPrivilege SeImpersonatePrivilege
Security	Audit Success	12548	2015-04-25 17:49:43		Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Logon ID: 0x3e7 Privileges: SeAssignPrimaryTokenPrivilege SeTcbPrivilege SeSecurityPrivilege SeTakeOwnershipPrivilege SeLoadDriverPrivilege SeBackupPrivilege SeRestorePrivilege SeDebugPrivilege SeAuditPrivilege SeSystemEnvironmentPrivilege SeImpersonatePrivilege
Security	Audit Success	12548	2015-04-25 17:49:43		Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Logon ID: 0x3e7 Privileges: SeAssignPrimaryTokenPrivilege SeTcbPrivilege SeSecurityPrivilege SeTakeOwnershipPrivilege SeLoadDriverPrivilege SeBackupPrivilege SeRestorePrivilege SeDebugPrivilege SeAuditPrivilege SeSystemEnvironmentPrivilege SeImpersonatePrivilege
Security	Audit Success	13568	2015-04-25 17:49:43		Microsoft-Windows-Security-Auditing	4902: The Per-user audit policy table was created. Number of Elements: 0 Policy ID: 0xa045
Security	Audit	12292	2015-04-25		Microsoft-Windows-Security-	5033: The Windows Firewall Driver started successfully.

	Success		17:49:44	Auditing	
Security	Audit Success	12292	2015-04-25 17:49:44	Microsoft-Windows-Security-Auditing	5024: The Windows Firewall service started successfully.
Security	Audit Success	12544	2015-04-25 17:49:44	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: LTRANPHD$ Account Domain: WORKGROUP Logon ID: 0x3e7 Logon Type: 5 Impersonation Level: %%1833 New Logon: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Logon ID: 0x3e7 Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x230 Process Name: C:\Windows\System32\services.exe Network Information: Workstation Name: Source Network Address: - Source Port: - Detailed Authentication Information: Logon Process: Advapi Authentication Package: Negotiate Transited Services: - Package Name (NTLM only): - Key Length: 0 This event is generated when a logon session is created. It is generated on the computer that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service such as the Server service, or a local process such as Winlogon.exe or Services.exe. The logon type field indicates the kind of logon that occurred. The most common types are 2 (interactive) and 3 (network). The New Logon fields indicate the account for whom the new logon was created, i.e. the account that was logged on. The network fields indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impersonation level field indicates the extent to which a process in the logon session can impersonate. The authentication information fields provide detailed information about this specific logon request. - Logon GUID is a unique identifier that can be used to correlate this event with a KDC event. - Transited services indicate which intermediate services have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indicates the length of the generated session key. This will be 0 if no session key was requested.
Security	Audit Success	12544	2015-04-25 17:49:44	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: LTRANPHD$ Account Domain: WORKGROUP Logon ID: 0x3e7 Logon Type: 5 Impersonation Level: %%1833 New Logon: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Logon ID: 0x3e7 Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x230 Process Name: C:\Windows\System32\services.exe Network Information: Workstation Name: Source Network Address: - Source Port: - Detailed Authentication Information: Logon Process: Advapi Authentication Package: Negotiate Transited Services: - Package Name (NTLM only): - Key Length: 0 This event is generated when a logon session is created. It is generated on the computer that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service such as the Server service, or a local process such as Winlogon.exe or Services.exe. The logon type field indicates the kind of logon that occurred. The most common types are 2 (interactive) and 3 (network). The New Logon fields indicate the account for whom the new logon was created, i.e. the account that was logged on. The network fields indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impersonation level field indicates the extent to which a process in the logon session can impersonate. The authentication information fields provide detailed information about this specific logon request. - Logon GUID is a unique identifier that can be used to correlate this event with a KDC event. - Transited services indicate which intermediate services have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indicates the length of the generated session key. This will be 0 if no session key was requested.
Security	Audit Success	12544	2015-04-25 17:49:44	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: LTRANPHD$ Account Domain: WORKGROUP Logon ID: 0x3e7 Logon Type: 5 Impersonation Level: %%1833 New Logon: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Logon ID: 0x3e7 Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x230 Process Name: C:\Windows\System32\services.exe Network Information: Workstation Name: Source Network Address: - Source Port: - Detailed Authentication Information: Logon Process: Advapi Authentication Package: Negotiate Transited Services: - Package Name (NTLM only): - Key Length: 0 This event is generated when a logon session is created. It is generated on the computer that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service such as the Server service, or a local process such as Winlogon.exe or Services.exe. The logon type field indicates the kind of logon that occurred. The most common types are 2 (interactive) and 3 (network). The New Logon fields indicate the account for whom the new logon was created, i.e. the account that was logged on. The network fields indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impersonation level field indicates the extent to which a process in the logon session can impersonate. The authentication information fields provide detailed information about this specific logon request. - Logon GUID is a unique identifier that can be used to correlate this event with a KDC event. - Transited services indicate which intermediate services have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indicates the length of the generated session key. This will be 0 if no session key was requested.
Security	Audit Success	12548	2015-04-25 17:49:44	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Logon ID: 0x3e7 Privileges: SeAssignPrimaryTokenPrivilege SeTcbPrivilege SeSecurityPrivilege SeTakeOwnershipPrivilege SeLoadDriverPrivilege SeBackupPrivilege SeRestorePrivilege SeDebugPrivilege SeAuditPrivilege SeSystemEnvironmentPrivilege SeImpersonatePrivilege
					4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account

Security	Audit Success	12548	2015-04-25 17:49:44	Microsoft-Windows-Security-Auditing	Domain: NT AUTHORITY Logon ID: 0x3e7 Privileges: SeAssignPrimaryTokenPrivilege SeTcbPrivilege SeSecurityPrivilege SeTakeOwnershipPrivilege SeLoadDriverPrivilege SeBackupPrivilege SeRestorePrivilege SeDebugPrivilege SeAuditPrivilege SeSystemEnvironmentPrivilege SeImpersonatePrivilege
Security	Audit Success	12548	2015-04-25 17:49:44	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Logon ID: 0x3e7 Privileges: SeAssignPrimaryTokenPrivilege SeTcbPrivilege SeSecurityPrivilege SeTakeOwnershipPrivilege SeLoadDriverPrivilege SeBackupPrivilege SeRestorePrivilege SeDebugPrivilege SeAuditPrivilege SeSystemEnvironmentPrivilege SeImpersonatePrivilege
Security	Audit Success	12544	2015-04-25 17:49:45	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-0-0 Account Name: - Account Domain: - Logon ID: 0x0 Logon Type: 3 Impersonation Level: %%1833 New Logon: Security ID: S-1-5-7 Account Name: ANONYMOUS LOGON Account Domain: NT AUTHORITY Logon ID: 0x1adee Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x0 Process Name: - Network Information: Workstation Name: Source Network Address: - Source Port: - Detailed Authentication Information: Logon Process: NtLmSsp Authentication Package: NTLM Transited Services: - Package Name (NTLM only): NTLM V1 Key Length: 0 This event is generated when a logon session is created. It is generated on the computer that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service such as the Server service, or a local process such as Winlogon.exe or Services.exe. The logon type field indicates the kind of logon that occurred. The most common types are 2 (interactive) and 3 (network). The New Logon fields indicate the account for whom the new logon was created, i.e. the account that was logged on. The network fields indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impersonation level field indicates the extent to which a process in the logon session can impersonate. The authentication information fields provide detailed information about this specific logon request. - Logon GUID is a unique identifier that can be used to correlate this event with a KDC event. - Transited services indicate which intermediate services have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indicates the length of the generated session key. This will be 0 if no session key was requested.
Security	Audit Success	12544	2015-04-25 17:49:50	Microsoft-Windows-Security-Auditing	4648: A logon was attempted using explicit credentials. Subject: Security ID: S-1-5-18 Account Name: LTRANPHD$ Account Domain: WORKGROUP Logon ID: 0x3e7 Logon GUID: {00000000-0000-0000-0000-000000000000} Account Whose Credentials Were Used: Account Name: Liem Account Domain: LTRANPHD Logon GUID: {00000000-0000-0000-0000-000000000000} Target Server: Target Server Name: localhost Additional Information: localhost Process Information: Process ID: 0x208 Process Name: C:\Windows\System32\winlogon.exe Network Information: Network Address: 127.0.0.1 Port: 0 This event is generated when a process attempts to log on an account by explicitly specifying that account's credentials. This most commonly occurs in batch-type configurations such as scheduled tasks, or when using the RUNAS command.
Security	Audit Success	12544	2015-04-25 17:49:50	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: LTRANPHD$ Account Domain: WORKGROUP Logon ID: 0x3e7 Logon Type: 2 Impersonation Level: %%1833 New Logon: Security ID: S-1-5-21-1888849264-3803429180-4108621888-1001 Account Name: Liem Account Domain: LTRANPHD Logon ID: 0x206d4 Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x208 Process Name: C:\Windows\System32\winlogon.exe Network Information: Workstation Name: LTRANPHD Source Network Address: 127.0.0.1 Source Port: 0 Detailed Authentication Information: Logon Process: User32 Authentication Package: Negotiate Transited Services: - Package Name (NTLM only): - Key Length: 0 This event is generated when a logon session is created. It is generated on the computer that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service such as the Server service, or a local process such as Winlogon.exe or Services.exe. The logon type field indicates the kind of logon that occurred. The most common types are 2 (interactive) and 3 (network). The New Logon fields indicate the account for whom the new logon was created, i.e. the account that was logged on. The network fields indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impersonation level field indicates the extent to which a process in the logon session can impersonate. The authentication information fields provide detailed information about this specific logon request. - Logon GUID is a unique identifier that can be used to correlate this event with a KDC event. - Transited services indicate which intermediate services have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indicates the length of the generated session key. This will be 0 if no session key was requested.
Security	Audit Success	12544	2015-04-25 17:49:50	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: LTRANPHD$ Account Domain: WORKGROUP Logon ID: 0x3e7 Logon Type: 2 Impersonation Level: %%1833 New Logon: Security ID: S-1-5-21-1888849264-3803429180-4108621888-1001 Account Name: Liem Account Domain: LTRANPHD Logon ID: 0x20703 Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x208 Process Name: C:\Windows\System32\winlogon.exe Network Information: Workstation Name: LTRANPHD Source Network Address: 127.0.0.1 Source Port: 0 Detailed Authentication Information: Logon Process: User32 Authentication Package: Negotiate Transited Services: - Package Name (NTLM only): - Key Length: 0 This event is generated when a logon session is created. It is generated on the computer that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service such as the Server service, or a local process such as Winlogon.exe or Services.exe. The logon type field indicates the kind of logon that occurred. The most common types are 2 (interactive) and 3 (network). The New Logon fields indicate the account for whom the new logon was created, i.e. the account that was logged on. The network fields indicate where a remote logon request originated. Workstation name is

					not always available and may be left blank in some cases. The impersonation level field indicates the extent to which a process in the logon session can impersonate. The authentication information fields provide detailed information about this specific logon request. - Logon GUID is a unique identifier that can be used to correlate this event with a KDC event. - Transited services indicate which intermediate services have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indicates the length of the generated session key. This will be 0 if no session key was requested.
Security	Audit Success	12544	2015-04-25 17:49:50	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: LTRANPHD$ Account Domain: WORKGROUP Logon ID: 0x3e7 Logon Type: 5 Impersonation Level: %%1833 New Logon: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Logon ID: 0x3e7 Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x230 Process Name: C:\Windows\System32\services.exe Network Information: Workstation Name: Source Network Address: - Source Port: - Detailed Authentication Information: Logon Process: Advapi Authentication Package: Negotiate Transited Services: - Package Name (NTLM only): - Key Length: 0 This event is generated when a logon session is created. It is generated on the computer that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service such as the Server service, or a local process such as Winlogon.exe or Services.exe. The logon type field indicates the kind of logon that occurred. The most common types are 2 (interactive) and 3 (network). The New Logon fields indicate the account for whom the new logon was created, i.e. the account that was logged on. The network fields indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impersonation level field indicates the extent to which a process in the logon session can impersonate. The authentication information fields provide detailed information about this specific logon request. - Logon GUID is a unique identifier that can be used to correlate this event with a KDC event. - Transited services indicate which intermediate services have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indicates the length of the generated session key. This will be 0 if no session key was requested.
Security	Audit Success	12548	2015-04-25 17:49:50	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-21-1888849264-3803429180-4108621888-1001 Account Name: Liem Account Domain: LTRANPHD Logon ID: 0x206d4 Privileges: SeSecurityPrivilege SeTakeOwnershipPrivilege SeLoadDriverPrivilege SeBackupPrivilege SeRestorePrivilege SeDebugPrivilege SeSystemEnvironmentPrivilege SeImpersonatePrivilege
Security	Audit Success	12548	2015-04-25 17:49:50	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Logon ID: 0x3e7 Privileges: SeAssignPrimaryTokenPrivilege SeTcbPrivilege SeSecurityPrivilege SeTakeOwnershipPrivilege SeLoadDriverPrivilege SeBackupPrivilege SeRestorePrivilege SeDebugPrivilege SeAuditPrivilege SeSystemEnvironmentPrivilege SeImpersonatePrivilege
Security	Audit Success	13824	2015-04-25 17:49:52	Microsoft-Windows-Security-Auditing	4797: An attempt was made to query the existence of a blank password for an account. Subject: Security ID: S-1-5-21-1888849264-3803429180-4108621888-1001 Account Name: Liem Account Domain: LTRANPHD Logon ID: 0x20703 Additional Information: Caller Workstation: LTRANPHD Target Account Name: Administrator Target Account Domain: LTRANPHD
Security	Audit Success	13824	2015-04-25 17:49:52	Microsoft-Windows-Security-Auditing	4797: An attempt was made to query the existence of a blank password for an account. Subject: Security ID: S-1-5-21-1888849264-3803429180-4108621888-1001 Account Name: Liem Account Domain: LTRANPHD Logon ID: 0x20703 Additional Information: Caller Workstation: LTRANPHD Target Account Name: Guest Target Account Domain: LTRANPHD
Security	Audit Success	13824	2015-04-25 17:49:52	Microsoft-Windows-Security-Auditing	4797: An attempt was made to query the existence of a blank password for an account. Subject: Security ID: S-1-5-21-1888849264-3803429180-4108621888-1001 Account Name: Liem Account Domain: LTRANPHD Logon ID: 0x20703 Additional Information: Caller Workstation: LTRANPHD Target Account Name: Administrator Target Account Domain: LTRANPHD
Security	Audit Success	13824	2015-04-25 17:49:52	Microsoft-Windows-Security-Auditing	4797: An attempt was made to query the existence of a blank password for an account. Subject: Security ID: S-1-5-21-1888849264-3803429180-4108621888-1001 Account Name: Liem Account Domain: LTRANPHD Logon ID: 0x20703 Additional Information: Caller Workstation: LTRANPHD Target Account Name: Guest Target Account Domain: LTRANPHD
Security	Audit Success	13824	2015-04-25 17:49:53	Microsoft-Windows-Security-Auditing	4797: An attempt was made to query the existence of a blank password for an account. Subject: Security ID: S-1-5-19 Account Name: LOCAL SERVICE Account Domain: NT AUTHORITY Logon ID: 0x3e5 Additional Information: Caller Workstation: LTRANPHD Target Account Name: Administrator Target Account Domain: LTRANPHD
Security	Audit Success	13824	2015-04-25 17:49:53	Microsoft-Windows-Security-Auditing	4797: An attempt was made to query the existence of a blank password for an account. Subject: Security ID: S-1-5-19 Account Name: LOCAL SERVICE Account Domain: NT AUTHORITY Logon ID: 0x3e5 Additional Information: Caller Workstation: LTRANPHD Target Account Name: Administrator Target Account Domain: LTRANPHD
Security	Audit Success	13824	2015-04-25 17:49:53	Microsoft-Windows-Security-Auditing	4797: An attempt was made to query the existence of a blank password for an account. Subject: Security ID: S-1-5-19 Account Name: LOCAL SERVICE Account Domain: NT AUTHORITY Logon ID: 0x3e5 Additional Information: Caller Workstation: LTRANPHD Target Account Name: Guest Target Account Domain: LTRANPHD
Security	Audit Success	13824	2015-04-25 17:49:53	Microsoft-Windows-Security-Auditing	4797: An attempt was made to query the existence of a blank password for an account. Subject: Security ID: S-1-5-19 Account Name: LOCAL SERVICE Account Domain: NT AUTHORITY Logon ID: 0x3e5 Additional Information: Caller Workstation: LTRANPHD Target Account Name: Guest Target Account Domain: LTRANPHD
Security	Audit	13824	2015-04-25	Microsoft-Windows-Security-	4797: An attempt was made to query the existence of a blank password for an account. Subject: Security ID: S-1-5-19 Account Name: LOCAL SERVICE Account Domain: NT AUTHORITY Logon ID: 0x3e5 Additional

	Success		17:49:53	Auditing	Information: Caller Workstation: LTRANPHD Target Account Name: Liem Target Account Domain: LTRANPHD
Security	Audit Success	13824	2015-04-25 17:49:53	Microsoft-Windows-Security-Auditing	4797: An attempt was made to query the existence of a blank password for an account. Subject: Security ID: S-1-5-19 Account Name: LOCAL SERVICE Account Domain: NT AUTHORITY Logon ID: 0x3e5 Additional Information: Caller Workstation: LTRANPHD Target Account Name: Liem Target Account Domain: LTRANPHD
Security	Audit Success	13824	2015-04-25 17:49:53	Microsoft-Windows-Security-Auditing	4797: An attempt was made to query the existence of a blank password for an account. Subject: Security ID: S-1-5-19 Account Name: LOCAL SERVICE Account Domain: NT AUTHORITY Logon ID: 0x3e5 Additional Information: Caller Workstation: LTRANPHD Target Account Name: Liem Target Account Domain: LTRANPHD
Security	Audit Success	13824	2015-04-25 17:49:53	Microsoft-Windows-Security-Auditing	4797: An attempt was made to query the existence of a blank password for an account. Subject: Security ID: S-1-5-19 Account Name: LOCAL SERVICE Account Domain: NT AUTHORITY Logon ID: 0x3e5 Additional Information: Caller Workstation: LTRANPHD Target Account Name: Liem Target Account Domain: LTRANPHD
Security	Audit Success	12544	2015-04-25 17:59:50	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: LTRANPHD$ Account Domain: WORKGROUP Logon ID: 0x3e7 Logon Type: 5 Impersonation Level: %%1833 New Logon: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Logon ID: 0x3e7 Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x230 Process Name: C:\Windows\System32\services.exe Network Information: Workstation Name: Source Network Address: - Source Port: - Detailed Authentication Information: Logon Process: Advapi Authentication Package: Negotiate Transited Services: - Package Name (NTLM only): - Key Length: 0 This event is generated when a logon session is created. It is generated on the computer that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service such as the Server service, or a local process such as Winlogon.exe or Services.exe. The logon type field indicates the kind of logon that occurred. The most common types are 2 (interactive) and 3 (network). The New Logon fields indicate the account for whom the new logon was created, i.e. the account that was logged on. The network fields indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impersonation level field indicates the extent to which a process in the logon session can impersonate. The authentication information fields provide detailed information about this specific logon request. - Logon GUID is a unique identifier that can be used to correlate this event with a KDC event. - Transited services indicate which intermediate services have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indicates the length of the generated session key. This will be 0 if no session key was requested.
Security	Audit Success	12548	2015-04-25 17:59:50	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Logon ID: 0x3e7 Privileges: SeAssignPrimaryTokenPrivilege SeTcbPrivilege SeSecurityPrivilege SeTakeOwnershipPrivilege SeLoadDriverPrivilege SeBackupPrivilege SeRestorePrivilege SeDebugPrivilege SeAuditPrivilege SeSystemEnvironmentPrivilege SeImpersonatePrivilege
Security	Audit Success	12544	2015-04-25 17:59:51	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: LTRANPHD$ Account Domain: WORKGROUP Logon ID: 0x3e7 Logon Type: 5 Impersonation Level: %%1833 New Logon: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Logon ID: 0x3e7 Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x230 Process Name: C:\Windows\System32\services.exe Network Information: Workstation Name: Source Network Address: - Source Port: - Detailed Authentication Information: Logon Process: Advapi Authentication Package: Negotiate Transited Services: - Package Name (NTLM only): - Key Length: 0 This event is generated when a logon session is created. It is generated on the computer that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service such as the Server service, or a local process such as Winlogon.exe or Services.exe. The logon type field indicates the kind of logon that occurred. The most common types are 2 (interactive) and 3 (network). The New Logon fields indicate the account for whom the new logon was created, i.e. the account that was logged on. The network fields indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impersonation level field indicates the extent to which a process in the logon session can impersonate. The authentication information fields provide detailed information about this specific logon request. - Logon GUID is a unique identifier that can be used to correlate this event with a KDC event. - Transited services indicate which intermediate services have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indicates the length of the generated session key. This will be 0 if no session key was requested.
Security	Audit Success	12548	2015-04-25 17:59:51	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Logon ID: 0x3e7 Privileges: SeAssignPrimaryTokenPrivilege SeTcbPrivilege SeSecurityPrivilege SeTakeOwnershipPrivilege SeLoadDriverPrivilege SeBackupPrivilege SeRestorePrivilege SeDebugPrivilege SeAuditPrivilege SeSystemEnvironmentPrivilege SeImpersonatePrivilege
	Audit		2015-04-	Microsoft-Windows-Security-	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: LTRANPHD$ Account Domain: WORKGROUP Logon ID: 0x3e7 Logon Type: 5 Impersonation Level: %%1833 New Logon: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Logon ID: 0x3e7 Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x230 Process Name: C:\Windows\System32\services.exe Network Information: Workstation Name: Source Network Address: - Source Port: - Detailed Authentication Information: Logon Process: Advapi Authentication Package: Negotiate Transited Services: - Package Name (NTLM only): - Key Length: 0 This event is generated when a logon session is created. It is generated on the computer that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service such as the Server service, or a local

Security	Success	12544	25 18:18:46	Auditing	process such as Winlogon.exe or Services.exe. The logon type field indicates the kind of logon that occurred. The most common types are 2 (interactive) and 3 (network). The New Logon fields indicate the account for whom the new logon was created, i.e. the account that was logged on. The network fields indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impersonation level field indicates the extent to which a process in the logon session can impersonate. The authentication information fields provide detailed information about this specific logon request. - Logon GUID is a unique identifier that can be used to correlate this event with a KDC event. - Transited services indicate which intermediate services have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indicates the length of the generated session key. This will be 0 if no session key was requested.
Security	Audit Success	12548	2015-04-25 18:18:46	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Logon ID: 0x3e7 Privileges: SeAssignPrimaryTokenPrivilege SeTcbPrivilege SeSecurityPrivilege SeTakeOwnershipPrivilege SeLoadDriverPrivilege SeBackupPrivilege SeRestorePrivilege SeDebugPrivilege SeAuditPrivilege SeSystemEnvironmentPrivilege SeImpersonatePrivilege
Security	Audit Success	12544	2015-04-25 18:18:47	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: LTRANPHD$ Account Domain: WORKGROUP Logon ID: 0x3e7 Logon Type: 5 Impersonation Level: %%1833 New Logon: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Logon ID: 0x3e7 Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x230 Process Name: C:\Windows\System32\services.exe Network Information: Workstation Name: Source Network Address: - Source Port: - Detailed Authentication Information: Logon Process: Advapi Authentication Package: Negotiate Transited Services: - Package Name (NTLM only): - Key Length: 0 This event is generated when a logon session is created. It is generated on the computer that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service such as the Server service, or a local process such as Winlogon.exe or Services.exe. The logon type field indicates the kind of logon that occurred. The most common types are 2 (interactive) and 3 (network). The New Logon fields indicate the account for whom the new logon was created, i.e. the account that was logged on. The network fields indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impersonation level field indicates the extent to which a process in the logon session can impersonate. The authentication information fields provide detailed information about this specific logon request. - Logon GUID is a unique identifier that can be used to correlate this event with a KDC event. - Transited services indicate which intermediate services have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indicates the length of the generated session key. This will be 0 if no session key was requested.
Security	Audit Success	12548	2015-04-25 18:18:47	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Logon ID: 0x3e7 Privileges: SeAssignPrimaryTokenPrivilege SeTcbPrivilege SeSecurityPrivilege SeTakeOwnershipPrivilege SeLoadDriverPrivilege SeBackupPrivilege SeRestorePrivilege SeDebugPrivilege SeAuditPrivilege SeSystemEnvironmentPrivilege SeImpersonatePrivilege
Security	Audit Success	12288	2015-04-26 08:56:23	Microsoft-Windows-Security-Auditing	4608: Windows is starting up. This event is logged when LSASS.EXE starts and the auditing subsystem is initialized.
Security	Audit Success	12544	2015-04-26 08:56:23	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-0-0 Account Name: - Account Domain: - Logon ID: 0x0 Logon Type: 0 Impersonation Level: - New Logon: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Logon ID: 0x3e7 Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x4 Process Name: Network Information: Workstation Name: - Source Network Address: - Source Port: - Detailed Authentication Information: Logon Process: - Authentication Package: - Transited Services: - Package Name (NTLM only): - Key Length: 0 This event is generated when a logon session is created. It is generated on the computer that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service such as the Server service, or a local process such as Winlogon.exe or Services.exe. The logon type field indicates the kind of logon that occurred. The most common types are 2 (interactive) and 3 (network). The New Logon fields indicate the account for whom the new logon was created, i.e. the account that was logged on. The network fields indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impersonation level field indicates the extent to which a process in the logon session can impersonate. The authentication information fields provide detailed information about this specific logon request. - Logon GUID is a unique identifier that can be used to correlate this event with a KDC event. - Transited services indicate which intermediate services have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indicates the length of the generated session key. This will be 0 if no session key was requested.
					4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: LTRANPHD$ Account Domain: WORKGROUP Logon ID: 0x3e7 Logon Type: 5 Impersonation Level: %%1833 New Logon: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Logon ID: 0x3e7 Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x230 Process Name: C:\Windows\System32\services.exe Network Information: Workstation Name: Source Network Address: - Source Port: - Detailed Authentication Information: Logon Process: Advapi Authentication Package: Negotiate Transited Services: - Package Name (NTLM only): - Key Length: 0 This event is generated when a logon session is created. It is generated on the computer that was accessed. The subject fields indicate the account on the local

Security	Audit Success	12544	2015-04-26 08:56:23	Microsoft-Windows-Security-Auditing	system which requested the logon. This is most commonly a service such as the Server service, or a local process such as Winlogon.exe or Services.exe. The logon type field indicates the kind of logon that occurred. The most common types are 2 (interactive) and 3 (network). The New Logon fields indicate the account for whom the new logon was created, i.e. the account that was logged on. The network fields indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impersonation level field indicates the extent to which a process in the logon session can impersonate. The authentication information fields provide detailed information about this specific logon request. - Logon GUID is a unique identifier that can be used to correlate this event with a KDC event. - Transited services indicate which intermediate services have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indicates the length of the generated session key. This will be 0 if no session key was requested.
Security	Audit Success	12544	2015-04-26 08:56:23	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: LTRANPHD$ Account Domain: WORKGROUP Logon ID: 0x3e7 Logon Type: 5 Impersonation Level: %%1833 New Logon: Security ID: S-1-5-20 Account Name: NETWORK SERVICE Account Domain: NT AUTHORITY Logon ID: 0x3e4 Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x230 Process Name: C:\Windows\System32\services.exe Network Information: Workstation Name: Source Network Address: - Source Port: - Detailed Authentication Information: Logon Process: Advapi Authentication Package: Negotiate Transited Services: - Package Name (NTLM only): - Key Length: 0 This event is generated when a logon session is created. It is generated on the computer that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service such as the Server service, or a local process such as Winlogon.exe or Services.exe. The logon type field indicates the kind of logon that occurred. The most common types are 2 (interactive) and 3 (network). The New Logon fields indicate the account for whom the new logon was created, i.e. the account that was logged on. The network fields indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impersonation level field indicates the extent to which a process in the logon session can impersonate. The authentication information fields provide detailed information about this specific logon request. - Logon GUID is a unique identifier that can be used to correlate this event with a KDC event. - Transited services indicate which intermediate services have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indicates the length of the generated session key. This will be 0 if no session key was requested.
Security	Audit Success	12544	2015-04-26 08:56:23	Microsoft-Windows-Security-Auditing	4648: A logon was attempted using explicit credentials. Subject: Security ID: S-1-5-18 Account Name: LTRANPHD$ Account Domain: WORKGROUP Logon ID: 0x3e7 Logon GUID: {00000000-0000-0000-0000-000000000000} Account Whose Credentials Were Used: Account Name: DWM-1 Account Domain: Window Manager Logon GUID: {00000000-0000-0000-0000-000000000000} Target Server: Target Server Name: localhost Additional Information: localhost Process Information: Process ID: 0x204 Process Name: C:\Windows\System32\winlogon.exe Network Information: Network Address: - Port: - This event is generated when a process attempts to log on an account by explicitly specifying that account's credentials. This most commonly occurs in batch-type configurations such as scheduled tasks, or when using the RUNAS command.
Security	Audit Success	12544	2015-04-26 08:56:23	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: LTRANPHD$ Account Domain: WORKGROUP Logon ID: 0x3e7 Logon Type: 2 Impersonation Level: %%1833 New Logon: Security ID: S-1-5-90-1 Account Name: DWM-1 Account Domain: Window Manager Logon ID: 0xdee4 Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x204 Process Name: C:\Windows\System32\winlogon.exe Network Information: Workstation Name: Source Network Address: - Source Port: - Detailed Authentication Information: Logon Process: Advapi Authentication Package: Negotiate Transited Services: - Package Name (NTLM only): - Key Length: 0 This event is generated when a logon session is created. It is generated on the computer that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service such as the Server service, or a local process such as Winlogon.exe or Services.exe. The logon type field indicates the kind of logon that occurred. The most common types are 2 (interactive) and 3 (network). The New Logon fields indicate the account for whom the new logon was created, i.e. the account that was logged on. The network fields indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impersonation level field indicates the extent to which a process in the logon session can impersonate. The authentication information fields provide detailed information about this specific logon request. - Logon GUID is a unique identifier that can be used to correlate this event with a KDC event. - Transited services indicate which intermediate services have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indicates the length of the generated session key. This will be 0 if no session key was requested.
Security	Audit	12544	2015-04-26	Microsoft-Windows-Security-	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: LTRANPHD$ Account Domain: WORKGROUP Logon ID: 0x3e7 Logon Type: 2 Impersonation Level: %%1833 New Logon: Security ID: S-1-5-90-1 Account Name: DWM-1 Account Domain: Window Manager Logon ID: 0xdefe Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x204 Process Name: C:\Windows\System32\winlogon.exe Network Information: Workstation Name: Source Network Address: - Source Port: - Detailed Authentication Information: Logon Process: Advapi Authentication Package: Negotiate Transited Services: - Package Name (NTLM only): - Key Length: 0 This event is generated when a logon session is created. It is generated on the computer that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service such as the Server service, or a local process such as Winlogon.exe or Services.exe. The logon type field indicates the kind of logon that occurred.

	Success		08:56:23	Auditing	The most common types are 2 (interactive) and 3 (network). The New Logon fields indicate the account for whom the new logon was created, i.e. the account that was logged on. The network fields indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impersonation level field indicates the extent to which a process in the logon session can impersonate. The authentication information fields provide detailed information about this specific logon request. - Logon GUID is a unique identifier that can be used to correlate this event with a KDC event. - Transited services indicate which intermediate services have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indicates the length of the generated session key. This will be 0 if no session key was requested.
Security	Audit Success	12544	2015-04-26 08:56:23	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: LTRANPHD$ Account Domain: WORKGROUP Logon ID: 0x3e7 Logon Type: 5 Impersonation Level: %%1833 New Logon: Security ID: S-1-5-19 Account Name: LOCAL SERVICE Account Domain: NT AUTHORITY Logon ID: 0x3e5 Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x230 Process Name: C:\Windows\System32\services.exe Network Information: Workstation Name: Source Network Address: - Source Port: - Detailed Authentication Information: Logon Process: Advapi Authentication Package: Negotiate Transited Services: - Package Name (NTLM only): - Key Length: 0 This event is generated when a logon session is created. It is generated on the computer that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service such as the Server service, or a local process such as Winlogon.exe or Services.exe. The logon type field indicates the kind of logon that occurred. The most common types are 2 (interactive) and 3 (network). The New Logon fields indicate the account for whom the new logon was created, i.e. the account that was logged on. The network fields indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impersonation level field indicates the extent to which a process in the logon session can impersonate. The authentication information fields provide detailed information about this specific logon request. - Logon GUID is a unique identifier that can be used to correlate this event with a KDC event. - Transited services indicate which intermediate services have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indicates the length of the generated session key. This will be 0 if no session key was requested.
Security	Audit Success	12548	2015-04-26 08:56:23	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Logon ID: 0x3e7 Privileges: SeAssignPrimaryTokenPrivilege SeTcbPrivilege SeSecurityPrivilege SeTakeOwnershipPrivilege SeLoadDriverPrivilege SeBackupPrivilege SeRestorePrivilege SeDebugPrivilege SeAuditPrivilege SeSystemEnvironmentPrivilege SeImpersonatePrivilege
Security	Audit Success	12548	2015-04-26 08:56:23	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-20 Account Name: NETWORK SERVICE Account Domain: NT AUTHORITY Logon ID: 0x3e4 Privileges: SeAssignPrimaryTokenPrivilege SeAuditPrivilege SeImpersonatePrivilege
Security	Audit Success	12548	2015-04-26 08:56:23	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-90-1 Account Name: DWM-1 Account Domain: Window Manager Logon ID: 0xdee4 Privileges: SeAssignPrimaryTokenPrivilege SeAuditPrivilege SeImpersonatePrivilege
Security	Audit Success	12548	2015-04-26 08:56:23	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-90-1 Account Name: DWM-1 Account Domain: Window Manager Logon ID: 0xdefe Privileges: SeAssignPrimaryTokenPrivilege SeAuditPrivilege
Security	Audit Success	12548	2015-04-26 08:56:23	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-19 Account Name: LOCAL SERVICE Account Domain: NT AUTHORITY Logon ID: 0x3e5 Privileges: SeAssignPrimaryTokenPrivilege SeAuditPrivilege SeImpersonatePrivilege
Security	Audit Success	13568	2015-04-26 08:56:23	Microsoft-Windows-Security-Auditing	4902: The Per-user audit policy table was created. Number of Elements: 0 Policy ID: 0x8dba
Security	Audit Success	12544	2015-04-26 08:56:24	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: LTRANPHD$ Account Domain: WORKGROUP Logon ID: 0x3e7 Logon Type: 5 Impersonation Level: %%1833 New Logon: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Logon ID: 0x3e7 Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x230 Process Name: C:\Windows\System32\services.exe Network Information: Workstation Name: Source Network Address: - Source Port: - Detailed Authentication Information: Logon Process: Advapi Authentication Package: Negotiate Transited Services: - Package Name (NTLM only): - Key Length: 0 This event is generated when a logon session is created. It is generated on the computer that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service such as the Server service, or a local process such as Winlogon.exe or Services.exe. The logon type field indicates the kind of logon that occurred. The most common types are 2 (interactive) and 3 (network). The New Logon fields indicate the account for whom the new logon was created, i.e. the account that was logged on. The network fields indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impersonation level field indicates the extent to which a process in the logon session can impersonate. The authentication information fields provide detailed information about this specific logon request. - Logon GUID is a unique identifier that can be used to correlate this event with a KDC event. - Transited services indicate which intermediate services have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indicates the length of the generated

					session key. This will be 0 if no session key was requested.
Security	Audit Success	12544	2015-04-26 08:56:24	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: LTRANPHD$ Account Domain: WORKGROUP Logon ID: 0x3e7 Logon Type: 5 Impersonation Level: %%1833 New Logon: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Logon ID: 0x3e7 Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x230 Process Name: C:\Windows\System32\services.exe Network Information: Workstation Name: Source Network Address: - Source Port: - Detailed Authentication Information: Logon Process: Advapi Authentication Package: Negotiate Transited Services: - Package Name (NTLM only): - Key Length: 0 This event is generated when a logon session is created. It is generated on the computer that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service such as the Server service, or a local process such as Winlogon.exe or Services.exe. The logon type field indicates the kind of logon that occurred. The most common types are 2 (interactive) and 3 (network). The New Logon fields indicate the account for whom the new logon was created, i.e. the account that was logged on. The network fields indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impersonation level field indicates the extent to which a process in the logon session can impersonate. The authentication information fields provide detailed information about this specific logon request. - Logon GUID is a unique identifier that can be used to correlate this event with a KDC event. - Transited services indicate which intermediate services have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indicates the length of the generated session key. This will be 0 if no session key was requested.
Security	Audit Success	12548	2015-04-26 08:56:24	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Logon ID: 0x3e7 Privileges: SeAssignPrimaryTokenPrivilege SeTcbPrivilege SeSecurityPrivilege SeTakeOwnershipPrivilege SeLoadDriverPrivilege SeBackupPrivilege SeRestorePrivilege SeDebugPrivilege SeAuditPrivilege SeSystemEnvironmentPrivilege SeImpersonatePrivilege
Security	Audit Success	12548	2015-04-26 08:56:24	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Logon ID: 0x3e7 Privileges: SeAssignPrimaryTokenPrivilege SeTcbPrivilege SeSecurityPrivilege SeTakeOwnershipPrivilege SeLoadDriverPrivilege SeBackupPrivilege SeRestorePrivilege SeDebugPrivilege SeAuditPrivilege SeSystemEnvironmentPrivilege SeImpersonatePrivilege
Security	Audit Success	101	2015-04-26 08:56:26	Microsoft-Windows-Eventlog	1101: Audit events have been dropped by the transport. 0
Security	Audit Success	12292	2015-04-26 08:56:26	Microsoft-Windows-Security-Auditing	5033: The Windows Firewall Driver started successfully.
Security	Audit Success	12292	2015-04-26 08:56:26	Microsoft-Windows-Security-Auditing	5024: The Windows Firewall service started successfully.
Security	Audit Success	12544	2015-04-26 08:56:26	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: LTRANPHD$ Account Domain: WORKGROUP Logon ID: 0x3e7 Logon Type: 5 Impersonation Level: %%1833 New Logon: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Logon ID: 0x3e7 Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x230 Process Name: C:\Windows\System32\services.exe Network Information: Workstation Name: Source Network Address: - Source Port: - Detailed Authentication Information: Logon Process: Advapi Authentication Package: Negotiate Transited Services: - Package Name (NTLM only): - Key Length: 0 This event is generated when a logon session is created. It is generated on the computer that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service such as the Server service, or a local process such as Winlogon.exe or Services.exe. The logon type field indicates the kind of logon that occurred. The most common types are 2 (interactive) and 3 (network). The New Logon fields indicate the account for whom the new logon was created, i.e. the account that was logged on. The network fields indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impersonation level field indicates the extent to which a process in the logon session can impersonate. The authentication information fields provide detailed information about this specific logon request. - Logon GUID is a unique identifier that can be used to correlate this event with a KDC event. - Transited services indicate which intermediate services have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indicates the length of the generated session key. This will be 0 if no session key was requested.
Security	Audit	12544	2015-04-26	Microsoft-Windows-Security-	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: LTRANPHD$ Account Domain: WORKGROUP Logon ID: 0x3e7 Logon Type: 5 Impersonation Level: %%1833 New Logon: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Logon ID: 0x3e7 Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x230 Process Name: C:\Windows\System32\services.exe Network Information: Workstation Name: Source Network Address: - Source Port: - Detailed Authentication Information: Logon Process: Advapi Authentication Package: Negotiate Transited Services: - Package Name (NTLM only): - Key Length: 0 This event is generated when a logon session is created. It is generated on the computer that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service such as the Server service, or a local process such as Winlogon.exe or Services.exe. The logon type field indicates the kind of logon that occurred.

	Success		08:56:26	Auditing	The most common types are 2 (interactive) and 3 (network). The New Logon fields indicate the account for whom the new logon was created, i.e. the account that was logged on. The network fields indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impersonation level field indicates the extent to which a process in the logon session can impersonate. The authentication information fields provide detailed information about this specific logon request. - Logon GUID is a unique identifier that can be used to correlate this event with a KDC event. - Transited services indicate which intermediate services have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indicates the length of the generated session key. This will be 0 if no session key was requested.
Security	Audit Success	12544	2015-04-26 08:56:26	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: LTRANPHD$ Account Domain: WORKGROUP Logon ID: 0x3e7 Logon Type: 5 Impersonation Level: %%1833 New Logon: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Logon ID: 0x3e7 Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x230 Process Name: C:\Windows\System32\services.exe Network Information: Workstation Name: Source Network Address: - Source Port: - Detailed Authentication Information: Logon Process: Advapi Authentication Package: Negotiate Transited Services: - Package Name (NTLM only): - Key Length: 0 This event is generated when a logon session is created. It is generated on the computer that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service such as the Server service, or a local process such as Winlogon.exe or Services.exe. The logon type field indicates the kind of logon that occurred. The most common types are 2 (interactive) and 3 (network). The New Logon fields indicate the account for whom the new logon was created, i.e. the account that was logged on. The network fields indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impersonation level field indicates the extent to which a process in the logon session can impersonate. The authentication information fields provide detailed information about this specific logon request. - Logon GUID is a unique identifier that can be used to correlate this event with a KDC event. - Transited services indicate which intermediate services have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indicates the length of the generated session key. This will be 0 if no session key was requested.
Security	Audit Success	12544	2015-04-26 08:56:26	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-0-0 Account Name: - Account Domain: - Logon ID: 0x0 Logon Type: 3 Impersonation Level: %%1833 New Logon: Security ID: S-1-5-7 Account Name: ANONYMOUS LOGON Account Domain: NT AUTHORITY Logon ID: 0x19f34 Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x0 Process Name: - Network Information: Workstation Name: Source Network Address: - Source Port: - Detailed Authentication Information: Logon Process: NtLmSsp Authentication Package: NTLM Transited Services: - Package Name (NTLM only): NTLM V1 Key Length: 0 This event is generated when a logon session is created. It is generated on the computer that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service such as the Server service, or a local process such as Winlogon.exe or Services.exe. The logon type field indicates the kind of logon that occurred. The most common types are 2 (interactive) and 3 (network). The New Logon fields indicate the account for whom the new logon was created, i.e. the account that was logged on. The network fields indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impersonation level field indicates the extent to which a process in the logon session can impersonate. The authentication information fields provide detailed information about this specific logon request. - Logon GUID is a unique identifier that can be used to correlate this event with a KDC event. - Transited services indicate which intermediate services have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indicates the length of the generated session key. This will be 0 if no session key was requested.
Security	Audit Success	12548	2015-04-26 08:56:26	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Logon ID: 0x3e7 Privileges: SeAssignPrimaryTokenPrivilege SeTcbPrivilege SeSecurityPrivilege SeTakeOwnershipPrivilege SeLoadDriverPrivilege SeBackupPrivilege SeRestorePrivilege SeDebugPrivilege SeAuditPrivilege SeSystemEnvironmentPrivilege SeImpersonatePrivilege
Security	Audit Success	12548	2015-04-26 08:56:26	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Logon ID: 0x3e7 Privileges: SeAssignPrimaryTokenPrivilege SeTcbPrivilege SeSecurityPrivilege SeTakeOwnershipPrivilege SeLoadDriverPrivilege SeBackupPrivilege SeRestorePrivilege SeDebugPrivilege SeAuditPrivilege SeSystemEnvironmentPrivilege SeImpersonatePrivilege
Security	Audit Success	12548	2015-04-26 08:56:26	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Logon ID: 0x3e7 Privileges: SeAssignPrimaryTokenPrivilege SeTcbPrivilege SeSecurityPrivilege SeTakeOwnershipPrivilege SeLoadDriverPrivilege SeBackupPrivilege SeRestorePrivilege SeDebugPrivilege SeAuditPrivilege SeSystemEnvironmentPrivilege SeImpersonatePrivilege
Security	Audit Success	12544	2015-04-26 08:56:27	Microsoft-Windows-Security-Auditing	4648: A logon was attempted using explicit credentials. Subject: Security ID: S-1-5-18 Account Name: LTRANPHD$ Account Domain: WORKGROUP Logon ID: 0x3e7 Logon GUID: {00000000-0000-0000-0000-000000000000} Account Whose Credentials Were Used: Account Name: Liem Account Domain: LTRANPHD Logon GUID: {00000000-0000-0000-0000-000000000000} Target Server: Target Server Name: localhost Additional Information: localhost Process Information: Process ID: 0x204 Process Name: C:\Windows\System32\winlogon.exe Network Information: Network Address: 127.0.0.1 Port: 0 This event is generated when a process attempts to log on an account by explicitly specifying that account’s credentials. This most commonly occurs in batch-type configurations such as scheduled tasks, or when using the RUNAS

					command.
Security	Audit Success	12544	2015-04-26 08:56:27	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: LTRANPHD$ Account Domain: WORKGROUP Logon ID: 0x3e7 Logon Type: 2 Impersonation Level: %%1833 New Logon: Security ID: S-1-5-21-1888849264-3803429180-4108621888-1001 Account Name: Liem Account Domain: LTRANPHD Logon ID: 0x1b8d6 Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x204 Process Name: C:\Windows\System32\winlogon.exe Network Information: Workstation Name: LTRANPHD Source Network Address: 127.0.0.1 Source Port: 0 Detailed Authentication Information: Logon Process: User32 Authentication Package: Negotiate Transited Services: - Package Name (NTLM only): - Key Length: 0 This event is generated when a logon session is created. It is generated on the computer that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service such as the Server service, or a local process such as Winlogon.exe or Services.exe. The logon type field indicates the kind of logon that occurred. The most common types are 2 (interactive) and 3 (network). The New Logon fields indicate the account for whom the new logon was created, i.e. the account that was logged on. The network fields indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impersonation level field indicates the extent to which a process in the logon session can impersonate. The authentication information fields provide detailed information about this specific logon request. - Logon GUID is a unique identifier that can be used to correlate this event with a KDC event. - Transited services indicate which intermediate services have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indicates the length of the generated session key. This will be 0 if no session key was requested.
Security	Audit Success	12544	2015-04-26 08:56:27	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: LTRANPHD$ Account Domain: WORKGROUP Logon ID: 0x3e7 Logon Type: 2 Impersonation Level: %%1833 New Logon: Security ID: S-1-5-21-1888849264-3803429180-4108621888-1001 Account Name: Liem Account Domain: LTRANPHD Logon ID: 0x1b909 Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x204 Process Name: C:\Windows\System32\winlogon.exe Network Information: Workstation Name: LTRANPHD Source Network Address: 127.0.0.1 Source Port: 0 Detailed Authentication Information: Logon Process: User32 Authentication Package: Negotiate Transited Services: - Package Name (NTLM only): - Key Length: 0 This event is generated when a logon session is created. It is generated on the computer that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service such as the Server service, or a local process such as Winlogon.exe or Services.exe. The logon type field indicates the kind of logon that occurred. The most common types are 2 (interactive) and 3 (network). The New Logon fields indicate the account for whom the new logon was created, i.e. the account that was logged on. The network fields indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impersonation level field indicates the extent to which a process in the logon session can impersonate. The authentication information fields provide detailed information about this specific logon request. - Logon GUID is a unique identifier that can be used to correlate this event with a KDC event. - Transited services indicate which intermediate services have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indicates the length of the generated session key. This will be 0 if no session key was requested.
Security	Audit Success	12548	2015-04-26 08:56:27	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-21-1888849264-3803429180-4108621888-1001 Account Name: Liem Account Domain: LTRANPHD Logon ID: 0x1b8d6 Privileges: SeSecurityPrivilege SeTakeOwnershipPrivilege SeLoadDriverPrivilege SeBackupPrivilege SeRestorePrivilege SeDebugPrivilege SeSystemEnvironmentPrivilege SeImpersonatePrivilege
Security	Audit Success	12544	2015-04-26 08:56:29	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: LTRANPHD$ Account Domain: WORKGROUP Logon ID: 0x3e7 Logon Type: 5 Impersonation Level: %%1833 New Logon: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Logon ID: 0x3e7 Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x230 Process Name: C:\Windows\System32\services.exe Network Information: Workstation Name: Source Network Address: - Source Port: - Detailed Authentication Information: Logon Process: Advapi Authentication Package: Negotiate Transited Services: - Package Name (NTLM only): - Key Length: 0 This event is generated when a logon session is created. It is generated on the computer that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service such as the Server service, or a local process such as Winlogon.exe or Services.exe. The logon type field indicates the kind of logon that occurred. The most common types are 2 (interactive) and 3 (network). The New Logon fields indicate the account for whom the new logon was created, i.e. the account that was logged on. The network fields indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impersonation level field indicates the extent to which a process in the logon session can impersonate. The authentication information fields provide detailed information about this specific logon request. - Logon GUID is a unique identifier that can be used to correlate this event with a KDC event. - Transited services indicate which intermediate services have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indicates the length of the generated session key. This will be 0 if no session key was requested.
Security	Audit Success	12548	2015-04-26 08:56:29	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Logon ID: 0x3e7 Privileges: SeAssignPrimaryTokenPrivilege SeTcbPrivilege SeSecurityPrivilege SeTakeOwnershipPrivilege SeLoadDriverPrivilege SeBackupPrivilege SeRestorePrivilege SeDebugPrivilege SeAuditPrivilege SeSystemEnvironmentPrivilege SeImpersonatePrivilege

Security	Audit Success	13824	2015-04-26 08:56:30	Microsoft-Windows-Security-Auditing	4797: An attempt was made to query the existence of a blank password for an account. Subject: Security ID: S-1-5-21-1888849264-3803429180-4108621888-1001 Account Name: Liem Account Domain: LTRANPHD Logon ID: 0x1b909 Additional Information: Caller Workstation: LTRANPHD Target Account Name: Administrator Target Account Domain: LTRANPHD
Security	Audit Success	13824	2015-04-26 08:56:30	Microsoft-Windows-Security-Auditing	4797: An attempt was made to query the existence of a blank password for an account. Subject: Security ID: S-1-5-21-1888849264-3803429180-4108621888-1001 Account Name: Liem Account Domain: LTRANPHD Logon ID: 0x1b909 Additional Information: Caller Workstation: LTRANPHD Target Account Name: Guest Target Account Domain: LTRANPHD
Security	Audit Success	13824	2015-04-26 08:56:30	Microsoft-Windows-Security-Auditing	4797: An attempt was made to query the existence of a blank password for an account. Subject: Security ID: S-1-5-21-1888849264-3803429180-4108621888-1001 Account Name: Liem Account Domain: LTRANPHD Logon ID: 0x1b909 Additional Information: Caller Workstation: LTRANPHD Target Account Name: Administrator Target Account Domain: LTRANPHD
Security	Audit Success	13824	2015-04-26 08:56:30	Microsoft-Windows-Security-Auditing	4797: An attempt was made to query the existence of a blank password for an account. Subject: Security ID: S-1-5-21-1888849264-3803429180-4108621888-1001 Account Name: Liem Account Domain: LTRANPHD Logon ID: 0x1b909 Additional Information: Caller Workstation: LTRANPHD Target Account Name: Guest Target Account Domain: LTRANPHD
Security	Audit Success	13824	2015-04-26 08:56:35	Microsoft-Windows-Security-Auditing	4797: An attempt was made to query the existence of a blank password for an account. Subject: Security ID: S-1-5-19 Account Name: LOCAL SERVICE Account Domain: NT AUTHORITY Logon ID: 0x3e5 Additional Information: Caller Workstation: LTRANPHD Target Account Name: Administrator Target Account Domain: LTRANPHD
Security	Audit Success	13824	2015-04-26 08:56:35	Microsoft-Windows-Security-Auditing	4797: An attempt was made to query the existence of a blank password for an account. Subject: Security ID: S-1-5-19 Account Name: LOCAL SERVICE Account Domain: NT AUTHORITY Logon ID: 0x3e5 Additional Information: Caller Workstation: LTRANPHD Target Account Name: Guest Target Account Domain: LTRANPHD
Security	Audit Success	13824	2015-04-26 08:56:35	Microsoft-Windows-Security-Auditing	4797: An attempt was made to query the existence of a blank password for an account. Subject: Security ID: S-1-5-19 Account Name: LOCAL SERVICE Account Domain: NT AUTHORITY Logon ID: 0x3e5 Additional Information: Caller Workstation: LTRANPHD Target Account Name: Administrator Target Account Domain: LTRANPHD
Security	Audit Success	13824	2015-04-26 08:56:35	Microsoft-Windows-Security-Auditing	4797: An attempt was made to query the existence of a blank password for an account. Subject: Security ID: S-1-5-19 Account Name: LOCAL SERVICE Account Domain: NT AUTHORITY Logon ID: 0x3e5 Additional Information: Caller Workstation: LTRANPHD Target Account Name: Liem Target Account Domain: LTRANPHD
Security	Audit Success	13824	2015-04-26 08:56:35	Microsoft-Windows-Security-Auditing	4797: An attempt was made to query the existence of a blank password for an account. Subject: Security ID: S-1-5-19 Account Name: LOCAL SERVICE Account Domain: NT AUTHORITY Logon ID: 0x3e5 Additional Information: Caller Workstation: LTRANPHD Target Account Name: Guest Target Account Domain: LTRANPHD
Security	Audit Success	13824	2015-04-26 08:56:35	Microsoft-Windows-Security-Auditing	4797: An attempt was made to query the existence of a blank password for an account. Subject: Security ID: S-1-5-19 Account Name: LOCAL SERVICE Account Domain: NT AUTHORITY Logon ID: 0x3e5 Additional Information: Caller Workstation: LTRANPHD Target Account Name: Liem Target Account Domain: LTRANPHD
Security	Audit Success	13824	2015-04-26 08:56:35	Microsoft-Windows-Security-Auditing	4797: An attempt was made to query the existence of a blank password for an account. Subject: Security ID: S-1-5-19 Account Name: LOCAL SERVICE Account Domain: NT AUTHORITY Logon ID: 0x3e5 Additional Information: Caller Workstation: LTRANPHD Target Account Name: Liem Target Account Domain: LTRANPHD
Security	Audit Success	12544	2015-04-26 09:00:28	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: LTRANPHD$ Account Domain: WORKGROUP Logon ID: 0x3e7 Logon Type: 5 Impersonation Level: %%1833 New Logon: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Logon ID: 0x3e7 Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x230 Process Name: C:\Windows\System32\services.exe Network Information: Workstation Name: Source Network Address: - Source Port: - Detailed Authentication Information: Logon Process: Advapi Authentication Package: Negotiate Transited Services: - Package Name (NTLM only): - Key Length: 0 This event is generated when a logon session is created. It is generated on the computer that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service such as the Server service, or a local process such as Winlogon.exe or Services.exe. The logon type field indicates the kind of logon that occurred. The most common types are 2 (interactive) and 3 (network). The New Logon fields indicate the account for whom the new logon was created, i.e. the account that was logged on. The network fields indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impersonation level field indicates the extent to which a process in the logon session can impersonate. The authentication information fields provide detailed information about this specific logon request. - Logon GUID is a unique identifier that can be used to correlate this event with a KDC event. - Transited services indicate which intermediate services have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indicates the length of the generated session key. This will be 0 if no session key was requested.
					4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: LTRANPHD$ Account Domain: WORKGROUP Logon ID: 0x3e7 Logon Type: 5 Impersonation Level: %%1833 New Logon: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Logon ID: 0x3e7 Logon GUID:

Security	Audit Success	12544	2015-04-26 09:00:28	Microsoft-Windows-Security-Auditing	{00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x230 Process Name: C:\Windows\System32\services.exe Network Information: Workstation Name: Source Network Address: - Source Port: - Detailed Authentication Information: Logon Process: Advapi Authentication Package: Negotiate Transited Services: - Package Name (NTLM only): - Key Length: 0 This event is generated when a logon session is created. It is generated on the computer that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service such as the Server service, or a local process such as Winlogon.exe or Services.exe. The logon type field indicates the kind of logon that occurred. The most common types are 2 (interactive) and 3 (network). The New Logon fields indicate the account for whom the new logon was created, i.e. the account that was logged on. The network fields indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impersonation level field indicates the extent to which a process in the logon session can impersonate. The authentication information fields provide detailed information about this specific logon request. - Logon GUID is a unique identifier that can be used to correlate this event with a KDC event. - Transited services indicate which intermediate services have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indicates the length of the generated session key. This will be 0 if no session key was requested.
Security	Audit Success	12548	2015-04-26 09:00:28	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Logon ID: 0x3e7 Privileges: SeAssignPrimaryTokenPrivilege SeTcbPrivilege SeSecurityPrivilege SeTakeOwnershipPrivilege SeLoadDriverPrivilege SeBackupPrivilege SeRestorePrivilege SeDebugPrivilege SeAuditPrivilege SeSystemEnvironmentPrivilege SeImpersonatePrivilege
Security	Audit Success	12548	2015-04-26 09:00:28	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Logon ID: 0x3e7 Privileges: SeAssignPrimaryTokenPrivilege SeTcbPrivilege SeSecurityPrivilege SeTakeOwnershipPrivilege SeLoadDriverPrivilege SeBackupPrivilege SeRestorePrivilege SeDebugPrivilege SeAuditPrivilege SeSystemEnvironmentPrivilege SeImpersonatePrivilege
Security	Audit Success	12544	2015-04-26 09:06:35	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: LTRANPHD$ Account Domain: WORKGROUP Logon ID: 0x3e7 Logon Type: 5 Impersonation Level: %%1833 New Logon: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Logon ID: 0x3e7 Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x230 Process Name: C:\Windows\System32\services.exe Network Information: Workstation Name: Source Network Address: - Source Port: - Detailed Authentication Information: Logon Process: Advapi Authentication Package: Negotiate Transited Services: - Package Name (NTLM only): - Key Length: 0 This event is generated when a logon session is created. It is generated on the computer that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service such as the Server service, or a local process such as Winlogon.exe or Services.exe. The logon type field indicates the kind of logon that occurred. The most common types are 2 (interactive) and 3 (network). The New Logon fields indicate the account for whom the new logon was created, i.e. the account that was logged on. The network fields indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impersonation level field indicates the extent to which a process in the logon session can impersonate. The authentication information fields provide detailed information about this specific logon request. - Logon GUID is a unique identifier that can be used to correlate this event with a KDC event. - Transited services indicate which intermediate services have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indicates the length of the generated session key. This will be 0 if no session key was requested.
Security	Audit Success	12548	2015-04-26 09:06:35	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Logon ID: 0x3e7 Privileges: SeAssignPrimaryTokenPrivilege SeTcbPrivilege SeSecurityPrivilege SeTakeOwnershipPrivilege SeLoadDriverPrivilege SeBackupPrivilege SeRestorePrivilege SeDebugPrivilege SeAuditPrivilege SeSystemEnvironmentPrivilege SeImpersonatePrivilege
Security	Audit Success	12544	2015-04-26 09:06:36	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: LTRANPHD$ Account Domain: WORKGROUP Logon ID: 0x3e7 Logon Type: 5 Impersonation Level: %%1833 New Logon: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Logon ID: 0x3e7 Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x230 Process Name: C:\Windows\System32\services.exe Network Information: Workstation Name: Source Network Address: - Source Port: - Detailed Authentication Information: Logon Process: Advapi Authentication Package: Negotiate Transited Services: - Package Name (NTLM only): - Key Length: 0 This event is generated when a logon session is created. It is generated on the computer that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service such as the Server service, or a local process such as Winlogon.exe or Services.exe. The logon type field indicates the kind of logon that occurred. The most common types are 2 (interactive) and 3 (network). The New Logon fields indicate the account for whom the new logon was created, i.e. the account that was logged on. The network fields indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impersonation level field indicates the extent to which a process in the logon session can impersonate. The authentication information fields provide detailed information about this specific logon request. - Logon GUID is a unique identifier that can be used to correlate this event with a KDC event. - Transited services indicate which intermediate services have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indicates the length of the generated session key. This will be 0 if no session key was requested.

Security	Audit Success	12548	2015-04-26 09:06:36	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Logon ID: 0x3e7 Privileges: SeAssignPrimaryTokenPrivilege SeTcbPrivilege SeSecurityPrivilege SeTakeOwnershipPrivilege SeLoadDriverPrivilege SeBackupPrivilege SeRestorePrivilege SeDebugPrivilege SeAuditPrivilege SeSystemEnvironmentPrivilege SeImpersonatePrivilege
Security	Audit Success	12288	2015-04-26 09:30:03	Microsoft-Windows-Security-Auditing	4608: Windows is starting up. This event is logged when LSASS.EXE starts and the auditing subsystem is initialized.
Security	Audit Success	12544	2015-04-26 09:30:03	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-0-0 Account Name: - Account Domain: - Logon ID: 0x0 Logon Type: 0 Impersonation Level: - New Logon: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Logon ID: 0x3e7 Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x4 Process Name: Network Information: Workstation Name: - Source Network Address: - Source Port: - Detailed Authentication Information: Logon Process: - Authentication Package: - Transited Services: - Package Name (NTLM only): - Key Length: 0 This event is generated when a logon session is created. It is generated on the computer that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service such as the Server service, or a local process such as Winlogon.exe or Services.exe. The logon type field indicates the kind of logon that occurred. The most common types are 2 (interactive) and 3 (network). The New Logon fields indicate the account for whom the new logon was created, i.e. the account that was logged on. The network fields indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impersonation level field indicates the extent to which a process in the logon session can impersonate. The authentication information fields provide detailed information about this specific logon request. - Logon GUID is a unique identifier that can be used to correlate this event with a KDC event. - Transited services indicate which intermediate services have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indicates the length of the generated session key. This will be 0 if no session key was requested.
Security	Audit Success	12544	2015-04-26 09:30:03	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: LTRANPHD$ Account Domain: WORKGROUP Logon ID: 0x3e7 Logon Type: 5 Impersonation Level: %%1833 New Logon: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Logon ID: 0x3e7 Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x244 Process Name: C:\Windows\System32\services.exe Network Information: Workstation Name: Source Network Address: - Source Port: - Detailed Authentication Information: Logon Process: Advapi Authentication Package: Negotiate Transited Services: - Package Name (NTLM only): - Key Length: 0 This event is generated when a logon session is created. It is generated on the computer that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service such as the Server service, or a local process such as Winlogon.exe or Services.exe. The logon type field indicates the kind of logon that occurred. The most common types are 2 (interactive) and 3 (network). The New Logon fields indicate the account for whom the new logon was created, i.e. the account that was logged on. The network fields indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impersonation level field indicates the extent to which a process in the logon session can impersonate. The authentication information fields provide detailed information about this specific logon request. - Logon GUID is a unique identifier that can be used to correlate this event with a KDC event. - Transited services indicate which intermediate services have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indicates the length of the generated session key. This will be 0 if no session key was requested.
Security	Audit Success	12544	2015-04-26 09:30:03	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: LTRANPHD$ Account Domain: WORKGROUP Logon ID: 0x3e7 Logon Type: 5 Impersonation Level: %%1833 New Logon: Security ID: S-1-5-20 Account Name: NETWORK SERVICE Account Domain: NT AUTHORITY Logon ID: 0x3e4 Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x244 Process Name: C:\Windows\System32\services.exe Network Information: Workstation Name: Source Network Address: - Source Port: - Detailed Authentication Information: Logon Process: Advapi Authentication Package: Negotiate Transited Services: - Package Name (NTLM only): - Key Length: 0 This event is generated when a logon session is created. It is generated on the computer that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service such as the Server service, or a local process such as Winlogon.exe or Services.exe. The logon type field indicates the kind of logon that occurred. The most common types are 2 (interactive) and 3 (network). The New Logon fields indicate the account for whom the new logon was created, i.e. the account that was logged on. The network fields indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impersonation level field indicates the extent to which a process in the logon session can impersonate. The authentication information fields provide detailed information about this specific logon request. - Logon GUID is a unique identifier that can be used to correlate this event with a KDC event. - Transited services indicate which intermediate services have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indicates the length of the generated session key. This will be 0 if no session key was requested.
			2015-04-		4648: A logon was attempted using explicit credentials. Subject: Security ID: S-1-5-18 Account Name: LTRANPHD$ Account Domain: WORKGROUP Logon ID: 0x3e7 Logon GUID: {00000000-0000-0000-0000-000000000000} Account Whose Credentials Were Used: Account Name: DWM-1 Account Domain: Window

Security	Audit Success	12544	26 09:30:03	Microsoft-Windows-Security-Auditing	Manager Logon GUID: {00000000-0000-0000-0000-000000000000} Target Server: Target Server Name: localhost Additional Information: localhost Process Information: Process ID: 0x224 Process Name: C:\Windows\System32\winlogon.exe Network Information: Network Address: - Port: - This event is generated when a process attempts to log on an account by explicitly specifying that account's credentials. This most commonly occurs in batch-type configurations such as scheduled tasks, or when using the RUNAS command.
Security	Audit Success	12544	2015-04-26 09:30:03	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: LTRANPHD$ Account Domain: WORKGROUP Logon ID: 0x3e7 Logon Type: 2 Impersonation Level: %%1833 New Logon: Security ID: S-1-5-90-1 Account Name: DWM-1 Account Domain: Window Manager Logon ID: 0xe92b Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x224 Process Name: C:\Windows\System32\winlogon.exe Network Information: Workstation Name: Source Network Address: - Source Port: - Detailed Authentication Information: Logon Process: Advapi Authentication Package: Negotiate Transited Services: - Package Name (NTLM only): - Key Length: 0 This event is generated when a logon session is created. It is generated on the computer that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service such as the Server service, or a local process such as Winlogon.exe or Services.exe. The logon type field indicates the kind of logon that occurred. The most common types are 2 (interactive) and 3 (network). The New Logon fields indicate the account for whom the new logon was created, i.e. the account that was logged on. The network fields indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impersonation level field indicates the extent to which a process in the logon session can impersonate. The authentication information fields provide detailed information about this specific logon request. - Logon GUID is a unique identifier that can be used to correlate this event with a KDC event. - Transited services indicate which intermediate services have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indicates the length of the generated session key. This will be 0 if no session key was requested.
Security	Audit Success	12544	2015-04-26 09:30:03	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: LTRANPHD$ Account Domain: WORKGROUP Logon ID: 0x3e7 Logon Type: 2 Impersonation Level: %%1833 New Logon: Security ID: S-1-5-90-1 Account Name: DWM-1 Account Domain: Window Manager Logon ID: 0xe942 Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x224 Process Name: C:\Windows\System32\winlogon.exe Network Information: Workstation Name: Source Network Address: - Source Port: - Detailed Authentication Information: Logon Process: Advapi Authentication Package: Negotiate Transited Services: - Package Name (NTLM only): - Key Length: 0 This event is generated when a logon session is created. It is generated on the computer that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service such as the Server service, or a local process such as Winlogon.exe or Services.exe. The logon type field indicates the kind of logon that occurred. The most common types are 2 (interactive) and 3 (network). The New Logon fields indicate the account for whom the new logon was created, i.e. the account that was logged on. The network fields indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impersonation level field indicates the extent to which a process in the logon session can impersonate. The authentication information fields provide detailed information about this specific logon request. - Logon GUID is a unique identifier that can be used to correlate this event with a KDC event. - Transited services indicate which intermediate services have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indicates the length of the generated session key. This will be 0 if no session key was requested.
Security	Audit Success	12544	2015-04-26 09:30:03	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: LTRANPHD$ Account Domain: WORKGROUP Logon ID: 0x3e7 Logon Type: 5 Impersonation Level: %%1833 New Logon: Security ID: S-1-5-19 Account Name: LOCAL SERVICE Account Domain: NT AUTHORITY Logon ID: 0x3e5 Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x244 Process Name: C:\Windows\System32\services.exe Network Information: Workstation Name: Source Network Address: - Source Port: - Detailed Authentication Information: Logon Process: Advapi Authentication Package: Negotiate Transited Services: - Package Name (NTLM only): - Key Length: 0 This event is generated when a logon session is created. It is generated on the computer that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service such as the Server service, or a local process such as Winlogon.exe or Services.exe. The logon type field indicates the kind of logon that occurred. The most common types are 2 (interactive) and 3 (network). The New Logon fields indicate the account for whom the new logon was created, i.e. the account that was logged on. The network fields indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impersonation level field indicates the extent to which a process in the logon session can impersonate. The authentication information fields provide detailed information about this specific logon request. - Logon GUID is a unique identifier that can be used to correlate this event with a KDC event. - Transited services indicate which intermediate services have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indicates the length of the generated session key. This will be 0 if no session key was requested.
					4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: LTRANPHD$ Account Domain: WORKGROUP Logon ID: 0x3e7 Logon Type: 5 Impersonation Level: %%1833 New Logon: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Logon ID: 0x3e7 Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x244 Process Name: C:\Windows\System32\services.exe Network Information: Workstation Name: Source Network Address: - Source

Security	Audit Success	12544	2015-04-26 09:30:03	Microsoft-Windows-Security-Auditing	Port: - Detailed Authentication Information: Logon Process: Advapi Authentication Package: Negotiate Transited Services: - Package Name (NTLM only): - Key Length: 0 This event is generated when a logon session is created. It is generated on the computer that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service such as the Server service, or a local process such as Winlogon.exe or Services.exe. The logon type field indicates the kind of logon that occurred. The most common types are 2 (interactive) and 3 (network). The New Logon fields indicate the account for whom the new logon was created, i.e. the account that was logged on. The network fields indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impersonation level field indicates the extent to which a process in the logon session can impersonate. The authentication information fields provide detailed information about this specific logon request. - Logon GUID is a unique identifier that can be used to correlate this event with a KDC event. - Transited services indicate which intermediate services have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indicates the length of the generated session key. This will be 0 if no session key was requested.
Security	Audit Success	12544	2015-04-26 09:30:03	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: LTRANPHD$ Account Domain: WORKGROUP Logon ID: 0x3e7 Logon Type: 5 Impersonation Level: %%1833 New Logon: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Logon ID: 0x3e7 Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x244 Process Name: C:\Windows\System32\services.exe Network Information: Workstation Name: Source Network Address: - Source Port: - Detailed Authentication Information: Logon Process: Advapi Authentication Package: Negotiate Transited Services: - Package Name (NTLM only): - Key Length: 0 This event is generated when a logon session is created. It is generated on the computer that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service such as the Server service, or a local process such as Winlogon.exe or Services.exe. The logon type field indicates the kind of logon that occurred. The most common types are 2 (interactive) and 3 (network). The New Logon fields indicate the account for whom the new logon was created, i.e. the account that was logged on. The network fields indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impersonation level field indicates the extent to which a process in the logon session can impersonate. The authentication information fields provide detailed information about this specific logon request. - Logon GUID is a unique identifier that can be used to correlate this event with a KDC event. - Transited services indicate which intermediate services have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indicates the length of the generated session key. This will be 0 if no session key was requested.
Security	Audit Success	12544	2015-04-26 09:30:03	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: LTRANPHD$ Account Domain: WORKGROUP Logon ID: 0x3e7 Logon Type: 5 Impersonation Level: %%1833 New Logon: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Logon ID: 0x3e7 Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x244 Process Name: C:\Windows\System32\services.exe Network Information: Workstation Name: Source Network Address: - Source Port: - Detailed Authentication Information: Logon Process: Advapi Authentication Package: Negotiate Transited Services: - Package Name (NTLM only): - Key Length: 0 This event is generated when a logon session is created. It is generated on the computer that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service such as the Server service, or a local process such as Winlogon.exe or Services.exe. The logon type field indicates the kind of logon that occurred. The most common types are 2 (interactive) and 3 (network). The New Logon fields indicate the account for whom the new logon was created, i.e. the account that was logged on. The network fields indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impersonation level field indicates the extent to which a process in the logon session can impersonate. The authentication information fields provide detailed information about this specific logon request. - Logon GUID is a unique identifier that can be used to correlate this event with a KDC event. - Transited services indicate which intermediate services have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indicates the length of the generated session key. This will be 0 if no session key was requested.
Security	Audit Success	12548	2015-04-26 09:30:03	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Logon ID: 0x3e7 Privileges: SeAssignPrimaryTokenPrivilege SeTcbPrivilege SeSecurityPrivilege SeTakeOwnershipPrivilege SeLoadDriverPrivilege SeBackupPrivilege SeRestorePrivilege SeDebugPrivilege SeAuditPrivilege SeSystemEnvironmentPrivilege SeImpersonatePrivilege
Security	Audit Success	12548	2015-04-26 09:30:03	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-20 Account Name: NETWORK SERVICE Account Domain: NT AUTHORITY Logon ID: 0x3e4 Privileges: SeAssignPrimaryTokenPrivilege SeAuditPrivilege SeImpersonatePrivilege
Security	Audit Success	12548	2015-04-26 09:30:03	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-90-1 Account Name: DWM-1 Account Domain: Window Manager Logon ID: 0xe92b Privileges: SeAssignPrimaryTokenPrivilege SeAuditPrivilege SeImpersonatePrivilege
Security	Audit Success	12548	2015-04-26 09:30:03	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-90-1 Account Name: DWM-1 Account Domain: Window Manager Logon ID: 0xe942 Privileges: SeAssignPrimaryTokenPrivilege SeAuditPrivilege
			2015-04-		4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-19 Account Name: LOCAL SERVICE

Security	Audit Success	12548	26 09:30:03	Microsoft-Windows-Security-Auditing	Account Domain: NT AUTHORITY Logon ID: 0x3e5 Privileges: SeAssignPrimaryTokenPrivilege SeAuditPrivilege SeImpersonatePrivilege
Security	Audit Success	12548	2015-04-26 09:30:03	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Logon ID: 0x3e7 Privileges: SeAssignPrimaryTokenPrivilege SeTcbPrivilege SeSecurityPrivilege SeTakeOwnershipPrivilege SeLoadDriverPrivilege SeBackupPrivilege SeRestorePrivilege SeDebugPrivilege SeAuditPrivilege SeSystemEnvironmentPrivilege SeImpersonatePrivilege
Security	Audit Success	12548	2015-04-26 09:30:03	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Logon ID: 0x3e7 Privileges: SeAssignPrimaryTokenPrivilege SeTcbPrivilege SeSecurityPrivilege SeTakeOwnershipPrivilege SeLoadDriverPrivilege SeBackupPrivilege SeRestorePrivilege SeDebugPrivilege SeAuditPrivilege SeSystemEnvironmentPrivilege SeImpersonatePrivilege
Security	Audit Success	12548	2015-04-26 09:30:03	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Logon ID: 0x3e7 Privileges: SeAssignPrimaryTokenPrivilege SeTcbPrivilege SeSecurityPrivilege SeTakeOwnershipPrivilege SeLoadDriverPrivilege SeBackupPrivilege SeRestorePrivilege SeDebugPrivilege SeAuditPrivilege SeSystemEnvironmentPrivilege SeImpersonatePrivilege
Security	Audit Success	13568	2015-04-26 09:30:03	Microsoft-Windows-Security-Auditing	4902: The Per-user audit policy table was created. Number of Elements: 0 Policy ID: 0xb0e5
Security	Audit Success	101	2015-04-26 09:30:06	Microsoft-Windows-Eventlog	1101: Audit events have been dropped by the transport. 0
Security	Audit Success	12292	2015-04-26 09:30:06	Microsoft-Windows-Security-Auditing	5033: The Windows Firewall Driver started successfully.
Security	Audit Success	12292	2015-04-26 09:30:06	Microsoft-Windows-Security-Auditing	5024: The Windows Firewall service started successfully.
Security	Audit Success	12544	2015-04-26 09:30:06	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: LTRANPHD$ Account Domain: WORKGROUP Logon ID: 0x3e7 Logon Type: 5 Impersonation Level: %%1833 New Logon: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Logon ID: 0x3e7 Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x244 Process Name: C:\Windows\System32\services.exe Network Information: Workstation Name: Source Network Address: - Source Port: - Detailed Authentication Information: Logon Process: Advapi Authentication Package: Negotiate Transited Services: - Package Name (NTLM only): - Key Length: 0 This event is generated when a logon session is created. It is generated on the computer that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service such as the Server service, or a local process such as Winlogon.exe or Services.exe. The logon type field indicates the kind of logon that occurred. The most common types are 2 (interactive) and 3 (network). The New Logon fields indicate the account for whom the new logon was created, i.e. the account that was logged on. The network fields indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impersonation level field indicates the extent to which a process in the logon session can impersonate. The authentication information fields provide detailed information about this specific logon request. - Logon GUID is a unique identifier that can be used to correlate this event with a KDC event. - Transited services indicate which intermediate services have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indicates the length of the generated session key. This will be 0 if no session key was requested.
Security	Audit Success	12544	2015-04-26 09:30:06	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: LTRANPHD$ Account Domain: WORKGROUP Logon ID: 0x3e7 Logon Type: 5 Impersonation Level: %%1833 New Logon: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Logon ID: 0x3e7 Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x244 Process Name: C:\Windows\System32\services.exe Network Information: Workstation Name: Source Network Address: - Source Port: - Detailed Authentication Information: Logon Process: Advapi Authentication Package: Negotiate Transited Services: - Package Name (NTLM only): - Key Length: 0 This event is generated when a logon session is created. It is generated on the computer that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service such as the Server service, or a local process such as Winlogon.exe or Services.exe. The logon type field indicates the kind of logon that occurred. The most common types are 2 (interactive) and 3 (network). The New Logon fields indicate the account for whom the new logon was created, i.e. the account that was logged on. The network fields indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impersonation level field indicates the extent to which a process in the logon session can impersonate. The authentication information fields provide detailed information about this specific logon request. - Logon GUID is a unique identifier that can be used to correlate this event with a KDC event. - Transited services indicate which intermediate services have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indicates the length of the generated session key. This will be 0 if no session key was requested.
					4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: LTRANPHD$

Security	Audit Success	12544	2015-04-26 09:30:06		Microsoft-Windows-Security-Auditing	Account Domain: WORKGROUP Logon ID: 0x3e7 Logon Type: 5 Impersonation Level: %%1833 New Logon: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Logon ID: 0x3e7 Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x244 Process Name: C:\Windows\System32\services.exe Network Information: Workstation Name: Source Network Address: - Source Port: - Detailed Authentication Information: Logon Process: Advapi Authentication Package: Negotiate Transited Services: - Package Name (NTLM only): - Key Length: 0 This event is generated when a logon session is created. It is generated on the computer that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service such as the Server service, or a local process such as Winlogon.exe or Services.exe. The logon type field indicates the kind of logon that occurred. The most common types are 2 (interactive) and 3 (network). The New Logon fields indicate the account for whom the new logon was created, i.e. the account that was logged on. The network fields indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impersonation level field indicates the extent to which a process in the logon session can impersonate. The authentication information fields provide detailed information about this specific logon request. - Logon GUID is a unique identifier that can be used to correlate this event with a KDC event. - Transited services indicate which intermediate services have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indicates the length of the generated session key. This will be 0 if no session key was requested.
Security	Audit Success	12544	2015-04-26 09:30:06		Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-0-0 Account Name: - Account Domain: - Logon ID: 0x0 Logon Type: 3 Impersonation Level: %%1833 New Logon: Security ID: S-1-5-7 Account Name: ANONYMOUS LOGON Account Domain: NT AUTHORITY Logon ID: 0x1af3c Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x0 Process Name: - Network Information: Workstation Name: Source Network Address: - Source Port: - Detailed Authentication Information: Logon Process: NtLmSsp Authentication Package: NTLM Transited Services: - Package Name (NTLM only): NTLM V1 Key Length: 0 This event is generated when a logon session is created. It is generated on the computer that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service such as the Server service, or a local process such as Winlogon.exe or Services.exe. The logon type field indicates the kind of logon that occurred. The most common types are 2 (interactive) and 3 (network). The New Logon fields indicate the account for whom the new logon was created, i.e. the account that was logged on. The network fields indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impersonation level field indicates the extent to which a process in the logon session can impersonate. The authentication information fields provide detailed information about this specific logon request. - Logon GUID is a unique identifier that can be used to correlate this event with a KDC event. - Transited services indicate which intermediate services have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indicates the length of the generated session key. This will be 0 if no session key was requested.
Security	Audit Success	12548	2015-04-26 09:30:06		Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Logon ID: 0x3e7 Privileges: SeAssignPrimaryTokenPrivilege SeTcbPrivilege SeSecurityPrivilege SeTakeOwnershipPrivilege SeLoadDriverPrivilege SeBackupPrivilege SeRestorePrivilege SeDebugPrivilege SeAuditPrivilege SeSystemEnvironmentPrivilege SeImpersonatePrivilege
Security	Audit Success	12548	2015-04-26 09:30:06		Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Logon ID: 0x3e7 Privileges: SeAssignPrimaryTokenPrivilege SeTcbPrivilege SeSecurityPrivilege SeTakeOwnershipPrivilege SeLoadDriverPrivilege SeBackupPrivilege SeRestorePrivilege SeDebugPrivilege SeAuditPrivilege SeSystemEnvironmentPrivilege SeImpersonatePrivilege
Security	Audit Success	12548	2015-04-26 09:30:06		Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Logon ID: 0x3e7 Privileges: SeAssignPrimaryTokenPrivilege SeTcbPrivilege SeSecurityPrivilege SeTakeOwnershipPrivilege SeLoadDriverPrivilege SeBackupPrivilege SeRestorePrivilege SeDebugPrivilege SeAuditPrivilege SeSystemEnvironmentPrivilege SeImpersonatePrivilege
Security	Audit Success	12544	2015-04-26 09:30:08		Microsoft-Windows-Security-Auditing	4648: A logon was attempted using explicit credentials. Subject: Security ID: S-1-5-18 Account Name: LTRANPHD$ Account Domain: WORKGROUP Logon ID: 0x3e7 Logon GUID: {00000000-0000-0000-0000-000000000000} Account Whose Credentials Were Used: Account Name: Liem Account Domain: LTRANPHD Logon GUID: {00000000-0000-0000-0000-000000000000} Target Server: Target Server Name: localhost Additional Information: localhost Process Information: Process ID: 0x224 Process Name: C:\Windows\System32\winlogon.exe Network Information: Network Address: 127.0.0.1 Port: 0 This event is generated when a process attempts to log on an account by explicitly specifying that account's credentials. This most commonly occurs in batch-type configurations such as scheduled tasks, or when using the RUNAS command.
	Audit		2015-04-		Microsoft-Windows-Security-	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: LTRANPHD$ Account Domain: WORKGROUP Logon ID: 0x3e7 Logon Type: 2 Impersonation Level: %%1833 New Logon: Security ID: S-1-5-21-1888849264-3803429180-4108621888-1001 Account Name: Liem Account Domain: LTRANPHD Logon ID: 0x1d4a5 Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x224 Process Name: C:\Windows\System32\winlogon.exe Network Information: Workstation Name: LTRANPHD Source Network Address: 127.0.0.1 Source Port: 0 Detailed Authentication Information: Logon Process: User32 Authentication Package: Negotiate Transited Services: - Package Name (NTLM only): - Key Length: 0 This event is generated when a logon session is created. It is generated on the computer that was accessed. The subject fields indicate the account on the local system which requested the logon. This is

Security	Success	12544	26 09:30:08	Auditing	most commonly a service such as the Server service, or a local process such as Winlogon.exe or Services.exe. The logon type field indicates the kind of logon that occurred. The most common types are 2 (interactive) and 3 (network). The New Logon fields indicate the account for whom the new logon was created, i.e. the account that was logged on. The network fields indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impersonation level field indicates the extent to which a process in the logon session can impersonate. The authentication information fields provide detailed information about this specific logon request. - Logon GUID is a unique identifier that can be used to correlate this event with a KDC event. - Transited services indicate which intermediate services have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indicates the length of the generated session key. This will be 0 if no session key was requested.
Security	Audit Success	12544	2015-04-26 09:30:08	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: LTRANPHD$ Account Domain: WORKGROUP Logon ID: 0x3e7 Logon Type: 2 Impersonation Level: %%1833 New Logon: Security ID: S-1-5-21-1888849264-3803429180-4108621888-1001 Account Name: Liem Account Domain: LTRANPHD Logon ID: 0x1d4d6 Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x224 Process Name: C:\Windows\System32\winlogon.exe Network Information: Workstation Name: LTRANPHD Source Network Address: 127.0.0.1 Source Port: 0 Detailed Authentication Information: Logon Process: User32 Authentication Package: Negotiate Transited Services: - Package Name (NTLM only): - Key Length: 0 This event is generated when a logon session is created. It is generated on the computer that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service such as the Server service, or a local process such as Winlogon.exe or Services.exe. The logon type field indicates the kind of logon that occurred. The most common types are 2 (interactive) and 3 (network). The New Logon fields indicate the account for whom the new logon was created, i.e. the account that was logged on. The network fields indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impersonation level field indicates the extent to which a process in the logon session can impersonate. The authentication information fields provide detailed information about this specific logon request. - Logon GUID is a unique identifier that can be used to correlate this event with a KDC event. - Transited services indicate which intermediate services have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indicates the length of the generated session key. This will be 0 if no session key was requested.
Security	Audit Success	12548	2015-04-26 09:30:08	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-21-1888849264-3803429180-4108621888-1001 Account Name: Liem Account Domain: LTRANPHD Logon ID: 0x1d4a5 Privileges: SeSecurityPrivilege SeTakeOwnershipPrivilege SeLoadDriverPrivilege SeBackupPrivilege SeRestorePrivilege SeDebugPrivilege SeSystemEnvironmentPrivilege SeImpersonatePrivilege
Security	Audit Success	12544	2015-04-26 09:30:09	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: LTRANPHD$ Account Domain: WORKGROUP Logon ID: 0x3e7 Logon Type: 5 Impersonation Level: %%1833 New Logon: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Logon ID: 0x3e7 Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x244 Process Name: C:\Windows\System32\services.exe Network Information: Workstation Name: Source Network Address: - Source Port: - Detailed Authentication Information: Logon Process: Advapi Authentication Package: Negotiate Transited Services: - Package Name (NTLM only): - Key Length: 0 This event is generated when a logon session is created. It is generated on the computer that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service such as the Server service, or a local process such as Winlogon.exe or Services.exe. The logon type field indicates the kind of logon that occurred. The most common types are 2 (interactive) and 3 (network). The New Logon fields indicate the account for whom the new logon was created, i.e. the account that was logged on. The network fields indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impersonation level field indicates the extent to which a process in the logon session can impersonate. The authentication information fields provide detailed information about this specific logon request. - Logon GUID is a unique identifier that can be used to correlate this event with a KDC event. - Transited services indicate which intermediate services have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indicates the length of the generated session key. This will be 0 if no session key was requested.
Security	Audit Success	12548	2015-04-26 09:30:09	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Logon ID: 0x3e7 Privileges: SeAssignPrimaryTokenPrivilege SeTcbPrivilege SeSecurityPrivilege SeTakeOwnershipPrivilege SeLoadDriverPrivilege SeBackupPrivilege SeRestorePrivilege SeDebugPrivilege SeAuditPrivilege SeSystemEnvironmentPrivilege SeImpersonatePrivilege
Security	Audit Success	13824	2015-04-26 09:30:10	Microsoft-Windows-Security-Auditing	4797: An attempt was made to query the existence of a blank password for an account. Subject: Security ID: S-1-5-21-1888849264-3803429180-4108621888-1001 Account Name: Liem Account Domain: LTRANPHD Logon ID: 0x1d4d6 Additional Information: Caller Workstation: LTRANPHD Target Account Name: Administrator Target Account Domain: LTRANPHD
Security	Audit Success	13824	2015-04-26 09:30:10	Microsoft-Windows-Security-Auditing	4797: An attempt was made to query the existence of a blank password for an account. Subject: Security ID: S-1-5-21-1888849264-3803429180-4108621888-1001 Account Name: Liem Account Domain: LTRANPHD Logon ID: 0x1d4d6 Additional Information: Caller Workstation: LTRANPHD Target Account Name: Guest Target Account Domain: LTRANPHD
	Audit		2015-04-	Microsoft-Windows-Security-	4797: An attempt was made to query the existence of a blank password for an account. Subject: Security ID: S-1-5-21-1888849264-3803429180-4108621888-1001 Account Name: Liem Account Domain: LTRANPHD Logon

Security	Success	13824	26 09:30:10	Auditing	ID: 0x1d4d6 Additional Information: Caller Workstation: LTRANPHD Target Account Name: Administrator Target Account Domain: LTRANPHD
Security	Audit Success	13824	2015-04-26 09:30:10	Microsoft-Windows-Security-Auditing	4797: An attempt was made to query the existence of a blank password for an account. Subject: Security ID: S-1-5-21-1888849264-3803429180-4108621888-1001 Account Name: Liem Account Domain: LTRANPHD Logon ID: 0x1d4d6 Additional Information: Caller Workstation: LTRANPHD Target Account Name: Guest Target Account Domain: LTRANPHD
Security	Audit Success	13824	2015-04-26 09:30:11	Microsoft-Windows-Security-Auditing	4797: An attempt was made to query the existence of a blank password for an account. Subject: Security ID: S-1-5-19 Account Name: LOCAL SERVICE Account Domain: NT AUTHORITY Logon ID: 0x3e5 Additional Information: Caller Workstation: LTRANPHD Target Account Name: Administrator Target Account Domain: LTRANPHD
Security	Audit Success	13824	2015-04-26 09:30:11	Microsoft-Windows-Security-Auditing	4797: An attempt was made to query the existence of a blank password for an account. Subject: Security ID: S-1-5-19 Account Name: LOCAL SERVICE Account Domain: NT AUTHORITY Logon ID: 0x3e5 Additional Information: Caller Workstation: LTRANPHD Target Account Name: Guest Target Account Domain: LTRANPHD
Security	Audit Success	13824	2015-04-26 09:30:11	Microsoft-Windows-Security-Auditing	4797: An attempt was made to query the existence of a blank password for an account. Subject: Security ID: S-1-5-19 Account Name: LOCAL SERVICE Account Domain: NT AUTHORITY Logon ID: 0x3e5 Additional Information: Caller Workstation: LTRANPHD Target Account Name: Administrator Target Account Domain: LTRANPHD
Security	Audit Success	13824	2015-04-26 09:30:11	Microsoft-Windows-Security-Auditing	4797: An attempt was made to query the existence of a blank password for an account. Subject: Security ID: S-1-5-19 Account Name: LOCAL SERVICE Account Domain: NT AUTHORITY Logon ID: 0x3e5 Additional Information: Caller Workstation: LTRANPHD Target Account Name: Liem Target Account Domain: LTRANPHD
Security	Audit Success	13824	2015-04-26 09:30:11	Microsoft-Windows-Security-Auditing	4797: An attempt was made to query the existence of a blank password for an account. Subject: Security ID: S-1-5-19 Account Name: LOCAL SERVICE Account Domain: NT AUTHORITY Logon ID: 0x3e5 Additional Information: Caller Workstation: LTRANPHD Target Account Name: Guest Target Account Domain: LTRANPHD
Security	Audit Success	13824	2015-04-26 09:30:11	Microsoft-Windows-Security-Auditing	4797: An attempt was made to query the existence of a blank password for an account. Subject: Security ID: S-1-5-19 Account Name: LOCAL SERVICE Account Domain: NT AUTHORITY Logon ID: 0x3e5 Additional Information: Caller Workstation: LTRANPHD Target Account Name: Liem Target Account Domain: LTRANPHD
Security	Audit Success	13824	2015-04-26 09:30:11	Microsoft-Windows-Security-Auditing	4797: An attempt was made to query the existence of a blank password for an account. Subject: Security ID: S-1-5-19 Account Name: LOCAL SERVICE Account Domain: NT AUTHORITY Logon ID: 0x3e5 Additional Information: Caller Workstation: LTRANPHD Target Account Name: Liem Target Account Domain: LTRANPHD
Security	Audit Success	13824	2015-04-26 09:30:11	Microsoft-Windows-Security-Auditing	4797: An attempt was made to query the existence of a blank password for an account. Subject: Security ID: S-1-5-19 Account Name: LOCAL SERVICE Account Domain: NT AUTHORITY Logon ID: 0x3e5 Additional Information: Caller Workstation: LTRANPHD Target Account Name: Liem Target Account Domain: LTRANPHD
Security	Audit Success	12544	2015-04-26 09:46:17	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: LTRANPHD$ Account Domain: WORKGROUP Logon ID: 0x3e7 Logon Type: 5 Impersonation Level: %%1833 New Logon: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Logon ID: 0x3e7 Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x244 Process Name: C:\Windows\System32\services.exe Network Information: Workstation Name: Source Network Address: - Source Port: - Detailed Authentication Information: Logon Process: Advapi Authentication Package: Negotiate Transited Services: - Package Name (NTLM only): - Key Length: 0 This event is generated when a logon session is created. It is generated on the computer that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service such as the Server service, or a local process such as Winlogon.exe or Services.exe. The logon type field indicates the kind of logon that occurred. The most common types are 2 (interactive) and 3 (network). The New Logon fields indicate the account for whom the new logon was created, i.e. the account that was logged on. The network fields indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impersonation level field indicates the extent to which a process in the logon session can impersonate. The authentication information fields provide detailed information about this specific logon request. - Logon GUID is a unique identifier that can be used to correlate this event with a KDC event. - Transited services indicate which intermediate services have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indicates the length of the generated session key. This will be 0 if no session key was requested.
Security	Audit Success	12548	2015-04-26 09:46:17	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Logon ID: 0x3e7 Privileges: SeAssignPrimaryTokenPrivilege SeTcbPrivilege SeSecurityPrivilege SeTakeOwnershipPrivilege SeLoadDriverPrivilege SeBackupPrivilege SeRestorePrivilege SeDebugPrivilege SeAuditPrivilege SeSystemEnvironmentPrivilege SeImpersonatePrivilege
Security	Audit Success	12288	2015-04-26 10:00:02	Microsoft-Windows-Security-Auditing	4608: Windows is starting up. This event is logged when LSASS.EXE starts and the auditing subsystem is initialized.
					4624: An account was successfully logged on. Subject: Security ID: S-1-0-0 Account Name: - Account Domain: - Logon ID: 0x0 Logon Type: 0 Impersonation Level: - New Logon: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Logon ID: 0x3e7 Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x4 Process Name: Network Information: Workstation Name: - Source Network Address: - Source Port: - Detailed Authentication Information: Logon Process: - Authentication Package: - Transited Services: - Package Name (NTLM only): - Key Length: 0 This event is

Security	Audit Success	12544	2015-04-26 10:00:02	Microsoft-Windows-Security-Auditing	generated when a logon session is created. It is generated on the computer that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service such as the Server service, or a local process such as Winlogon.exe or Services.exe. The logon type field indicates the kind of logon that occurred. The most common types are 2 (interactive) and 3 (network). The New Logon fields indicate the account for whom the new logon was created, i.e. the account that was logged on. The network fields indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impersonation level field indicates the extent to which a process in the logon session can impersonate. The authentication information fields provide detailed information about this specific logon request. - Logon GUID is a unique identifier that can be used to correlate this event with a KDC event. - Transited services indicate which intermediate services have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indicates the length of the generated session key. This will be 0 if no session key was requested.
Security	Audit Success	12544	2015-04-26 10:00:02	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: LTRANPHD$ Account Domain: WORKGROUP Logon ID: 0x3e7 Logon Type: 5 Impersonation Level: %%1833 New Logon: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Logon ID: 0x3e7 Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x238 Process Name: C:\Windows\System32\services.exe Network Information: Workstation Name: Source Network Address: - Source Port: - Detailed Authentication Information: Logon Process: Advapi Authentication Package: Negotiate Transited Services: - Package Name (NTLM only): - Key Length: 0 This event is generated when a logon session is created. It is generated on the computer that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service such as the Server service, or a local process such as Winlogon.exe or Services.exe. The logon type field indicates the kind of logon that occurred. The most common types are 2 (interactive) and 3 (network). The New Logon fields indicate the account for whom the new logon was created, i.e. the account that was logged on. The network fields indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impersonation level field indicates the extent to which a process in the logon session can impersonate. The authentication information fields provide detailed information about this specific logon request. - Logon GUID is a unique identifier that can be used to correlate this event with a KDC event. - Transited services indicate which intermediate services have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indicates the length of the generated session key. This will be 0 if no session key was requested.
Security	Audit Success	12544	2015-04-26 10:00:02	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: LTRANPHD$ Account Domain: WORKGROUP Logon ID: 0x3e7 Logon Type: 5 Impersonation Level: %%1833 New Logon: Security ID: S-1-5-20 Account Name: NETWORK SERVICE Account Domain: NT AUTHORITY Logon ID: 0x3e4 Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x238 Process Name: C:\Windows\System32\services.exe Network Information: Workstation Name: Source Network Address: - Source Port: - Detailed Authentication Information: Logon Process: Advapi Authentication Package: Negotiate Transited Services: - Package Name (NTLM only): - Key Length: 0 This event is generated when a logon session is created. It is generated on the computer that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service such as the Server service, or a local process such as Winlogon.exe or Services.exe. The logon type field indicates the kind of logon that occurred. The most common types are 2 (interactive) and 3 (network). The New Logon fields indicate the account for whom the new logon was created, i.e. the account that was logged on. The network fields indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impersonation level field indicates the extent to which a process in the logon session can impersonate. The authentication information fields provide detailed information about this specific logon request. - Logon GUID is a unique identifier that can be used to correlate this event with a KDC event. - Transited services indicate which intermediate services have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indicates the length of the generated session key. This will be 0 if no session key was requested.
Security	Audit Success	12544	2015-04-26 10:00:02	Microsoft-Windows-Security-Auditing	4648: A logon was attempted using explicit credentials. Subject: Security ID: S-1-5-18 Account Name: LTRANPHD$ Account Domain: WORKGROUP Logon ID: 0x3e7 Logon GUID: {00000000-0000-0000-0000-000000000000} Account Whose Credentials Were Used: Account Name: DWM-1 Account Domain: Window Manager Logon GUID: {00000000-0000-0000-0000-000000000000} Target Server: Target Server Name: localhost Additional Information: localhost Process Information: Process ID: 0x210 Process Name: C:\Windows\System32\winlogon.exe Network Information: Network Address: - Port: - This event is generated when a process attempts to log on an account by explicitly specifying that account's credentials. This most commonly occurs in batch-type configurations such as scheduled tasks, or when using the RUNAS command.
			2015-04-		4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: LTRANPHD$ Account Domain: WORKGROUP Logon ID: 0x3e7 Logon Type: 2 Impersonation Level: %%1833 New Logon: Security ID: S-1-5-90-1 Account Name: DWM-1 Account Domain: Window Manager Logon ID: 0xef54 Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x210 Process Name: C:\Windows\System32\winlogon.exe Network Information: Workstation Name: Source Network Address: - Source Port: - Detailed Authentication Information: Logon Process: Advapi Authentication Package: Negotiate Transited Services: - Package Name (NTLM only): - Key Length: 0 This event is generated when a logon session is created. It is generated on the computer that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service such as the Server service, or a local

Security	Audit Success	12544	26 10:00:02	Microsoft-Windows-Security-Auditing	process such as Winlogon.exe or Services.exe. The logon type field indicates the kind of logon that occurred. The most common types are 2 (interactive) and 3 (network). The New Logon fields indicate the account for whom the new logon was created, i.e. the account that was logged on. The network fields indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impersonation level field indicates the extent to which a process in the logon session can impersonate. The authentication information fields provide detailed information about this specific logon request. - Logon GUID is a unique identifier that can be used to correlate this event with a KDC event. - Transited services indicate which intermediate services have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indicates the length of the generated session key. This will be 0 if no session key was requested.
Security	Audit Success	12544	2015-04-26 10:00:02	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: LTRANPHD$ Account Domain: WORKGROUP Logon ID: 0x3e7 Logon Type: 2 Impersonation Level: %%1833 New Logon: Security ID: S-1-5-90-1 Account Name: DWM-1 Account Domain: Window Manager Logon ID: 0xef66 Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x210 Process Name: C:\Windows\System32\winlogon.exe Network Information: Workstation Name: Source Network Address: - Source Port: - Detailed Authentication Information: Logon Process: Advapi Authentication Package: Negotiate Transited Services: - Package Name (NTLM only): - Key Length: 0 This event is generated when a logon session is created. It is generated on the computer that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service such as the Server service, or a local process such as Winlogon.exe or Services.exe. The logon type field indicates the kind of logon that occurred. The most common types are 2 (interactive) and 3 (network). The New Logon fields indicate the account for whom the new logon was created, i.e. the account that was logged on. The network fields indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impersonation level field indicates the extent to which a process in the logon session can impersonate. The authentication information fields provide detailed information about this specific logon request. - Logon GUID is a unique identifier that can be used to correlate this event with a KDC event. - Transited services indicate which intermediate services have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indicates the length of the generated session key. This will be 0 if no session key was requested.
Security	Audit Success	12548	2015-04-26 10:00:02	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Logon ID: 0x3e7 Privileges: SeAssignPrimaryTokenPrivilege SeTcbPrivilege SeSecurityPrivilege SeTakeOwnershipPrivilege SeLoadDriverPrivilege SeBackupPrivilege SeRestorePrivilege SeDebugPrivilege SeAuditPrivilege SeSystemEnvironmentPrivilege SeImpersonatePrivilege
Security	Audit Success	12548	2015-04-26 10:00:02	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-20 Account Name: NETWORK SERVICE Account Domain: NT AUTHORITY Logon ID: 0x3e4 Privileges: SeAssignPrimaryTokenPrivilege SeAuditPrivilege SeImpersonatePrivilege
Security	Audit Success	12548	2015-04-26 10:00:02	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-90-1 Account Name: DWM-1 Account Domain: Window Manager Logon ID: 0xef54 Privileges: SeAssignPrimaryTokenPrivilege SeAuditPrivilege SeImpersonatePrivilege
Security	Audit Success	12548	2015-04-26 10:00:02	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-90-1 Account Name: DWM-1 Account Domain: Window Manager Logon ID: 0xef66 Privileges: SeAssignPrimaryTokenPrivilege SeAuditPrivilege
Security	Audit Success	13568	2015-04-26 10:00:02	Microsoft-Windows-Security-Auditing	4902: The Per-user audit policy table was created. Number of Elements: 0 Policy ID: 0x9c54
Security	Audit Success	12544	2015-04-26 10:00:03	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: LTRANPHD$ Account Domain: WORKGROUP Logon ID: 0x3e7 Logon Type: 5 Impersonation Level: %%1833 New Logon: Security ID: S-1-5-19 Account Name: LOCAL SERVICE Account Domain: NT AUTHORITY Logon ID: 0x3e5 Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x238 Process Name: C:\Windows\System32\services.exe Network Information: Workstation Name: Source Network Address: - Source Port: - Detailed Authentication Information: Logon Process: Advapi Authentication Package: Negotiate Transited Services: - Package Name (NTLM only): - Key Length: 0 This event is generated when a logon session is created. It is generated on the computer that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service such as the Server service, or a local process such as Winlogon.exe or Services.exe. The logon type field indicates the kind of logon that occurred. The most common types are 2 (interactive) and 3 (network). The New Logon fields indicate the account for whom the new logon was created, i.e. the account that was logged on. The network fields indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impersonation level field indicates the extent to which a process in the logon session can impersonate. The authentication information fields provide detailed information about this specific logon request. - Logon GUID is a unique identifier that can be used to correlate this event with a KDC event. - Transited services indicate which intermediate services have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indicates the length of the generated session key. This will be 0 if no session key was requested.
					4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: LTRANPHD$

Security	Audit Success	12544	2015-04-26 10:00:03	Microsoft-Windows-Security-Auditing	Account Domain: WORKGROUP Logon ID: 0x3e7 Logon Type: 5 Impersonation Level: %%1833 New Logon: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Logon ID: 0x3e7 Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x238 Process Name: C:\Windows\System32\services.exe Network Information: Workstation Name: Source Network Address: - Source Port: - Detailed Authentication Information: Logon Process: Advapi Authentication Package: Negotiate Transited Services: - Package Name (NTLM only): - Key Length: 0 This event is generated when a logon session is created. It is generated on the computer that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service such as the Server service, or a local process such as Winlogon.exe or Services.exe. The logon type field indicates the kind of logon that occurred. The most common types are 2 (interactive) and 3 (network). The New Logon fields indicate the account for whom the new logon was created, i.e. the account that was logged on. The network fields indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impersonation level field indicates the extent to which a process in the logon session can impersonate. The authentication information fields provide detailed information about this specific logon request. - Logon GUID is a unique identifier that can be used to correlate this event with a KDC event. - Transited services indicate which intermediate services have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indicates the length of the generated session key. This will be 0 if no session key was requested.
Security	Audit Success	12544	2015-04-26 10:00:03	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: LTRANPHD$ Account Domain: WORKGROUP Logon ID: 0x3e7 Logon Type: 5 Impersonation Level: %%1833 New Logon: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Logon ID: 0x3e7 Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x238 Process Name: C:\Windows\System32\services.exe Network Information: Workstation Name: Source Network Address: - Source Port: - Detailed Authentication Information: Logon Process: Advapi Authentication Package: Negotiate Transited Services: - Package Name (NTLM only): - Key Length: 0 This event is generated when a logon session is created. It is generated on the computer that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service such as the Server service, or a local process such as Winlogon.exe or Services.exe. The logon type field indicates the kind of logon that occurred. The most common types are 2 (interactive) and 3 (network). The New Logon fields indicate the account for whom the new logon was created, i.e. the account that was logged on. The network fields indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impersonation level field indicates the extent to which a process in the logon session can impersonate. The authentication information fields provide detailed information about this specific logon request. - Logon GUID is a unique identifier that can be used to correlate this event with a KDC event. - Transited services indicate which intermediate services have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indicates the length of the generated session key. This will be 0 if no session key was requested.
Security	Audit Success	12544	2015-04-26 10:00:03	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: LTRANPHD$ Account Domain: WORKGROUP Logon ID: 0x3e7 Logon Type: 5 Impersonation Level: %%1833 New Logon: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Logon ID: 0x3e7 Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x238 Process Name: C:\Windows\System32\services.exe Network Information: Workstation Name: Source Network Address: - Source Port: - Detailed Authentication Information: Logon Process: Advapi Authentication Package: Negotiate Transited Services: - Package Name (NTLM only): - Key Length: 0 This event is generated when a logon session is created. It is generated on the computer that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service such as the Server service, or a local process such as Winlogon.exe or Services.exe. The logon type field indicates the kind of logon that occurred. The most common types are 2 (interactive) and 3 (network). The New Logon fields indicate the account for whom the new logon was created, i.e. the account that was logged on. The network fields indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impersonation level field indicates the extent to which a process in the logon session can impersonate. The authentication information fields provide detailed information about this specific logon request. - Logon GUID is a unique identifier that can be used to correlate this event with a KDC event. - Transited services indicate which intermediate services have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indicates the length of the generated session key. This will be 0 if no session key was requested.
Security	Audit Success	12548	2015-04-26 10:00:03	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-19 Account Name: LOCAL SERVICE Account Domain: NT AUTHORITY Logon ID: 0x3e5 Privileges: SeAssignPrimaryTokenPrivilege SeAuditPrivilege SeImpersonatePrivilege
Security	Audit Success	12548	2015-04-26 10:00:03	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Logon ID: 0x3e7 Privileges: SeAssignPrimaryTokenPrivilege SeTcbPrivilege SeSecurityPrivilege SeTakeOwnershipPrivilege SeLoadDriverPrivilege SeBackupPrivilege SeRestorePrivilege SeDebugPrivilege SeAuditPrivilege SeSystemEnvironmentPrivilege SeImpersonatePrivilege
Security	Audit Success	12548	2015-04-26 10:00:03	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Logon ID: 0x3e7 Privileges: SeAssignPrimaryTokenPrivilege SeTcbPrivilege SeSecurityPrivilege SeTakeOwnershipPrivilege SeLoadDriverPrivilege SeBackupPrivilege SeRestorePrivilege

					SeDebugPrivilege SeAuditPrivilege SeSystemEnvironmentPrivilege SeImpersonatePrivilege
Security	Audit Success	12548	2015-04-26 10:00:03	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Logon ID: 0x3e7 Privileges: SeAssignPrimaryTokenPrivilege SeTcbPrivilege SeSecurityPrivilege SeTakeOwnershipPrivilege SeLoadDriverPrivilege SeBackupPrivilege SeRestorePrivilege SeDebugPrivilege SeAuditPrivilege SeSystemEnvironmentPrivilege SeImpersonatePrivilege
Security	Audit Success	101	2015-04-26 10:00:04	Microsoft-Windows-Eventlog	1101: Audit events have been dropped by the transport. 0
Security	Audit Success	12292	2015-04-26 10:00:04	Microsoft-Windows-Security-Auditing	5033: The Windows Firewall Driver started successfully.
Security	Audit Success	12292	2015-04-26 10:00:04	Microsoft-Windows-Security-Auditing	5024: The Windows Firewall service started successfully.
Security	Audit Success	12544	2015-04-26 10:00:04	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: LTRANPHD$ Account Domain: WORKGROUP Logon ID: 0x3e7 Logon Type: 5 Impersonation Level: %%1833 New Logon: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Logon ID: 0x3e7 Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x238 Process Name: C:\Windows\System32\services.exe Network Information: Workstation Name: Source Network Address: - Source Port: - Detailed Authentication Information: Logon Process: Advapi Authentication Package: Negotiate Transited Services: - Package Name (NTLM only): - Key Length: 0 This event is generated when a logon session is created. It is generated on the computer that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service such as the Server service, or a local process such as Winlogon.exe or Services.exe. The logon type field indicates the kind of logon that occurred. The most common types are 2 (interactive) and 3 (network). The New Logon fields indicate the account for whom the new logon was created, i.e. the account that was logged on. The network fields indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impersonation level field indicates the extent to which a process in the logon session can impersonate. The authentication information fields provide detailed information about this specific logon request. - Logon GUID is a unique identifier that can be used to correlate this event with a KDC event. - Transited services indicate which intermediate services have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indicates the length of the generated session key. This will be 0 if no session key was requested.
Security	Audit Success	12544	2015-04-26 10:00:04	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: LTRANPHD$ Account Domain: WORKGROUP Logon ID: 0x3e7 Logon Type: 5 Impersonation Level: %%1833 New Logon: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Logon ID: 0x3e7 Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x238 Process Name: C:\Windows\System32\services.exe Network Information: Workstation Name: Source Network Address: - Source Port: - Detailed Authentication Information: Logon Process: Advapi Authentication Package: Negotiate Transited Services: - Package Name (NTLM only): - Key Length: 0 This event is generated when a logon session is created. It is generated on the computer that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service such as the Server service, or a local process such as Winlogon.exe or Services.exe. The logon type field indicates the kind of logon that occurred. The most common types are 2 (interactive) and 3 (network). The New Logon fields indicate the account for whom the new logon was created, i.e. the account that was logged on. The network fields indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impersonation level field indicates the extent to which a process in the logon session can impersonate. The authentication information fields provide detailed information about this specific logon request. - Logon GUID is a unique identifier that can be used to correlate this event with a KDC event. - Transited services indicate which intermediate services have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indicates the length of the generated session key. This will be 0 if no session key was requested.
Security	Audit Success	12548	2015-04-26 10:00:04	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Logon ID: 0x3e7 Privileges: SeAssignPrimaryTokenPrivilege SeTcbPrivilege SeSecurityPrivilege SeTakeOwnershipPrivilege SeLoadDriverPrivilege SeBackupPrivilege SeRestorePrivilege SeDebugPrivilege SeAuditPrivilege SeSystemEnvironmentPrivilege SeImpersonatePrivilege
Security	Audit Success	12548	2015-04-26 10:00:04	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Logon ID: 0x3e7 Privileges: SeAssignPrimaryTokenPrivilege SeTcbPrivilege SeSecurityPrivilege SeTakeOwnershipPrivilege SeLoadDriverPrivilege SeBackupPrivilege SeRestorePrivilege SeDebugPrivilege SeAuditPrivilege SeSystemEnvironmentPrivilege SeImpersonatePrivilege
					4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: LTRANPHD$ Account Domain: WORKGROUP Logon ID: 0x3e7 Logon Type: 5 Impersonation Level: %%1833 New Logon: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Logon ID: 0x3e7 Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x238 Process Name: C:\Windows\System32\services.exe Network Information: Workstation Name: Source Network Address: - Source

Security	Audit Success	12544	2015-04-26 10:00:05	Microsoft-Windows-Security-Auditing	Port: - Detailed Authentication Information: Logon Process: Advapi Authentication Package: Negotiate Transited Services: - Package Name (NTLM only): - Key Length: 0 This event is generated when a logon session is created. It is generated on the computer that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service such as the Server service, or a local process such as Winlogon.exe or Services.exe. The logon type field indicates the kind of logon that occurred. The most common types are 2 (interactive) and 3 (network). The New Logon fields indicate the account for whom the new logon was created, i.e. the account that was logged on. The network fields indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impersonation level field indicates the extent to which a process in the logon session can impersonate. The authentication information fields provide detailed information about this specific logon request. - Logon GUID is a unique identifier that can be used to correlate this event with a KDC event. - Transited services indicate which intermediate services have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indicates the length of the generated session key. This will be 0 if no session key was requested.
Security	Audit Success	12544	2015-04-26 10:00:05	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-0-0 Account Name: - Account Domain: - Logon ID: 0x0 Logon Type: 3 Impersonation Level: %%1833 New Logon: Security ID: S-1-5-7 Account Name: ANONYMOUS LOGON Account Domain: NT AUTHORITY Logon ID: 0x19479 Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x0 Process Name: - Network Information: Workstation Name: Source Network Address: - Source Port: - Detailed Authentication Information: Logon Process: NtLmSsp Authentication Package: NTLM Transited Services: - Package Name (NTLM only): NTLM V1 Key Length: 0 This event is generated when a logon session is created. It is generated on the computer that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service such as the Server service, or a local process such as Winlogon.exe or Services.exe. The logon type field indicates the kind of logon that occurred. The most common types are 2 (interactive) and 3 (network). The New Logon fields indicate the account for whom the new logon was created, i.e. the account that was logged on. The network fields indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impersonation level field indicates the extent to which a process in the logon session can impersonate. The authentication information fields provide detailed information about this specific logon request. - Logon GUID is a unique identifier that can be used to correlate this event with a KDC event. - Transited services indicate which intermediate services have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indicates the length of the generated session key. This will be 0 if no session key was requested.
Security	Audit Success	12548	2015-04-26 10:00:05	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Logon ID: 0x3e7 Privileges: SeAssignPrimaryTokenPrivilege SeTcbPrivilege SeSecurityPrivilege SeTakeOwnershipPrivilege SeLoadDriverPrivilege SeBackupPrivilege SeRestorePrivilege SeDebugPrivilege SeAuditPrivilege SeSystemEnvironmentPrivilege SeImpersonatePrivilege
Security	Audit Success	12544	2015-04-26 10:00:11	Microsoft-Windows-Security-Auditing	4648: A logon was attempted using explicit credentials. Subject: Security ID: S-1-5-18 Account Name: LTRANPHD$ Account Domain: WORKGROUP Logon ID: 0x3e7 Logon GUID: {00000000-0000-0000-0000-000000000000} Account Whose Credentials Were Used: Account Name: Liem Account Domain: LTRANPHD Logon GUID: {00000000-0000-0000-0000-000000000000} Target Server: Target Server Name: localhost Additional Information: localhost Process Information: Process ID: 0x210 Process Name: C:\Windows\System32\winlogon.exe Network Information: Network Address: 127.0.0.1 Port: 0 This event is generated when a process attempts to log on an account by explicitly specifying that account's credentials. This most commonly occurs in batch-type configurations such as scheduled tasks, or when using the RUNAS command.
Security	Audit Success	12544	2015-04-26 10:00:11	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: LTRANPHD$ Account Domain: WORKGROUP Logon ID: 0x3e7 Logon Type: 2 Impersonation Level: %%1833 New Logon: Security ID: S-1-5-21-1888849264-3803429180-4108621888-1001 Account Name: Liem Account Domain: LTRANPHD Logon ID: 0x21af7 Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x210 Process Name: C:\Windows\System32\winlogon.exe Network Information: Workstation Name: LTRANPHD Source Network Address: 127.0.0.1 Source Port: 0 Detailed Authentication Information: Logon Process: User32 Authentication Package: Negotiate Transited Services: - Package Name (NTLM only): - Key Length: 0 This event is generated when a logon session is created. It is generated on the computer that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service such as the Server service, or a local process such as Winlogon.exe or Services.exe. The logon type field indicates the kind of logon that occurred. The most common types are 2 (interactive) and 3 (network). The New Logon fields indicate the account for whom the new logon was created, i.e. the account that was logged on. The network fields indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impersonation level field indicates the extent to which a process in the logon session can impersonate. The authentication information fields provide detailed information about this specific logon request. - Logon GUID is a unique identifier that can be used to correlate this event with a KDC event. - Transited services indicate which intermediate services have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indicates the length of the generated session key. This will be 0 if no session key was requested.
					4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: LTRANPHD$ Account Domain: WORKGROUP Logon ID: 0x3e7 Logon Type: 2 Impersonation Level: %%1833 New Logon:

Security	Audit Success	12544	2015-04-26 10:00:11	Microsoft-Windows-Security-Auditing	Security ID: S-1-5-21-1888849264-3803429180-4108621888-1001 Account Name: Liem Account Domain: LTRANPHD Logon ID: 0x21b53 Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x210 Process Name: C:\Windows\System32\winlogon.exe Network Information: Workstation Name: LTRANPHD Source Network Address: 127.0.0.1 Source Port: 0 Detailed Authentication Information: Logon Process: User32 Authentication Package: Negotiate Transited Services: - Package Name (NTLM only): - Key Length: 0 This event is generated when a logon session is created. It is generated on the computer that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service such as the Server service, or a local process such as Winlogon.exe or Services.exe. The logon type field indicates the kind of logon that occurred. The most common types are 2 (interactive) and 3 (network). The New Logon fields indicate the account for whom the new logon was created, i.e. the account that was logged on. The network fields indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impersonation level field indicates the extent to which a process in the logon session can impersonate. The authentication information fields provide detailed information about this specific logon request. - Logon GUID is a unique identifier that can be used to correlate this event with a KDC event. - Transited services indicate which intermediate services have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indicates the length of the generated session key. This will be 0 if no session key was requested.
Security	Audit Success	12544	2015-04-26 10:00:11	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: LTRANPHD$ Account Domain: WORKGROUP Logon ID: 0x3e7 Logon Type: 5 Impersonation Level: %%1833 New Logon: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Logon ID: 0x3e7 Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x238 Process Name: C:\Windows\System32\services.exe Network Information: Workstation Name: Source Network Address: - Source Port: - Detailed Authentication Information: Logon Process: Advapi Authentication Package: Negotiate Transited Services: - Package Name (NTLM only): - Key Length: 0 This event is generated when a logon session is created. It is generated on the computer that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service such as the Server service, or a local process such as Winlogon.exe or Services.exe. The logon type field indicates the kind of logon that occurred. The most common types are 2 (interactive) and 3 (network). The New Logon fields indicate the account for whom the new logon was created, i.e. the account that was logged on. The network fields indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impersonation level field indicates the extent to which a process in the logon session can impersonate. The authentication information fields provide detailed information about this specific logon request. - Logon GUID is a unique identifier that can be used to correlate this event with a KDC event. - Transited services indicate which intermediate services have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indicates the length of the generated session key. This will be 0 if no session key was requested.
Security	Audit Success	12548	2015-04-26 10:00:11	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-21-1888849264-3803429180-4108621888-1001 Account Name: Liem Account Domain: LTRANPHD Logon ID: 0x21af7 Privileges: SeSecurityPrivilege SeTakeOwnershipPrivilege SeLoadDriverPrivilege SeBackupPrivilege SeRestorePrivilege SeDebugPrivilege SeSystemEnvironmentPrivilege SeImpersonatePrivilege
Security	Audit Success	12548	2015-04-26 10:00:11	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Logon ID: 0x3e7 Privileges: SeAssignPrimaryTokenPrivilege SeTcbPrivilege SeSecurityPrivilege SeTakeOwnershipPrivilege SeLoadDriverPrivilege SeBackupPrivilege SeRestorePrivilege SeDebugPrivilege SeAuditPrivilege SeSystemEnvironmentPrivilege SeImpersonatePrivilege
Security	Audit Success	13824	2015-04-26 10:00:13	Microsoft-Windows-Security-Auditing	4797: An attempt was made to query the existence of a blank password for an account. Subject: Security ID: S-1-5-19 Account Name: LOCAL SERVICE Account Domain: NT AUTHORITY Logon ID: 0x3e5 Additional Information: Caller Workstation: LTRANPHD Target Account Name: Administrator Target Account Domain: LTRANPHD
Security	Audit Success	13824	2015-04-26 10:00:13	Microsoft-Windows-Security-Auditing	4797: An attempt was made to query the existence of a blank password for an account. Subject: Security ID: S-1-5-19 Account Name: LOCAL SERVICE Account Domain: NT AUTHORITY Logon ID: 0x3e5 Additional Information: Caller Workstation: LTRANPHD Target Account Name: Guest Target Account Domain: LTRANPHD
Security	Audit Success	13824	2015-04-26 10:00:13	Microsoft-Windows-Security-Auditing	4797: An attempt was made to query the existence of a blank password for an account. Subject: Security ID: S-1-5-19 Account Name: LOCAL SERVICE Account Domain: NT AUTHORITY Logon ID: 0x3e5 Additional Information: Caller Workstation: LTRANPHD Target Account Name: Liem Target Account Domain: LTRANPHD
Security	Audit Success	13824	2015-04-26 10:00:13	Microsoft-Windows-Security-Auditing	4797: An attempt was made to query the existence of a blank password for an account. Subject: Security ID: S-1-5-19 Account Name: LOCAL SERVICE Account Domain: NT AUTHORITY Logon ID: 0x3e5 Additional Information: Caller Workstation: LTRANPHD Target Account Name: Liem Target Account Domain: LTRANPHD
Security	Audit Success	13824	2015-04-26 10:00:13	Microsoft-Windows-Security-Auditing	4797: An attempt was made to query the existence of a blank password for an account. Subject: Security ID: S-1-5-19 Account Name: LOCAL SERVICE Account Domain: NT AUTHORITY Logon ID: 0x3e5 Additional Information: Caller Workstation: LTRANPHD Target Account Name: Administrator Target Account Domain: LTRANPHD
Security	Audit Success	13824	2015-04-26 10:00:13	Microsoft-Windows-Security-Auditing	4797: An attempt was made to query the existence of a blank password for an account. Subject: Security ID: S-1-5-19 Account Name: LOCAL SERVICE Account Domain: NT AUTHORITY Logon ID: 0x3e5 Additional Information: Caller Workstation: LTRANPHD Target Account Name: Guest Target Account Domain: LTRANPHD
Security	Audit		2015-04-	Microsoft-Windows-Security-	4797: An attempt was made to query the existence of a blank password for an account. Subject: Security ID:

Security	Success	13824	26 10:00:13	Auditing	S-1-5-19 Account Name: LOCAL SERVICE Account Domain: NT AUTHORITY Logon ID: 0x3e5 Additional Information: Caller Workstation: LTRANPHD Target Account Name: Liem Target Account Domain: LTRANPHD
Security	Audit Success	13824	2015-04-26 10:00:13	Microsoft-Windows-Security-Auditing	4797: An attempt was made to query the existence of a blank password for an account. Subject: Security ID: S-1-5-19 Account Name: LOCAL SERVICE Account Domain: NT AUTHORITY Logon ID: 0x3e5 Additional Information: Caller Workstation: LTRANPHD Target Account Name: Liem Target Account Domain: LTRANPHD
Security	Audit Success	13824	2015-04-26 10:00:13	Microsoft-Windows-Security-Auditing	4797: An attempt was made to query the existence of a blank password for an account. Subject: Security ID: S-1-5-21-1888849264-3803429180-4108621888-1001 Account Name: Liem Account Domain: LTRANPHD Logon ID: 0x21b53 Additional Information: Caller Workstation: LTRANPHD Target Account Name: Administrator Target Account Domain: LTRANPHD
Security	Audit Success	13824	2015-04-26 10:00:13	Microsoft-Windows-Security-Auditing	4797: An attempt was made to query the existence of a blank password for an account. Subject: Security ID: S-1-5-21-1888849264-3803429180-4108621888-1001 Account Name: Liem Account Domain: LTRANPHD Logon ID: 0x21b53 Additional Information: Caller Workstation: LTRANPHD Target Account Name: Guest Target Account Domain: LTRANPHD
Security	Audit Success	13824	2015-04-26 10:00:13	Microsoft-Windows-Security-Auditing	4797: An attempt was made to query the existence of a blank password for an account. Subject: Security ID: S-1-5-21-1888849264-3803429180-4108621888-1001 Account Name: Liem Account Domain: LTRANPHD Logon ID: 0x21b53 Additional Information: Caller Workstation: LTRANPHD Target Account Name: Administrator Target Account Domain: LTRANPHD
Security	Audit Success	13824	2015-04-26 10:00:13	Microsoft-Windows-Security-Auditing	4797: An attempt was made to query the existence of a blank password for an account. Subject: Security ID: S-1-5-21-1888849264-3803429180-4108621888-1001 Account Name: Liem Account Domain: LTRANPHD Logon ID: 0x21b53 Additional Information: Caller Workstation: LTRANPHD Target Account Name: Guest Target Account Domain: LTRANPHD
Security	Audit Success	12544	2015-04-26 10:10:10	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: LTRANPHD$ Account Domain: WORKGROUP Logon ID: 0x3e7 Logon Type: 5 Impersonation Level: %%1833 New Logon: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Logon ID: 0x3e7 Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x238 Process Name: C:\Windows\System32\services.exe Network Information: Workstation Name: Source Network Address: - Source Port: - Detailed Authentication Information: Logon Process: Advapi Authentication Package: Negotiate Transited Services: - Package Name (NTLM only): - Key Length: 0 This event is generated when a logon session is created. It is generated on the computer that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service such as the Server service, or a local process such as Winlogon.exe or Services.exe. The logon type field indicates the kind of logon that occurred. The most common types are 2 (interactive) and 3 (network). The New Logon fields indicate the account for whom the new logon was created, i.e. the account that was logged on. The network fields indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impersonation level field indicates the extent to which a process in the logon session can impersonate. The authentication information fields provide detailed information about this specific logon request. - Logon GUID is a unique identifier that can be used to correlate this event with a KDC event. - Transited services indicate which intermediate services have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indicates the length of the generated session key. This will be 0 if no session key was requested.
Security	Audit Success	12548	2015-04-26 10:10:10	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Logon ID: 0x3e7 Privileges: SeAssignPrimaryTokenPrivilege SeTcbPrivilege SeSecurityPrivilege SeTakeOwnershipPrivilege SeLoadDriverPrivilege SeBackupPrivilege SeRestorePrivilege SeDebugPrivilege SeAuditPrivilege SeSystemEnvironmentPrivilege SeImpersonatePrivilege
Security	Audit Success	12544	2015-04-26 12:25:56	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: LTRANPHD$ Account Domain: WORKGROUP Logon ID: 0x3e7 Logon Type: 5 Impersonation Level: %%1833 New Logon: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Logon ID: 0x3e7 Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x238 Process Name: C:\Windows\System32\services.exe Network Information: Workstation Name: Source Network Address: - Source Port: - Detailed Authentication Information: Logon Process: Advapi Authentication Package: Negotiate Transited Services: - Package Name (NTLM only): - Key Length: 0 This event is generated when a logon session is created. It is generated on the computer that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service such as the Server service, or a local process such as Winlogon.exe or Services.exe. The logon type field indicates the kind of logon that occurred. The most common types are 2 (interactive) and 3 (network). The New Logon fields indicate the account for whom the new logon was created, i.e. the account that was logged on. The network fields indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impersonation level field indicates the extent to which a process in the logon session can impersonate. The authentication information fields provide detailed information about this specific logon request. - Logon GUID is a unique identifier that can be used to correlate this event with a KDC event. - Transited services indicate which intermediate services have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indicates the length of the generated session key. This will be 0 if no session key was requested.
Security	Audit	12548	2015-04-26	Microsoft-Windows-Security-	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Logon ID: 0x3e7 Privileges: SeAssignPrimaryTokenPrivilege SeTcbPrivilege

	Success		12:25:56	Auditing	SeSecurityPrivilege SeTakeOwnershipPrivilege SeLoadDriverPrivilege SeBackupPrivilege SeRestorePrivilege SeDebugPrivilege SeAuditPrivilege SeSystemEnvironmentPrivilege SeImpersonatePrivilege
Security	Audit Success	12544	2015-04-26 12:26:04	Microsoft-Windows-Security-Auditing	4648: A logon was attempted using explicit credentials. Subject: Security ID: S-1-5-18 Account Name: LTRANPHD$ Account Domain: WORKGROUP Logon ID: 0x3e7 Logon GUID: {00000000-0000-0000-0000-000000000000} Account Whose Credentials Were Used: Account Name: Liem Account Domain: LTRANPHD Logon GUID: {00000000-0000-0000-0000-000000000000} Target Server: Target Server Name: localhost Additional Information: localhost Process Information: Process ID: 0x210 Process Name: C:\Windows\System32\winlogon.exe Network Information: Network Address: 127.0.0.1 Port: 0 This event is generated when a process attempts to log on an account by explicitly specifying that account's credentials. This most commonly occurs in batch-type configurations such as scheduled tasks, or when using the RUNAS command.
Security	Audit Success	12544	2015-04-26 12:26:04	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: LTRANPHD$ Account Domain: WORKGROUP Logon ID: 0x3e7 Logon Type: 7 Impersonation Level: %%1833 New Logon: Security ID: S-1-5-21-1888849264-3803429180-4108621888-1001 Account Name: Liem Account Domain: LTRANPHD Logon ID: 0xe6546 Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x210 Process Name: C:\Windows\System32\winlogon.exe Network Information: Workstation Name: LTRANPHD Source Network Address: 127.0.0.1 Source Port: 0 Detailed Authentication Information: Logon Process: User32 Authentication Package: Negotiate Transited Services: - Package Name (NTLM only): - Key Length: 0 This event is generated when a logon session is created. It is generated on the computer that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service such as the Server service, or a local process such as Winlogon.exe or Services.exe. The logon type field indicates the kind of logon that occurred. The most common types are 2 (interactive) and 3 (network). The New Logon fields indicate the account for whom the new logon was created, i.e. the account that was logged on. The network fields indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impersonation level field indicates the extent to which a process in the logon session can impersonate. The authentication information fields provide detailed information about this specific logon request. - Logon GUID is a unique identifier that can be used to correlate this event with a KDC event. - Transited services indicate which intermediate services have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indicates the length of the generated session key. This will be 0 if no session key was requested.
Security	Audit Success	12544	2015-04-26 12:26:04	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: LTRANPHD$ Account Domain: WORKGROUP Logon ID: 0x3e7 Logon Type: 7 Impersonation Level: %%1833 New Logon: Security ID: S-1-5-21-1888849264-3803429180-4108621888-1001 Account Name: Liem Account Domain: LTRANPHD Logon ID: 0xe6567 Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x210 Process Name: C:\Windows\System32\winlogon.exe Network Information: Workstation Name: LTRANPHD Source Network Address: 127.0.0.1 Source Port: 0 Detailed Authentication Information: Logon Process: User32 Authentication Package: Negotiate Transited Services: - Package Name (NTLM only): - Key Length: 0 This event is generated when a logon session is created. It is generated on the computer that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service such as the Server service, or a local process such as Winlogon.exe or Services.exe. The logon type field indicates the kind of logon that occurred. The most common types are 2 (interactive) and 3 (network). The New Logon fields indicate the account for whom the new logon was created, i.e. the account that was logged on. The network fields indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impersonation level field indicates the extent to which a process in the logon session can impersonate. The authentication information fields provide detailed information about this specific logon request. - Logon GUID is a unique identifier that can be used to correlate this event with a KDC event. - Transited services indicate which intermediate services have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indicates the length of the generated session key. This will be 0 if no session key was requested.
Security	Audit Success	12545	2015-04-26 12:26:04	Microsoft-Windows-Security-Auditing	4634: An account was logged off. Subject: Security ID: S-1-5-21-1888849264-3803429180-4108621888-1001 Account Name: Liem Account Domain: LTRANPHD Logon ID: 0xe6567 Logon Type: 7 This event is generated when a logon session is destroyed. It may be positively correlated with a logon event using the Logon ID value. Logon IDs are only unique between reboots on the same computer.
Security	Audit Success	12545	2015-04-26 12:26:04	Microsoft-Windows-Security-Auditing	4634: An account was logged off. Subject: Security ID: S-1-5-21-1888849264-3803429180-4108621888-1001 Account Name: Liem Account Domain: LTRANPHD Logon ID: 0xe6546 Logon Type: 7 This event is generated when a logon session is destroyed. It may be positively correlated with a logon event using the Logon ID value. Logon IDs are only unique between reboots on the same computer.
Security	Audit Success	12548	2015-04-26 12:26:04	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-21-1888849264-3803429180-4108621888-1001 Account Name: Liem Account Domain: LTRANPHD Logon ID: 0xe6546 Privileges: SeSecurityPrivilege SeTakeOwnershipPrivilege SeLoadDriverPrivilege SeBackupPrivilege SeRestorePrivilege SeDebugPrivilege SeSystemEnvironmentPrivilege SeImpersonatePrivilege
					4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: LTRANPHD$ Account Domain: WORKGROUP Logon ID: 0x3e7 Logon Type: 5 Impersonation Level: %%1833 New Logon: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Logon ID: 0x3e7 Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x238 Process Name: C:\Windows\System32\services.exe Network Information: Workstation Name: Source Network Address: - Source

Security	Audit Success	12544	2015-04-26 12:40:01	Microsoft-Windows-Security-Auditing	Port: - Detailed Authentication Information: Logon Process: Advapi Authentication Package: Negotiate Transited Services: - Package Name (NTLM only): - Key Length: 0 This event is generated when a logon session is created. It is generated on the computer that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service such as the Server service, or a local process such as Winlogon.exe or Services.exe. The logon type field indicates the kind of logon that occurred. The most common types are 2 (interactive) and 3 (network). The New Logon fields indicate the account for whom the new logon was created, i.e. the account that was logged on. The network fields indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impersonation level field indicates the extent to which a process in the logon session can impersonate. The authentication information fields provide detailed information about this specific logon request. - Logon GUID is a unique identifier that can be used to correlate this event with a KDC event. - Transited services indicate which intermediate services have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indicates the length of the generated session key. This will be 0 if no session key was requested.
Security	Audit Success	12548	2015-04-26 12:40:01	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Logon ID: 0x3e7 Privileges: SeAssignPrimaryTokenPrivilege SeTcbPrivilege SeSecurityPrivilege SeTakeOwnershipPrivilege SeLoadDriverPrivilege SeBackupPrivilege SeRestorePrivilege SeDebugPrivilege SeAuditPrivilege SeSystemEnvironmentPrivilege SeImpersonatePrivilege
Security	Audit Success	12288	2015-04-26 12:56:08	Microsoft-Windows-Security-Auditing	4608: Windows is starting up. This event is logged when LSASS.EXE starts and the auditing subsystem is initialized.
Security	Audit Success	12544	2015-04-26 12:56:08	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-0-0 Account Name: - Account Domain: - Logon ID: 0x0 Logon Type: 0 Impersonation Level: - New Logon: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Logon ID: 0x3e7 Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x4 Process Name: Network Information: Workstation Name: - Source Network Address: - Source Port: - Detailed Authentication Information: Logon Process: - Authentication Package: - Transited Services: - Package Name (NTLM only): - Key Length: 0 This event is generated when a logon session is created. It is generated on the computer that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service such as the Server service, or a local process such as Winlogon.exe or Services.exe. The logon type field indicates the kind of logon that occurred. The most common types are 2 (interactive) and 3 (network). The New Logon fields indicate the account for whom the new logon was created, i.e. the account that was logged on. The network fields indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impersonation level field indicates the extent to which a process in the logon session can impersonate. The authentication information fields provide detailed information about this specific logon request. - Logon GUID is a unique identifier that can be used to correlate this event with a KDC event. - Transited services indicate which intermediate services have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indicates the length of the generated session key. This will be 0 if no session key was requested.
Security	Audit Success	12544	2015-04-26 12:56:08	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: LTRANPHD$ Account Domain: WORKGROUP Logon ID: 0x3e7 Logon Type: 5 Impersonation Level: %%1833 New Logon: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Logon ID: 0x3e7 Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x234 Process Name: C:\Windows\System32\services.exe Network Information: Workstation Name: Source Network Address: - Source Port: - Detailed Authentication Information: Logon Process: Advapi Authentication Package: Negotiate Transited Services: - Package Name (NTLM only): - Key Length: 0 This event is generated when a logon session is created. It is generated on the computer that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service such as the Server service, or a local process such as Winlogon.exe or Services.exe. The logon type field indicates the kind of logon that occurred. The most common types are 2 (interactive) and 3 (network). The New Logon fields indicate the account for whom the new logon was created, i.e. the account that was logged on. The network fields indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impersonation level field indicates the extent to which a process in the logon session can impersonate. The authentication information fields provide detailed information about this specific logon request. - Logon GUID is a unique identifier that can be used to correlate this event with a KDC event. - Transited services indicate which intermediate services have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indicates the length of the generated session key. This will be 0 if no session key was requested.
					4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: LTRANPHD$ Account Domain: WORKGROUP Logon ID: 0x3e7 Logon Type: 5 Impersonation Level: %%1833 New Logon: Security ID: S-1-5-20 Account Name: NETWORK SERVICE Account Domain: NT AUTHORITY Logon ID: 0x3e4 Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x234 Process Name: C:\Windows\System32\services.exe Network Information: Workstation Name: Source Network Address: - Source Port: - Detailed Authentication Information: Logon Process: Advapi Authentication Package: Negotiate Transited Services: - Package Name (NTLM only): - Key Length: 0 This event is generated when a logon session is created. It is generated on the computer that was accessed. The subject fields indicate the account on the

Security	Audit Success	12544	2015-04-26 12:56:08	Microsoft-Windows-Security-Auditing	local system which requested the logon. This is most commonly a service such as the Server service, or a local process such as Winlogon.exe or Services.exe. The logon type field indicates the kind of logon that occurred. The most common types are 2 (interactive) and 3 (network). The New Logon fields indicate the account for whom the new logon was created, i.e. the account that was logged on. The network fields indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impersonation level field indicates the extent to which a process in the logon session can impersonate. The authentication information fields provide detailed information about this specific logon request. - Logon GUID is a unique identifier that can be used to correlate this event with a KDC event. - Transited services indicate which intermediate services have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indicates the length of the generated session key. This will be 0 if no session key was requested.
Security	Audit Success	12544	2015-04-26 12:56:08	Microsoft-Windows-Security-Auditing	4648: A logon was attempted using explicit credentials. Subject: Security ID: S-1-5-18 Account Name: LTRANPHD$ Account Domain: WORKGROUP Logon ID: 0x3e7 Logon GUID: {00000000-0000-0000-0000-000000000000} Account Whose Credentials Were Used: Account Name: DWM-1 Account Domain: Window Manager Logon GUID: {00000000-0000-0000-0000-000000000000} Target Server: Target Server Name: localhost Additional Information: localhost Process Information: Process ID: 0x204 Process Name: C:\Windows\System32\winlogon.exe Network Information: Network Address: - Port: - This event is generated when a process attempts to log on an account by explicitly specifying that account's credentials. This most commonly occurs in batch-type configurations such as scheduled tasks, or when using the RUNAS command.
Security	Audit Success	12544	2015-04-26 12:56:08	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: LTRANPHD$ Account Domain: WORKGROUP Logon ID: 0x3e7 Logon Type: 2 Impersonation Level: %%1833 New Logon: Security ID: S-1-5-90-1 Account Name: DWM-1 Account Domain: Window Manager Logon ID: 0xd2e3 Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x204 Process Name: C:\Windows\System32\winlogon.exe Network Information: Workstation Name: Source Network Address: - Source Port: - Detailed Authentication Information: Logon Process: Advapi Authentication Package: Negotiate Transited Services: - Package Name (NTLM only): - Key Length: 0 This event is generated when a logon session is created. It is generated on the computer that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service such as the Server service, or a local process such as Winlogon.exe or Services.exe. The logon type field indicates the kind of logon that occurred. The most common types are 2 (interactive) and 3 (network). The New Logon fields indicate the account for whom the new logon was created, i.e. the account that was logged on. The network fields indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impersonation level field indicates the extent to which a process in the logon session can impersonate. The authentication information fields provide detailed information about this specific logon request. - Logon GUID is a unique identifier that can be used to correlate this event with a KDC event. - Transited services indicate which intermediate services have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indicates the length of the generated session key. This will be 0 if no session key was requested.
Security	Audit Success	12544	2015-04-26 12:56:08	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: LTRANPHD$ Account Domain: WORKGROUP Logon ID: 0x3e7 Logon Type: 2 Impersonation Level: %%1833 New Logon: Security ID: S-1-5-90-1 Account Name: DWM-1 Account Domain: Window Manager Logon ID: 0xd2f7 Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x204 Process Name: C:\Windows\System32\winlogon.exe Network Information: Workstation Name: Source Network Address: - Source Port: - Detailed Authentication Information: Logon Process: Advapi Authentication Package: Negotiate Transited Services: - Package Name (NTLM only): - Key Length: 0 This event is generated when a logon session is created. It is generated on the computer that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service such as the Server service, or a local process such as Winlogon.exe or Services.exe. The logon type field indicates the kind of logon that occurred. The most common types are 2 (interactive) and 3 (network). The New Logon fields indicate the account for whom the new logon was created, i.e. the account that was logged on. The network fields indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impersonation level field indicates the extent to which a process in the logon session can impersonate. The authentication information fields provide detailed information about this specific logon request. - Logon GUID is a unique identifier that can be used to correlate this event with a KDC event. - Transited services indicate which intermediate services have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indicates the length of the generated session key. This will be 0 if no session key was requested.
Security	Audit	12544	2015-04-26	Microsoft-Windows-Security-	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: LTRANPHD$ Account Domain: WORKGROUP Logon ID: 0x3e7 Logon Type: 5 Impersonation Level: %%1833 New Logon: Security ID: S-1-5-19 Account Name: LOCAL SERVICE Account Domain: NT AUTHORITY Logon ID: 0x3e5 Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x234 Process Name: C:\Windows\System32\services.exe Network Information: Workstation Name: Source Network Address: - Source Port: - Detailed Authentication Information: Logon Process: Advapi Authentication Package: Negotiate Transited Services: - Package Name (NTLM only): - Key Length: 0 This event is generated when a logon session is created. It is generated on the computer that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service such as the Server service, or a local process such as Winlogon.exe or Services.exe. The logon type field indicates the kind of logon that occurred.

	Success		12:56:08	Auditing	The most common types are 2 (interactive) and 3 (network). The New Logon fields indicate the account for whom the new logon was created, i.e. the account that was logged on. The network fields indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impersonation level field indicates the extent to which a process in the logon session can impersonate. The authentication information fields provide detailed information about this specific logon request. - Logon GUID is a unique identifier that can be used to correlate this event with a KDC event. - Transited services indicate which intermediate services have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indicates the length of the generated session key. This will be 0 if no session key was requested.
Security	Audit Success	12544	2015-04-26 12:56:08	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: LTRANPHD$ Account Domain: WORKGROUP Logon ID: 0x3e7 Logon Type: 5 Impersonation Level: %%1833 New Logon: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Logon ID: 0x3e7 Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x234 Process Name: C:\Windows\System32\services.exe Network Information: Workstation Name: Source Network Address: - Source Port: - Detailed Authentication Information: Logon Process: Advapi Authentication Package: Negotiate Transited Services: - Package Name (NTLM only): - Key Length: 0 This event is generated when a logon session is created. It is generated on the computer that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service such as the Server service, or a local process such as Winlogon.exe or Services.exe. The logon type field indicates the kind of logon that occurred. The most common types are 2 (interactive) and 3 (network). The New Logon fields indicate the account for whom the new logon was created, i.e. the account that was logged on. The network fields indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impersonation level field indicates the extent to which a process in the logon session can impersonate. The authentication information fields provide detailed information about this specific logon request. - Logon GUID is a unique identifier that can be used to correlate this event with a KDC event. - Transited services indicate which intermediate services have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indicates the length of the generated session key. This will be 0 if no session key was requested.
Security	Audit Success	12544	2015-04-26 12:56:08	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: LTRANPHD$ Account Domain: WORKGROUP Logon ID: 0x3e7 Logon Type: 5 Impersonation Level: %%1833 New Logon: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Logon ID: 0x3e7 Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x234 Process Name: C:\Windows\System32\services.exe Network Information: Workstation Name: Source Network Address: - Source Port: - Detailed Authentication Information: Logon Process: Advapi Authentication Package: Negotiate Transited Services: - Package Name (NTLM only): - Key Length: 0 This event is generated when a logon session is created. It is generated on the computer that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service such as the Server service, or a local process such as Winlogon.exe or Services.exe. The logon type field indicates the kind of logon that occurred. The most common types are 2 (interactive) and 3 (network). The New Logon fields indicate the account for whom the new logon was created, i.e. the account that was logged on. The network fields indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impersonation level field indicates the extent to which a process in the logon session can impersonate. The authentication information fields provide detailed information about this specific logon request. - Logon GUID is a unique identifier that can be used to correlate this event with a KDC event. - Transited services indicate which intermediate services have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indicates the length of the generated session key. This will be 0 if no session key was requested.
Security	Audit Success	12548	2015-04-26 12:56:08	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Logon ID: 0x3e7 Privileges: SeAssignPrimaryTokenPrivilege SeTcbPrivilege SeSecurityPrivilege SeTakeOwnershipPrivilege SeLoadDriverPrivilege SeBackupPrivilege SeRestorePrivilege SeDebugPrivilege SeAuditPrivilege SeSystemEnvironmentPrivilege SeImpersonatePrivilege
Security	Audit Success	12548	2015-04-26 12:56:08	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-20 Account Name: NETWORK SERVICE Account Domain: NT AUTHORITY Logon ID: 0x3e4 Privileges: SeAssignPrimaryTokenPrivilege SeAuditPrivilege SeImpersonatePrivilege
Security	Audit Success	12548	2015-04-26 12:56:08	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-90-1 Account Name: DWM-1 Account Domain: Window Manager Logon ID: 0xd2e3 Privileges: SeAssignPrimaryTokenPrivilege SeAuditPrivilege SeImpersonatePrivilege
Security	Audit Success	12548	2015-04-26 12:56:08	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-90-1 Account Name: DWM-1 Account Domain: Window Manager Logon ID: 0xd2f7 Privileges: SeAssignPrimaryTokenPrivilege SeAuditPrivilege
Security	Audit Success	12548	2015-04-26 12:56:08	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-19 Account Name: LOCAL SERVICE Account Domain: NT AUTHORITY Logon ID: 0x3e5 Privileges: SeAssignPrimaryTokenPrivilege SeAuditPrivilege SeImpersonatePrivilege
Security	Audit	12548	2015-04-26	Microsoft-Windows-Security-	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Logon ID: 0x3e7 Privileges: SeAssignPrimaryTokenPrivilege SeTcbPrivilege

	Success		12:56:08	Auditing	SeSecurityPrivilege SeTakeOwnershipPrivilege SeLoadDriverPrivilege SeBackupPrivilege SeRestorePrivilege SeDebugPrivilege SeAuditPrivilege SeSystemEnvironmentPrivilege SeImpersonatePrivilege
Security	Audit Success	12548	2015-04-26 12:56:08	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Logon ID: 0x3e7 Privileges: SeAssignPrimaryTokenPrivilege SeTcbPrivilege SeSecurityPrivilege SeTakeOwnershipPrivilege SeLoadDriverPrivilege SeBackupPrivilege SeRestorePrivilege SeDebugPrivilege SeAuditPrivilege SeSystemEnvironmentPrivilege SeImpersonatePrivilege
Security	Audit Success	13568	2015-04-26 12:56:08	Microsoft-Windows-Security-Auditing	4902: The Per-user audit policy table was created. Number of Elements: 0 Policy ID: 0x81f7
Security	Audit Success	101	2015-04-26 12:56:09	Microsoft-Windows-Eventlog	1101: Audit events have been dropped by the transport. 0
Security	Audit Success	12292	2015-04-26 12:56:09	Microsoft-Windows-Security-Auditing	5033: The Windows Firewall Driver started successfully.
Security	Audit Success	12292	2015-04-26 12:56:09	Microsoft-Windows-Security-Auditing	5024: The Windows Firewall service started successfully.
Security	Audit Success	12544	2015-04-26 12:56:09	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: LTRANPHD$ Account Domain: WORKGROUP Logon ID: 0x3e7 Logon Type: 5 Impersonation Level: %%1833 New Logon: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Logon ID: 0x3e7 Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x234 Process Name: C:\Windows\System32\services.exe Network Information: Workstation Name: Source Network Address: - Source Port: - Detailed Authentication Information: Logon Process: Advapi Authentication Package: Negotiate Transited Services: - Package Name (NTLM only): - Key Length: 0 This event is generated when a logon session is created. It is generated on the computer that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service such as the Server service, or a local process such as Winlogon.exe or Services.exe. The logon type field indicates the kind of logon that occurred. The most common types are 2 (interactive) and 3 (network). The New Logon fields indicate the account for whom the new logon was created, i.e. the account that was logged on. The network fields indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impersonation level field indicates the extent to which a process in the logon session can impersonate. The authentication information fields provide detailed information about this specific logon request. - Logon GUID is a unique identifier that can be used to correlate this event with a KDC event. - Transited services indicate which intermediate services have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indicates the length of the generated session key. This will be 0 if no session key was requested.
Security	Audit Success	12544	2015-04-26 12:56:09	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: LTRANPHD$ Account Domain: WORKGROUP Logon ID: 0x3e7 Logon Type: 5 Impersonation Level: %%1833 New Logon: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Logon ID: 0x3e7 Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x234 Process Name: C:\Windows\System32\services.exe Network Information: Workstation Name: Source Network Address: - Source Port: - Detailed Authentication Information: Logon Process: Advapi Authentication Package: Negotiate Transited Services: - Package Name (NTLM only): - Key Length: 0 This event is generated when a logon session is created. It is generated on the computer that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service such as the Server service, or a local process such as Winlogon.exe or Services.exe. The logon type field indicates the kind of logon that occurred. The most common types are 2 (interactive) and 3 (network). The New Logon fields indicate the account for whom the new logon was created, i.e. the account that was logged on. The network fields indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impersonation level field indicates the extent to which a process in the logon session can impersonate. The authentication information fields provide detailed information about this specific logon request. - Logon GUID is a unique identifier that can be used to correlate this event with a KDC event. - Transited services indicate which intermediate services have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indicates the length of the generated session key. This will be 0 if no session key was requested.
Security	Audit	12544	2015-04-26	Microsoft-Windows-Security-	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: LTRANPHD$ Account Domain: WORKGROUP Logon ID: 0x3e7 Logon Type: 5 Impersonation Level: %%1833 New Logon: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Logon ID: 0x3e7 Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x234 Process Name: C:\Windows\System32\services.exe Network Information: Workstation Name: Source Network Address: - Source Port: - Detailed Authentication Information: Logon Process: Advapi Authentication Package: Negotiate Transited Services: - Package Name (NTLM only): - Key Length: 0 This event is generated when a logon session is created. It is generated on the computer that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service such as the Server service, or a local process such as Winlogon.exe or Services.exe. The logon type field indicates the kind of logon that occurred.

	Success		12:56:09	Auditing	The most common types are 2 (interactive) and 3 (network). The New Logon fields indicate the account for whom the new logon was created, i.e. the account that was logged on. The network fields indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impersonation level field indicates the extent to which a process in the logon session can impersonate. The authentication information fields provide detailed information about this specific logon request. - Logon GUID is a unique identifier that can be used to correlate this event with a KDC event. - Transited services indicate which intermediate services have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indicates the length of the generated session key. This will be 0 if no session key was requested.
Security	Audit Success	12544	2015-04-26 12:56:09	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-0-0 Account Name: - Account Domain: - Logon ID: 0x0 Logon Type: 3 Impersonation Level: %%1833 New Logon: Security ID: S-1-5-7 Account Name: ANONYMOUS LOGON Account Domain: NT AUTHORITY Logon ID: 0x1789f Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x0 Process Name: - Network Information: Workstation Name: Source Network Address: - Source Port: - Detailed Authentication Information: Logon Process: NtLmSsp Authentication Package: NTLM Transited Services: - Package Name (NTLM only): NTLM V1 Key Length: 0 This event is generated when a logon session is created. It is generated on the computer that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service such as the Server service, or a local process such as Winlogon.exe or Services.exe. The logon type field indicates the kind of logon that occurred. The most common types are 2 (interactive) and 3 (network). The New Logon fields indicate the account for whom the new logon was created, i.e. the account that was logged on. The network fields indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impersonation level field indicates the extent to which a process in the logon session can impersonate. The authentication information fields provide detailed information about this specific logon request. - Logon GUID is a unique identifier that can be used to correlate this event with a KDC event. - Transited services indicate which intermediate services have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indicates the length of the generated session key. This will be 0 if no session key was requested.
Security	Audit Success	12548	2015-04-26 12:56:09	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Logon ID: 0x3e7 Privileges: SeAssignPrimaryTokenPrivilege SeTcbPrivilege SeSecurityPrivilege SeTakeOwnershipPrivilege SeLoadDriverPrivilege SeBackupPrivilege SeRestorePrivilege SeDebugPrivilege SeAuditPrivilege SeSystemEnvironmentPrivilege SeImpersonatePrivilege
Security	Audit Success	12548	2015-04-26 12:56:09	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Logon ID: 0x3e7 Privileges: SeAssignPrimaryTokenPrivilege SeTcbPrivilege SeSecurityPrivilege SeTakeOwnershipPrivilege SeLoadDriverPrivilege SeBackupPrivilege SeRestorePrivilege SeDebugPrivilege SeAuditPrivilege SeSystemEnvironmentPrivilege SeImpersonatePrivilege
Security	Audit Success	12548	2015-04-26 12:56:09	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Logon ID: 0x3e7 Privileges: SeAssignPrimaryTokenPrivilege SeTcbPrivilege SeSecurityPrivilege SeTakeOwnershipPrivilege SeLoadDriverPrivilege SeBackupPrivilege SeRestorePrivilege SeDebugPrivilege SeAuditPrivilege SeSystemEnvironmentPrivilege SeImpersonatePrivilege
Security	Audit Success	12544	2015-04-26 12:56:15	Microsoft-Windows-Security-Auditing	4648: A logon was attempted using explicit credentials. Subject: Security ID: S-1-5-18 Account Name: LTRANPHD$ Account Domain: WORKGROUP Logon ID: 0x3e7 Logon GUID: {00000000-0000-0000-0000-000000000000} Account Whose Credentials Were Used: Account Name: Liem Account Domain: LTRANPHD Logon GUID: {00000000-0000-0000-0000-000000000000} Target Server: Target Server Name: localhost Additional Information: localhost Process Information: Process ID: 0x204 Process Name: C:\Windows\System32\winlogon.exe Network Information: Network Address: 127.0.0.1 Port: 0 This event is generated when a process attempts to log on an account by explicitly specifying that account's credentials. This most commonly occurs in batch-type configurations such as scheduled tasks, or when using the RUNAS command.
Security	Audit Success	12544	2015-04-26 12:56:15	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: LTRANPHD$ Account Domain: WORKGROUP Logon ID: 0x3e7 Logon Type: 2 Impersonation Level: %%1833 New Logon: Security ID: S-1-5-21-1888849264-3803429180-4108621888-1001 Account Name: Liem Account Domain: LTRANPHD Logon ID: 0x1f082 Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x204 Process Name: C:\Windows\System32\winlogon.exe Network Information: Workstation Name: LTRANPHD Source Network Address: 127.0.0.1 Source Port: 0 Detailed Authentication Information: Logon Process: User32 Authentication Package: Negotiate Transited Services: - Package Name (NTLM only): - Key Length: 0 This event is generated when a logon session is created. It is generated on the computer that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service such as the Server service, or a local process such as Winlogon.exe or Services.exe. The logon type field indicates the kind of logon that occurred. The most common types are 2 (interactive) and 3 (network). The New Logon fields indicate the account for whom the new logon was created, i.e. the account that was logged on. The network fields indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impersonation level field indicates the extent to which a process in the logon session can impersonate. The authentication information fields provide detailed information about this specific logon request. - Logon GUID is a unique identifier that can be used to correlate this event with a KDC event. - Transited services indicate which intermediate services have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length

					indicates the length of the generated session key. This will be 0 if no session key was requested.
Security	Audit Success	12544	2015-04-26 12:56:15	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: LTRANPHD$ Account Domain: WORKGROUP Logon ID: 0x3e7 Logon Type: 2 Impersonation Level: %%1833 New Logon: Security ID: S-1-5-21-1888849264-3803429180-4108621888-1001 Account Name: Liem Account Domain: LTRANPHD Logon ID: 0x1f0e5 Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x204 Process Name: C:\Windows\System32\winlogon.exe Network Information: Workstation Name: LTRANPHD Source Network Address: 127.0.0.1 Source Port: 0 Detailed Authentication Information: Logon Process: User32 Authentication Package: Negotiate Transited Services: - Package Name (NTLM only): - Key Length: 0 This event is generated when a logon session is created. It is generated on the computer that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service such as the Server service, or a local process such as Winlogon.exe or Services.exe. The logon type field indicates the kind of logon that occurred. The most common types are 2 (interactive) and 3 (network). The New Logon fields indicate the account for whom the new logon was created, i.e. the account that was logged on. The network fields indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impersonation level field indicates the extent to which a process in the logon session can impersonate. The authentication information fields provide detailed information about this specific logon request. - Logon GUID is a unique identifier that can be used to correlate this event with a KDC event. - Transited services indicate which intermediate services have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indicates the length of the generated session key. This will be 0 if no session key was requested.
Security	Audit Success	12548	2015-04-26 12:56:15	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-21-1888849264-3803429180-4108621888-1001 Account Name: Liem Account Domain: LTRANPHD Logon ID: 0x1f082 Privileges: SeSecurityPrivilege SeTakeOwnershipPrivilege SeLoadDriverPrivilege SeBackupPrivilege SeRestorePrivilege SeDebugPrivilege SeSystemEnvironmentPrivilege SeImpersonatePrivilege
Security	Audit Success	12544	2015-04-26 12:56:16	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: LTRANPHD$ Account Domain: WORKGROUP Logon ID: 0x3e7 Logon Type: 5 Impersonation Level: %%1833 New Logon: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Logon ID: 0x3e7 Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x234 Process Name: C:\Windows\System32\services.exe Network Information: Workstation Name: Source Network Address: - Source Port: - Detailed Authentication Information: Logon Process: Advapi Authentication Package: Negotiate Transited Services: - Package Name (NTLM only): - Key Length: 0 This event is generated when a logon session is created. It is generated on the computer that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service such as the Server service, or a local process such as Winlogon.exe or Services.exe. The logon type field indicates the kind of logon that occurred. The most common types are 2 (interactive) and 3 (network). The New Logon fields indicate the account for whom the new logon was created, i.e. the account that was logged on. The network fields indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impersonation level field indicates the extent to which a process in the logon session can impersonate. The authentication information fields provide detailed information about this specific logon request. - Logon GUID is a unique identifier that can be used to correlate this event with a KDC event. - Transited services indicate which intermediate services have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indicates the length of the generated session key. This will be 0 if no session key was requested.
Security	Audit Success	12548	2015-04-26 12:56:16	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Logon ID: 0x3e7 Privileges: SeAssignPrimaryTokenPrivilege SeTcbPrivilege SeSecurityPrivilege SeTakeOwnershipPrivilege SeLoadDriverPrivilege SeBackupPrivilege SeRestorePrivilege SeDebugPrivilege SeAuditPrivilege SeSystemEnvironmentPrivilege SeImpersonatePrivilege
Security	Audit Success	13824	2015-04-26 12:56:17	Microsoft-Windows-Security-Auditing	4797: An attempt was made to query the existence of a blank password for an account. Subject: Security ID: S-1-5-21-1888849264-3803429180-4108621888-1001 Account Name: Liem Account Domain: LTRANPHD Logon ID: 0x1f0e5 Additional Information: Caller Workstation: LTRANPHD Target Account Name: Administrator Target Account Domain: LTRANPHD
Security	Audit Success	13824	2015-04-26 12:56:17	Microsoft-Windows-Security-Auditing	4797: An attempt was made to query the existence of a blank password for an account. Subject: Security ID: S-1-5-21-1888849264-3803429180-4108621888-1001 Account Name: Liem Account Domain: LTRANPHD Logon ID: 0x1f0e5 Additional Information: Caller Workstation: LTRANPHD Target Account Name: Guest Target Account Domain: LTRANPHD
Security	Audit Success	13824	2015-04-26 12:56:17	Microsoft-Windows-Security-Auditing	4797: An attempt was made to query the existence of a blank password for an account. Subject: Security ID: S-1-5-21-1888849264-3803429180-4108621888-1001 Account Name: Liem Account Domain: LTRANPHD Logon ID: 0x1f0e5 Additional Information: Caller Workstation: LTRANPHD Target Account Name: Administrator Target Account Domain: LTRANPHD
Security	Audit Success	13824	2015-04-26 12:56:17	Microsoft-Windows-Security-Auditing	4797: An attempt was made to query the existence of a blank password for an account. Subject: Security ID: S-1-5-21-1888849264-3803429180-4108621888-1001 Account Name: Liem Account Domain: LTRANPHD Logon ID: 0x1f0e5 Additional Information: Caller Workstation: LTRANPHD Target Account Name: Guest Target Account Domain: LTRANPHD
Security	Audit	13824	2015-04-26	Microsoft-Windows-Security-	4797: An attempt was made to query the existence of a blank password for an account. Subject: Security ID: S-1-5-19 Account Name: LOCAL SERVICE Account Domain: NT AUTHORITY Logon ID: 0x3e5 Additional

	Success		12:56:18	Auditing	Information: Caller Workstation: LTRANPHD Target Account Name: Administrator Target Account Domain: LTRANPHD
Security	Audit Success	13824	2015-04-26 12:56:18	Microsoft-Windows-Security-Auditing	4797: An attempt was made to query the existence of a blank password for an account. Subject: Security ID: S-1-5-19 Account Name: LOCAL SERVICE Account Domain: NT AUTHORITY Logon ID: 0x3e5 Additional Information: Caller Workstation: LTRANPHD Target Account Name: Guest Target Account Domain: LTRANPHD
Security	Audit Success	13824	2015-04-26 12:56:18	Microsoft-Windows-Security-Auditing	4797: An attempt was made to query the existence of a blank password for an account. Subject: Security ID: S-1-5-19 Account Name: LOCAL SERVICE Account Domain: NT AUTHORITY Logon ID: 0x3e5 Additional Information: Caller Workstation: LTRANPHD Target Account Name: Liem Target Account Domain: LTRANPHD
Security	Audit Success	13824	2015-04-26 12:56:18	Microsoft-Windows-Security-Auditing	4797: An attempt was made to query the existence of a blank password for an account. Subject: Security ID: S-1-5-19 Account Name: LOCAL SERVICE Account Domain: NT AUTHORITY Logon ID: 0x3e5 Additional Information: Caller Workstation: LTRANPHD Target Account Name: Liem Target Account Domain: LTRANPHD
Security	Audit Success	13824	2015-04-26 12:56:18	Microsoft-Windows-Security-Auditing	4797: An attempt was made to query the existence of a blank password for an account. Subject: Security ID: S-1-5-19 Account Name: LOCAL SERVICE Account Domain: NT AUTHORITY Logon ID: 0x3e5 Additional Information: Caller Workstation: LTRANPHD Target Account Name: Administrator Target Account Domain: LTRANPHD
Security	Audit Success	13824	2015-04-26 12:56:18	Microsoft-Windows-Security-Auditing	4797: An attempt was made to query the existence of a blank password for an account. Subject: Security ID: S-1-5-19 Account Name: LOCAL SERVICE Account Domain: NT AUTHORITY Logon ID: 0x3e5 Additional Information: Caller Workstation: LTRANPHD Target Account Name: Guest Target Account Domain: LTRANPHD
Security	Audit Success	13824	2015-04-26 12:56:18	Microsoft-Windows-Security-Auditing	4797: An attempt was made to query the existence of a blank password for an account. Subject: Security ID: S-1-5-19 Account Name: LOCAL SERVICE Account Domain: NT AUTHORITY Logon ID: 0x3e5 Additional Information: Caller Workstation: LTRANPHD Target Account Name: Liem Target Account Domain: LTRANPHD
Security	Audit Success	13824	2015-04-26 12:56:18	Microsoft-Windows-Security-Auditing	4797: An attempt was made to query the existence of a blank password for an account. Subject: Security ID: S-1-5-19 Account Name: LOCAL SERVICE Account Domain: NT AUTHORITY Logon ID: 0x3e5 Additional Information: Caller Workstation: LTRANPHD Target Account Name: Liem Target Account Domain: LTRANPHD
Security	Audit Success	12544	2015-04-26 13:23:50	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: LTRANPHD$ Account Domain: WORKGROUP Logon ID: 0x3e7 Logon Type: 5 Impersonation Level: %%1833 New Logon: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Logon ID: 0x3e7 Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x234 Process Name: C:\Windows\System32\services.exe Network Information: Workstation Name: Source Network Address: - Source Port: - Detailed Authentication Information: Logon Process: Advapi Authentication Package: Negotiate Transited Services: - Package Name (NTLM only): - Key Length: 0 This event is generated when a logon session is created. It is generated on the computer that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service such as the Server service, or a local process such as Winlogon.exe or Services.exe. The logon type field indicates the kind of logon that occurred. The most common types are 2 (interactive) and 3 (network). The New Logon fields indicate the account for whom the new logon was created, i.e. the account that was logged on. The network fields indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impersonation level field indicates the extent to which a process in the logon session can impersonate. The authentication information fields provide detailed information about this specific logon request. - Logon GUID is a unique identifier that can be used to correlate this event with a KDC event. - Transited services indicate which intermediate services have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indicates the length of the generated session key. This will be 0 if no session key was requested.
Security	Audit Success	12548	2015-04-26 13:23:50	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Logon ID: 0x3e7 Privileges: SeAssignPrimaryTokenPrivilege SeTcbPrivilege SeSecurityPrivilege SeTakeOwnershipPrivilege SeLoadDriverPrivilege SeBackupPrivilege SeRestorePrivilege SeDebugPrivilege SeAuditPrivilege SeSystemEnvironmentPrivilege SeImpersonatePrivilege
Security	Audit Success	12288	2015-04-26 13:26:13	Microsoft-Windows-Security-Auditing	4608: Windows is starting up. This event is logged when LSASS.EXE starts and the auditing subsystem is initialized.
Security	Audit Success	12544	2015-04-26 13:26:13	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-0-0 Account Name: - Account Domain: - Logon ID: 0x0 Logon Type: 0 Impersonation Level: - New Logon: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Logon ID: 0x3e7 Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x4 Process Name: Network Information: Workstation Name: - Source Network Address: - Source Port: - Detailed Authentication Information: Logon Process: - Authentication Package: - Transited Services: - Package Name (NTLM only): - Key Length: 0 This event is generated when a logon session is created. It is generated on the computer that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service such as the Server service, or a local process such as Winlogon.exe or Services.exe. The logon type field indicates the kind of logon that occurred. The most common types are 2 (interactive) and 3 (network). The New Logon fields indicate the account for whom the new logon was created, i.e. the account that was logged on. The network fields indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impersonation level field indicates the extent to which a process in the logon session can impersonate. The authentication information fields provide detailed information about this specific logon request. - Logon GUID is a unique identifier that can be used to correlate this event

					with a KDC event. - Transited services indicate which intermediate services have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indicates the length of the generated session key. This will be 0 if no session key was requested.
Security	Audit Success	13568	2015-04-26 13:26:13	Microsoft-Windows-Security-Auditing	4902: The Per-user audit policy table was created. Number of Elements: 0 Policy ID: 0x7e20
Security	Audit Success	101	2015-04-26 13:26:14	Microsoft-Windows-Eventlog	1101: Audit events have been dropped by the transport. 0
Security	Audit Success	12544	2015-04-26 13:26:14	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: LTRANPHD$ Account Domain: WORKGROUP Logon ID: 0x3e7 Logon Type: 5 Impersonation Level: %%1833 New Logon: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Logon ID: 0x3e7 Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x234 Process Name: C:\Windows\System32\services.exe Network Information: Workstation Name: Source Network Address: - Source Port: - Detailed Authentication Information: Logon Process: Advapi Authentication Package: Negotiate Transited Services: - Package Name (NTLM only): - Key Length: 0 This event is generated when a logon session is created. It is generated on the computer that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service such as the Server service, or a local process such as Winlogon.exe or Services.exe. The logon type field indicates the kind of logon that occurred. The most common types are 2 (interactive) and 3 (network). The New Logon fields indicate the account for whom the new logon was created, i.e. the account that was logged on. The network fields indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impersonation level field indicates the extent to which a process in the logon session can impersonate. The authentication information fields provide detailed information about this specific logon request. - Logon GUID is a unique identifier that can be used to correlate this event with a KDC event. - Transited services indicate which intermediate services have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indicates the length of the generated session key. This will be 0 if no session key was requested.
Security	Audit Success	12544	2015-04-26 13:26:14	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: LTRANPHD$ Account Domain: WORKGROUP Logon ID: 0x3e7 Logon Type: 5 Impersonation Level: %%1833 New Logon: Security ID: S-1-5-20 Account Name: NETWORK SERVICE Account Domain: NT AUTHORITY Logon ID: 0x3e4 Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x234 Process Name: C:\Windows\System32\services.exe Network Information: Workstation Name: Source Network Address: - Source Port: - Detailed Authentication Information: Logon Process: Advapi Authentication Package: Negotiate Transited Services: - Package Name (NTLM only): - Key Length: 0 This event is generated when a logon session is created. It is generated on the computer that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service such as the Server service, or a local process such as Winlogon.exe or Services.exe. The logon type field indicates the kind of logon that occurred. The most common types are 2 (interactive) and 3 (network). The New Logon fields indicate the account for whom the new logon was created, i.e. the account that was logged on. The network fields indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impersonation level field indicates the extent to which a process in the logon session can impersonate. The authentication information fields provide detailed information about this specific logon request. - Logon GUID is a unique identifier that can be used to correlate this event with a KDC event. - Transited services indicate which intermediate services have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indicates the length of the generated session key. This will be 0 if no session key was requested.
Security	Audit Success	12544	2015-04-26 13:26:14	Microsoft-Windows-Security-Auditing	4648: A logon was attempted using explicit credentials. Subject: Security ID: S-1-5-18 Account Name: LTRANPHD$ Account Domain: WORKGROUP Logon ID: 0x3e7 Logon GUID: {00000000-0000-0000-0000-000000000000} Account Whose Credentials Were Used: Account Name: DWM-1 Account Domain: Window Manager Logon GUID: {00000000-0000-0000-0000-000000000000} Target Server: Target Server Name: localhost Additional Information: localhost Process Information: Process ID: 0x204 Process Name: C:\Windows\System32\winlogon.exe Network Information: Network Address: - Port: - This event is generated when a process attempts to log on an account by explicitly specifying that account's credentials. This most commonly occurs in batch-type configurations such as scheduled tasks, or when using the RUNAS command.
Security	Audit Success	12544	2015-04-26 13:26:14	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: LTRANPHD$ Account Domain: WORKGROUP Logon ID: 0x3e7 Logon Type: 2 Impersonation Level: %%1833 New Logon: Security ID: S-1-5-90-1 Account Name: DWM-1 Account Domain: Window Manager Logon ID: 0xce54 Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x204 Process Name: C:\Windows\System32\winlogon.exe Network Information: Workstation Name: Source Network Address: - Source Port: - Detailed Authentication Information: Logon Process: Advapi Authentication Package: Negotiate Transited Services: - Package Name (NTLM only): - Key Length: 0 This event is generated when a logon session is created. It is generated on the computer that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service such as the Server service, or a local process such as Winlogon.exe or Services.exe. The logon type field indicates the kind of logon that occurred. The most common types are 2 (interactive) and 3 (network). The New Logon fields indicate the account for

					whom the new logon was created, i.e. the account that was logged on. The network fields indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impersonation level field indicates the extent to which a process in the logon session can impersonate. The authentication information fields provide detailed information about this specific logon request. - Logon GUID is a unique identifier that can be used to correlate this event with a KDC event. - Transited services indicate which intermediate services have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indicates the length of the generated session key. This will be 0 if no session key was requested.
Security	Audit Success	12544	2015-04-26 13:26:14	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: LTRANPHD$ Account Domain: WORKGROUP Logon ID: 0x3e7 Logon Type: 2 Impersonation Level: %%1833 New Logon: Security ID: S-1-5-90-1 Account Name: DWM-1 Account Domain: Window Manager Logon ID: 0xce6c Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x204 Process Name: C:\Windows\System32\winlogon.exe Network Information: Workstation Name: Source Network Address: - Source Port: - Detailed Authentication Information: Logon Process: Advapi Authentication Package: Negotiate Transited Services: - Package Name (NTLM only): - Key Length: 0 This event is generated when a logon session is created. It is generated on the computer that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service such as the Server service, or a local process such as Winlogon.exe or Services.exe. The logon type field indicates the kind of logon that occurred. The most common types are 2 (interactive) and 3 (network). The New Logon fields indicate the account for whom the new logon was created, i.e. the account that was logged on. The network fields indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impersonation level field indicates the extent to which a process in the logon session can impersonate. The authentication information fields provide detailed information about this specific logon request. - Logon GUID is a unique identifier that can be used to correlate this event with a KDC event. - Transited services indicate which intermediate services have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indicates the length of the generated session key. This will be 0 if no session key was requested.
Security	Audit Success	12544	2015-04-26 13:26:14	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: LTRANPHD$ Account Domain: WORKGROUP Logon ID: 0x3e7 Logon Type: 5 Impersonation Level: %%1833 New Logon: Security ID: S-1-5-19 Account Name: LOCAL SERVICE Account Domain: NT AUTHORITY Logon ID: 0x3e5 Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x234 Process Name: C:\Windows\System32\services.exe Network Information: Workstation Name: Source Network Address: - Source Port: - Detailed Authentication Information: Logon Process: Advapi Authentication Package: Negotiate Transited Services: - Package Name (NTLM only): - Key Length: 0 This event is generated when a logon session is created. It is generated on the computer that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service such as the Server service, or a local process such as Winlogon.exe or Services.exe. The logon type field indicates the kind of logon that occurred. The most common types are 2 (interactive) and 3 (network). The New Logon fields indicate the account for whom the new logon was created, i.e. the account that was logged on. The network fields indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impersonation level field indicates the extent to which a process in the logon session can impersonate. The authentication information fields provide detailed information about this specific logon request. - Logon GUID is a unique identifier that can be used to correlate this event with a KDC event. - Transited services indicate which intermediate services have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indicates the length of the generated session key. This will be 0 if no session key was requested.
Security	Audit Success	12544	2015-04-26 13:26:14	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: LTRANPHD$ Account Domain: WORKGROUP Logon ID: 0x3e7 Logon Type: 5 Impersonation Level: %%1833 New Logon: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Logon ID: 0x3e7 Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x234 Process Name: C:\Windows\System32\services.exe Network Information: Workstation Name: Source Network Address: - Source Port: - Detailed Authentication Information: Logon Process: Advapi Authentication Package: Negotiate Transited Services: - Package Name (NTLM only): - Key Length: 0 This event is generated when a logon session is created. It is generated on the computer that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service such as the Server service, or a local process such as Winlogon.exe or Services.exe. The logon type field indicates the kind of logon that occurred. The most common types are 2 (interactive) and 3 (network). The New Logon fields indicate the account for whom the new logon was created, i.e. the account that was logged on. The network fields indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impersonation level field indicates the extent to which a process in the logon session can impersonate. The authentication information fields provide detailed information about this specific logon request. - Logon GUID is a unique identifier that can be used to correlate this event with a KDC event. - Transited services indicate which intermediate services have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indicates the length of the generated session key. This will be 0 if no session key was requested.
					4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: LTRANPHD$ Account Domain: WORKGROUP Logon ID: 0x3e7 Logon Type: 5 Impersonation Level: %%1833 New Logon:

Security	Audit Success	12544	2015-04-26 13:26:14	Microsoft-Windows-Security-Auditing	Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Logon ID: 0x3e7 Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x234 Process Name: C:\Windows\System32\services.exe Network Information: Workstation Name: Source Network Address: - Source Port: - Detailed Authentication Information: Logon Process: Advapi Authentication Package: Negotiate Transited Services: - Package Name (NTLM only): - Key Length: 0 This event is generated when a logon session is created. It is generated on the computer that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service such as the Server service, or a local process such as Winlogon.exe or Services.exe. The logon type field indicates the kind of logon that occurred. The most common types are 2 (interactive) and 3 (network). The New Logon fields indicate the account for whom the new logon was created, i.e. the account that was logged on. The network fields indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impersonation level field indicates the extent to which a process in the logon session can impersonate. The authentication information fields provide detailed information about this specific logon request. - Logon GUID is a unique identifier that can be used to correlate this event with a KDC event. - Transited services indicate which intermediate services have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indicates the length of the generated session key. This will be 0 if no session key was requested.
Security	Audit Success	12544	2015-04-26 13:26:14	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: LTRANPHD$ Account Domain: WORKGROUP Logon ID: 0x3e7 Logon Type: 5 Impersonation Level: %%1833 New Logon: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Logon ID: 0x3e7 Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x234 Process Name: C:\Windows\System32\services.exe Network Information: Workstation Name: Source Network Address: - Source Port: - Detailed Authentication Information: Logon Process: Advapi Authentication Package: Negotiate Transited Services: - Package Name (NTLM only): - Key Length: 0 This event is generated when a logon session is created. It is generated on the computer that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service such as the Server service, or a local process such as Winlogon.exe or Services.exe. The logon type field indicates the kind of logon that occurred. The most common types are 2 (interactive) and 3 (network). The New Logon fields indicate the account for whom the new logon was created, i.e. the account that was logged on. The network fields indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impersonation level field indicates the extent to which a process in the logon session can impersonate. The authentication information fields provide detailed information about this specific logon request. - Logon GUID is a unique identifier that can be used to correlate this event with a KDC event. - Transited services indicate which intermediate services have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indicates the length of the generated session key. This will be 0 if no session key was requested.
Security	Audit Success	12548	2015-04-26 13:26:14	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Logon ID: 0x3e7 Privileges: SeAssignPrimaryTokenPrivilege SeTcbPrivilege SeSecurityPrivilege SeTakeOwnershipPrivilege SeLoadDriverPrivilege SeBackupPrivilege SeRestorePrivilege SeDebugPrivilege SeAuditPrivilege SeSystemEnvironmentPrivilege SeImpersonatePrivilege
Security	Audit Success	12548	2015-04-26 13:26:14	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-20 Account Name: NETWORK SERVICE Account Domain: NT AUTHORITY Logon ID: 0x3e4 Privileges: SeAssignPrimaryTokenPrivilege SeAuditPrivilege SeImpersonatePrivilege
Security	Audit Success	12548	2015-04-26 13:26:14	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-90-1 Account Name: DWM-1 Account Domain: Window Manager Logon ID: 0xce54 Privileges: SeAssignPrimaryTokenPrivilege SeAuditPrivilege SeImpersonatePrivilege
Security	Audit Success	12548	2015-04-26 13:26:14	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-90-1 Account Name: DWM-1 Account Domain: Window Manager Logon ID: 0xce6c Privileges: SeAssignPrimaryTokenPrivilege SeAuditPrivilege
Security	Audit Success	12548	2015-04-26 13:26:14	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-19 Account Name: LOCAL SERVICE Account Domain: NT AUTHORITY Logon ID: 0x3e5 Privileges: SeAssignPrimaryTokenPrivilege SeAuditPrivilege SeImpersonatePrivilege
Security	Audit Success	12548	2015-04-26 13:26:14	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Logon ID: 0x3e7 Privileges: SeAssignPrimaryTokenPrivilege SeTcbPrivilege SeSecurityPrivilege SeTakeOwnershipPrivilege SeLoadDriverPrivilege SeBackupPrivilege SeRestorePrivilege SeDebugPrivilege SeAuditPrivilege SeSystemEnvironmentPrivilege SeImpersonatePrivilege
Security	Audit Success	12548	2015-04-26 13:26:14	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Logon ID: 0x3e7 Privileges: SeAssignPrimaryTokenPrivilege SeTcbPrivilege SeSecurityPrivilege SeTakeOwnershipPrivilege SeLoadDriverPrivilege SeBackupPrivilege SeRestorePrivilege SeDebugPrivilege SeAuditPrivilege SeSystemEnvironmentPrivilege SeImpersonatePrivilege
Security	Audit Success	12548	2015-04-26 13:26:14	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Logon ID: 0x3e7 Privileges: SeAssignPrimaryTokenPrivilege SeTcbPrivilege SeSecurityPrivilege SeTakeOwnershipPrivilege SeLoadDriverPrivilege SeBackupPrivilege SeRestorePrivilege SeDebugPrivilege SeAuditPrivilege SeSystemEnvironmentPrivilege SeImpersonatePrivilege
	Audit		2015-04-	Microsoft-Windows-Security-	

Security	Success	12292	26 13:26:15	Auditing	5033: The Windows Firewall Driver started successfully.
Security	Audit Success	12292	2015-04-26 13:26:15	Microsoft-Windows-Security-Auditing	5024: The Windows Firewall service started successfully.
Security	Audit Success	12544	2015-04-26 13:26:15	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: LTRANPHD$ Account Domain: WORKGROUP Logon ID: 0x3e7 Logon Type: 5 Impersonation Level: %%1833 New Logon: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Logon ID: 0x3e7 Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x234 Process Name: C:\Windows\System32\services.exe Network Information: Workstation Name: Source Network Address: - Source Port: - Detailed Authentication Information: Logon Process: Advapi Authentication Package: Negotiate Transited Services: - Package Name (NTLM only): - Key Length: 0 This event is generated when a logon session is created. It is generated on the computer that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service such as the Server service, or a local process such as Winlogon.exe or Services.exe. The logon type field indicates the kind of logon that occurred. The most common types are 2 (interactive) and 3 (network). The New Logon fields indicate the account for whom the new logon was created, i.e. the account that was logged on. The network fields indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impersonation level field indicates the extent to which a process in the logon session can impersonate. The authentication information fields provide detailed information about this specific logon request. - Logon GUID is a unique identifier that can be used to correlate this event with a KDC event. - Transited services indicate which intermediate services have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indicates the length of the generated session key. This will be 0 if no session key was requested.
Security	Audit Success	12544	2015-04-26 13:26:15	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: LTRANPHD$ Account Domain: WORKGROUP Logon ID: 0x3e7 Logon Type: 5 Impersonation Level: %%1833 New Logon: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Logon ID: 0x3e7 Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x234 Process Name: C:\Windows\System32\services.exe Network Information: Workstation Name: Source Network Address: - Source Port: - Detailed Authentication Information: Logon Process: Advapi Authentication Package: Negotiate Transited Services: - Package Name (NTLM only): - Key Length: 0 This event is generated when a logon session is created. It is generated on the computer that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service such as the Server service, or a local process such as Winlogon.exe or Services.exe. The logon type field indicates the kind of logon that occurred. The most common types are 2 (interactive) and 3 (network). The New Logon fields indicate the account for whom the new logon was created, i.e. the account that was logged on. The network fields indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impersonation level field indicates the extent to which a process in the logon session can impersonate. The authentication information fields provide detailed information about this specific logon request. - Logon GUID is a unique identifier that can be used to correlate this event with a KDC event. - Transited services indicate which intermediate services have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indicates the length of the generated session key. This will be 0 if no session key was requested.
Security	Audit Success	12544	2015-04-26 13:26:15	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-0-0 Account Name: - Account Domain: - Logon ID: 0x0 Logon Type: 3 Impersonation Level: %%1833 New Logon: Security ID: S-1-5-7 Account Name: ANONYMOUS LOGON Account Domain: NT AUTHORITY Logon ID: 0x1742d Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x0 Process Name: - Network Information: Workstation Name: Source Network Address: - Source Port: - Detailed Authentication Information: Logon Process: NtLmSsp Authentication Package: NTLM Transited Services: - Package Name (NTLM only): NTLM V1 Key Length: 0 This event is generated when a logon session is created. It is generated on the computer that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service such as the Server service, or a local process such as Winlogon.exe or Services.exe. The logon type field indicates the kind of logon that occurred. The most common types are 2 (interactive) and 3 (network). The New Logon fields indicate the account for whom the new logon was created, i.e. the account that was logged on. The network fields indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impersonation level field indicates the extent to which a process in the logon session can impersonate. The authentication information fields provide detailed information about this specific logon request. - Logon GUID is a unique identifier that can be used to correlate this event with a KDC event. - Transited services indicate which intermediate services have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indicates the length of the generated session key. This will be 0 if no session key was requested.
Security	Audit Success	12548	2015-04-26 13:26:15	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Logon ID: 0x3e7 Privileges: SeAssignPrimaryTokenPrivilege SeTcbPrivilege SeSecurityPrivilege SeTakeOwnershipPrivilege SeLoadDriverPrivilege SeBackupPrivilege SeRestorePrivilege SeDebugPrivilege SeAuditPrivilege SeSystemEnvironmentPrivilege SeImpersonatePrivilege
			2015-04-		4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account

Security	Audit Success	12548	26 13:26:15	Microsoft-Windows-Security-Auditing	Domain: NT AUTHORITY Logon ID: 0x3e7 Privileges: SeAssignPrimaryTokenPrivilege SeTcbPrivilege SeSecurityPrivilege SeTakeOwnershipPrivilege SeLoadDriverPrivilege SeBackupPrivilege SeRestorePrivilege SeDebugPrivilege SeAuditPrivilege SeSystemEnvironmentPrivilege SeImpersonatePrivilege
Security	Audit Success	12544	2015-04-26 13:26:19	Microsoft-Windows-Security-Auditing	4648: A logon was attempted using explicit credentials. Subject: Security ID: S-1-5-18 Account Name: LTRANPHD$ Account Domain: WORKGROUP Logon ID: 0x3e7 Logon GUID: {00000000-0000-0000-0000-000000000000} Account Whose Credentials Were Used: Account Name: Liem Account Domain: LTRANPHD Logon GUID: {00000000-0000-0000-0000-000000000000} Target Server: Target Server Name: localhost Additional Information: localhost Process Information: Process ID: 0x204 Process Name: C:\Windows\System32\winlogon.exe Network Information: Network Address: 127.0.0.1 Port: 0 This event is generated when a process attempts to log on an account by explicitly specifying that account's credentials. This most commonly occurs in batch-type configurations such as scheduled tasks, or when using the RUNAS command.
Security	Audit Success	12544	2015-04-26 13:26:19	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: LTRANPHD$ Account Domain: WORKGROUP Logon ID: 0x3e7 Logon Type: 2 Impersonation Level: %%1833 New Logon: Security ID: S-1-5-21-1888849264-3803429180-4108621888-1001 Account Name: Liem Account Domain: LTRANPHD Logon ID: 0x1dd0f Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x204 Process Name: C:\Windows\System32\winlogon.exe Network Information: Workstation Name: LTRANPHD Source Network Address: 127.0.0.1 Source Port: 0 Detailed Authentication Information: Logon Process: User32 Authentication Package: Negotiate Transited Services: - Package Name (NTLM only): - Key Length: 0 This event is generated when a logon session is created. It is generated on the computer that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service such as the Server service, or a local process such as Winlogon.exe or Services.exe. The logon type field indicates the kind of logon that occurred. The most common types are 2 (interactive) and 3 (network). The New Logon fields indicate the account for whom the new logon was created, i.e. the account that was logged on. The network fields indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impersonation level field indicates the extent to which a process in the logon session can impersonate. The authentication information fields provide detailed information about this specific logon request. - Logon GUID is a unique identifier that can be used to correlate this event with a KDC event. - Transited services indicate which intermediate services have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indicates the length of the generated session key. This will be 0 if no session key was requested.
Security	Audit Success	12544	2015-04-26 13:26:19	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: LTRANPHD$ Account Domain: WORKGROUP Logon ID: 0x3e7 Logon Type: 2 Impersonation Level: %%1833 New Logon: Security ID: S-1-5-21-1888849264-3803429180-4108621888-1001 Account Name: Liem Account Domain: LTRANPHD Logon ID: 0x1dd62 Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x204 Process Name: C:\Windows\System32\winlogon.exe Network Information: Workstation Name: LTRANPHD Source Network Address: 127.0.0.1 Source Port: 0 Detailed Authentication Information: Logon Process: User32 Authentication Package: Negotiate Transited Services: - Package Name (NTLM only): - Key Length: 0 This event is generated when a logon session is created. It is generated on the computer that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service such as the Server service, or a local process such as Winlogon.exe or Services.exe. The logon type field indicates the kind of logon that occurred. The most common types are 2 (interactive) and 3 (network). The New Logon fields indicate the account for whom the new logon was created, i.e. the account that was logged on. The network fields indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impersonation level field indicates the extent to which a process in the logon session can impersonate. The authentication information fields provide detailed information about this specific logon request. - Logon GUID is a unique identifier that can be used to correlate this event with a KDC event. - Transited services indicate which intermediate services have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indicates the length of the generated session key. This will be 0 if no session key was requested.
Security	Audit Success	12548	2015-04-26 13:26:19	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-21-1888849264-3803429180-4108621888-1001 Account Name: Liem Account Domain: LTRANPHD Logon ID: 0x1dd0f Privileges: SeSecurityPrivilege SeTakeOwnershipPrivilege SeLoadDriverPrivilege SeBackupPrivilege SeRestorePrivilege SeDebugPrivilege SeSystemEnvironmentPrivilege SeImpersonatePrivilege
Security	Audit Success	12544	2015-04-26 13:26:20	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: LTRANPHD$ Account Domain: WORKGROUP Logon ID: 0x3e7 Logon Type: 5 Impersonation Level: %%1833 New Logon: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Logon ID: 0x3e7 Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x234 Process Name: C:\Windows\System32\services.exe Network Information: Workstation Name: Source Network Address: - Source Port: - Detailed Authentication Information: Logon Process: Advapi Authentication Package: Negotiate Transited Services: - Package Name (NTLM only): - Key Length: 0 This event is generated when a logon session is created. It is generated on the computer that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service such as the Server service, or a local process such as Winlogon.exe or Services.exe. The logon type field indicates the kind of logon that occurred. The most common types are 2 (interactive) and 3 (network). The New Logon fields indicate the account for whom the new logon was created, i.e. the account that was logged on. The network fields indicate where a

					remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impersonation level field indicates the extent to which a process in the logon session can impersonate. The authentication information fields provide detailed information about this specific logon request. - Logon GUID is a unique identifier that can be used to correlate this event with a KDC event. - Transited services indicate which intermediate services have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indicates the length of the generated session key. This will be 0 if no session key was requested.
Security	Audit Success	12548	2015-04-26 13:26:20	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Logon ID: 0x3e7 Privileges: SeAssignPrimaryTokenPrivilege SeTcbPrivilege SeSecurityPrivilege SeTakeOwnershipPrivilege SeLoadDriverPrivilege SeBackupPrivilege SeRestorePrivilege SeDebugPrivilege SeAuditPrivilege SeSystemEnvironmentPrivilege SeImpersonatePrivilege
Security	Audit Success	13824	2015-04-26 13:26:20	Microsoft-Windows-Security-Auditing	4797: An attempt was made to query the existence of a blank password for an account. Subject: Security ID: S-1-5-19 Account Name: LOCAL SERVICE Account Domain: NT AUTHORITY Logon ID: 0x3e5 Additional Information: Caller Workstation: LTRANPHD Target Account Name: Administrator Target Account Domain: LTRANPHD
Security	Audit Success	13824	2015-04-26 13:26:20	Microsoft-Windows-Security-Auditing	4797: An attempt was made to query the existence of a blank password for an account. Subject: Security ID: S-1-5-19 Account Name: LOCAL SERVICE Account Domain: NT AUTHORITY Logon ID: 0x3e5 Additional Information: Caller Workstation: LTRANPHD Target Account Name: Guest Target Account Domain: LTRANPHD
Security	Audit Success	13824	2015-04-26 13:26:20	Microsoft-Windows-Security-Auditing	4797: An attempt was made to query the existence of a blank password for an account. Subject: Security ID: S-1-5-19 Account Name: LOCAL SERVICE Account Domain: NT AUTHORITY Logon ID: 0x3e5 Additional Information: Caller Workstation: LTRANPHD Target Account Name: Liem Target Account Domain: LTRANPHD
Security	Audit Success	13824	2015-04-26 13:26:20	Microsoft-Windows-Security-Auditing	4797: An attempt was made to query the existence of a blank password for an account. Subject: Security ID: S-1-5-19 Account Name: LOCAL SERVICE Account Domain: NT AUTHORITY Logon ID: 0x3e5 Additional Information: Caller Workstation: LTRANPHD Target Account Name: Liem Target Account Domain: LTRANPHD
Security	Audit Success	13824	2015-04-26 13:26:20	Microsoft-Windows-Security-Auditing	4797: An attempt was made to query the existence of a blank password for an account. Subject: Security ID: S-1-5-19 Account Name: LOCAL SERVICE Account Domain: NT AUTHORITY Logon ID: 0x3e5 Additional Information: Caller Workstation: LTRANPHD Target Account Name: Administrator Target Account Domain: LTRANPHD
Security	Audit Success	13824	2015-04-26 13:26:20	Microsoft-Windows-Security-Auditing	4797: An attempt was made to query the existence of a blank password for an account. Subject: Security ID: S-1-5-19 Account Name: LOCAL SERVICE Account Domain: NT AUTHORITY Logon ID: 0x3e5 Additional Information: Caller Workstation: LTRANPHD Target Account Name: Guest Target Account Domain: LTRANPHD
Security	Audit Success	13824	2015-04-26 13:26:20	Microsoft-Windows-Security-Auditing	4797: An attempt was made to query the existence of a blank password for an account. Subject: Security ID: S-1-5-19 Account Name: LOCAL SERVICE Account Domain: NT AUTHORITY Logon ID: 0x3e5 Additional Information: Caller Workstation: LTRANPHD Target Account Name: Liem Target Account Domain: LTRANPHD
Security	Audit Success	13824	2015-04-26 13:26:20	Microsoft-Windows-Security-Auditing	4797: An attempt was made to query the existence of a blank password for an account. Subject: Security ID: S-1-5-19 Account Name: LOCAL SERVICE Account Domain: NT AUTHORITY Logon ID: 0x3e5 Additional Information: Caller Workstation: LTRANPHD Target Account Name: Administrator Target Account Domain: LTRANPHD
Security	Audit Success	13824	2015-04-26 13:26:20	Microsoft-Windows-Security-Auditing	4797: An attempt was made to query the existence of a blank password for an account. Subject: Security ID: S-1-5-19 Account Name: LOCAL SERVICE Account Domain: NT AUTHORITY Logon ID: 0x3e5 Additional Information: Caller Workstation: LTRANPHD Target Account Name: Liem Target Account Domain: LTRANPHD
Security	Audit Success	13824	2015-04-26 13:26:20	Microsoft-Windows-Security-Auditing	4797: An attempt was made to query the existence of a blank password for an account. Subject: Security ID: S-1-5-19 Account Name: LOCAL SERVICE Account Domain: NT AUTHORITY Logon ID: 0x3e5 Additional Information: Caller Workstation: LTRANPHD Target Account Name: Administrator Target Account Domain: LTRANPHD
Security	Audit Success	13824	2015-04-26 13:26:20	Microsoft-Windows-Security-Auditing	4797: An attempt was made to query the existence of a blank password for an account. Subject: Security ID: S-1-5-19 Account Name: LOCAL SERVICE Account Domain: NT AUTHORITY Logon ID: 0x3e5 Additional Information: Caller Workstation: LTRANPHD Target Account Name: Guest Target Account Domain: LTRANPHD
Security	Audit Success	13824	2015-04-26 13:26:20	Microsoft-Windows-Security-Auditing	4797: An attempt was made to query the existence of a blank password for an account. Subject: Security ID: S-1-5-19 Account Name: LOCAL SERVICE Account Domain: NT AUTHORITY Logon ID: 0x3e5 Additional Information: Caller Workstation: LTRANPHD Target Account Name: Liem Target Account Domain: LTRANPHD
Security	Audit Success	13824	2015-04-26 13:26:20	Microsoft-Windows-Security-Auditing	4797: An attempt was made to query the existence of a blank password for an account. Subject: Security ID: S-1-5-19 Account Name: LOCAL SERVICE Account Domain: NT AUTHORITY Logon ID: 0x3e5 Additional Information: Caller Workstation: LTRANPHD Target Account Name: Administrator Target Account Domain: LTRANPHD
Security	Audit Success	13824	2015-04-26 13:26:20	Microsoft-Windows-Security-Auditing	4797: An attempt was made to query the existence of a blank password for an account. Subject: Security ID: S-1-5-19 Account Name: LOCAL SERVICE Account Domain: NT AUTHORITY Logon ID: 0x3e5 Additional Information: Caller Workstation: LTRANPHD Target Account Name: Guest Target Account Domain: LTRANPHD
Security	Audit Success	13824	2015-04-26	Microsoft-Windows-Security-Auditing	4797: An attempt was made to query the existence of a blank password for an account. Subject: Security ID: S-1-5-19 Account Name: LOCAL SERVICE Account Domain: NT AUTHORITY Logon ID: 0x3e5 Additional

			13:26:20		Information: Caller Workstation: LTRANPHD Target Account Name: Liem Target Account Domain: LTRANPHD
Security	Audit Success	13824	2015-04-26 13:26:20	Microsoft-Windows-Security-Auditing	4797: An attempt was made to query the existence of a blank password for an account. Subject: Security ID: S-1-5-19 Account Name: LOCAL SERVICE Account Domain: NT AUTHORITY Logon ID: 0x3e5 Additional Information: Caller Workstation: LTRANPHD Target Account Name: Liem Target Account Domain: LTRANPHD
Security	Audit Success	13824	2015-04-26 13:26:22	Microsoft-Windows-Security-Auditing	4797: An attempt was made to query the existence of a blank password for an account. Subject: Security ID: S-1-5-21-1888849264-3803429180-4108621888-1001 Account Name: Liem Account Domain: LTRANPHD Logon ID: 0x1dd62 Additional Information: Caller Workstation: LTRANPHD Target Account Name: Administrator Target Account Domain: LTRANPHD
Security	Audit Success	13824	2015-04-26 13:26:22	Microsoft-Windows-Security-Auditing	4797: An attempt was made to query the existence of a blank password for an account. Subject: Security ID: S-1-5-21-1888849264-3803429180-4108621888-1001 Account Name: Liem Account Domain: LTRANPHD Logon ID: 0x1dd62 Additional Information: Caller Workstation: LTRANPHD Target Account Name: Guest Target Account Domain: LTRANPHD
Security	Audit Success	13824	2015-04-26 13:26:22	Microsoft-Windows-Security-Auditing	4797: An attempt was made to query the existence of a blank password for an account. Subject: Security ID: S-1-5-21-1888849264-3803429180-4108621888-1001 Account Name: Liem Account Domain: LTRANPHD Logon ID: 0x1dd62 Additional Information: Caller Workstation: LTRANPHD Target Account Name: Administrator Target Account Domain: LTRANPHD
Security	Audit Success	13824	2015-04-26 13:26:22	Microsoft-Windows-Security-Auditing	4797: An attempt was made to query the existence of a blank password for an account. Subject: Security ID: S-1-5-21-1888849264-3803429180-4108621888-1001 Account Name: Liem Account Domain: LTRANPHD Logon ID: 0x1dd62 Additional Information: Caller Workstation: LTRANPHD Target Account Name: Guest Target Account Domain: LTRANPHD
Security	Audit Success	12544	2015-04-26 13:41:00	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: LTRANPHD$ Account Domain: WORKGROUP Logon ID: 0x3e7 Logon Type: 5 Impersonation Level: %%1833 New Logon: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Logon ID: 0x3e7 Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x234 Process Name: C:\Windows\System32\services.exe Network Information: Workstation Name: Source Network Address: - Source Port: - Detailed Authentication Information: Logon Process: Advapi Authentication Package: Negotiate Transited Services: - Package Name (NTLM only): - Key Length: 0 This event is generated when a logon session is created. It is generated on the computer that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service such as the Server service, or a local process such as Winlogon.exe or Services.exe. The logon type field indicates the kind of logon that occurred. The most common types are 2 (interactive) and 3 (network). The New Logon fields indicate the account for whom the new logon was created, i.e. the account that was logged on. The network fields indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impersonation level field indicates the extent to which a process in the logon session can impersonate. The authentication information fields provide detailed information about this specific logon request. - Logon GUID is a unique identifier that can be used to correlate this event with a KDC event. - Transited services indicate which intermediate services have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indicates the length of the generated session key. This will be 0 if no session key was requested.
Security	Audit Success	12548	2015-04-26 13:41:00	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Logon ID: 0x3e7 Privileges: SeAssignPrimaryTokenPrivilege SeTcbPrivilege SeSecurityPrivilege SeTakeOwnershipPrivilege SeLoadDriverPrivilege SeBackupPrivilege SeRestorePrivilege SeDebugPrivilege SeAuditPrivilege SeSystemEnvironmentPrivilege SeImpersonatePrivilege
Security	Audit Success	12288	2015-04-27 17:04:49	Microsoft-Windows-Security-Auditing	4608: Windows is starting up. This event is logged when LSASS.EXE starts and the auditing subsystem is initialized.
Security	Audit Success	12292	2015-04-27 17:04:49	Microsoft-Windows-Security-Auditing	5033: The Windows Firewall Driver started successfully.
Security	Audit Success	12544	2015-04-27 17:04:49	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-0-0 Account Name: - Account Domain: - Logon ID: 0x0 Logon Type: 0 Impersonation Level: - New Logon: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Logon ID: 0x3e7 Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x4 Process Name: Network Information: Workstation Name: - Source Network Address: - Source Port: - Detailed Authentication Information: Logon Process: - Authentication Package: - Transited Services: - Package Name (NTLM only): - Key Length: 0 This event is generated when a logon session is created. It is generated on the computer that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service such as the Server service, or a local process such as Winlogon.exe or Services.exe. The logon type field indicates the kind of logon that occurred. The most common types are 2 (interactive) and 3 (network). The New Logon fields indicate the account for whom the new logon was created, i.e. the account that was logged on. The network fields indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impersonation level field indicates the extent to which a process in the logon session can impersonate. The authentication information fields provide detailed information about this specific logon request. - Logon GUID is a unique identifier that can be used to correlate this event with a KDC event. - Transited services indicate which intermediate services have participated in this logon

					request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indicates the length of the generated session key. This will be 0 if no session key was requested.
Security	Audit Success	12544	2015-04-27 17:04:49	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: LTRANPHD$ Account Domain: WORKGROUP Logon ID: 0x3e7 Logon Type: 5 Impersonation Level: %%1833 New Logon: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Logon ID: 0x3e7 Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x234 Process Name: C:\Windows\System32\services.exe Network Information: Workstation Name: Source Network Address: - Source Port: - Detailed Authentication Information: Logon Process: Advapi Authentication Package: Negotiate Transited Services: - Package Name (NTLM only): - Key Length: 0 This event is generated when a logon session is created. It is generated on the computer that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service such as the Server service, or a local process such as Winlogon.exe or Services.exe. The logon type field indicates the kind of logon that occurred. The most common types are 2 (interactive) and 3 (network). The New Logon fields indicate the account for whom the new logon was created, i.e. the account that was logged on. The network fields indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impersonation level field indicates the extent to which a process in the logon session can impersonate. The authentication information fields provide detailed information about this specific logon request. - Logon GUID is a unique identifier that can be used to correlate this event with a KDC event. - Transited services indicate which intermediate services have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indicates the length of the generated session key. This will be 0 if no session key was requested.
Security	Audit Success	12544	2015-04-27 17:04:49	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: LTRANPHD$ Account Domain: WORKGROUP Logon ID: 0x3e7 Logon Type: 5 Impersonation Level: %%1833 New Logon: Security ID: S-1-5-20 Account Name: NETWORK SERVICE Account Domain: NT AUTHORITY Logon ID: 0x3e4 Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x234 Process Name: C:\Windows\System32\services.exe Network Information: Workstation Name: Source Network Address: - Source Port: - Detailed Authentication Information: Logon Process: Advapi Authentication Package: Negotiate Transited Services: - Package Name (NTLM only): - Key Length: 0 This event is generated when a logon session is created. It is generated on the computer that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service such as the Server service, or a local process such as Winlogon.exe or Services.exe. The logon type field indicates the kind of logon that occurred. The most common types are 2 (interactive) and 3 (network). The New Logon fields indicate the account for whom the new logon was created, i.e. the account that was logged on. The network fields indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impersonation level field indicates the extent to which a process in the logon session can impersonate. The authentication information fields provide detailed information about this specific logon request. - Logon GUID is a unique identifier that can be used to correlate this event with a KDC event. - Transited services indicate which intermediate services have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indicates the length of the generated session key. This will be 0 if no session key was requested.
Security	Audit Success	12544	2015-04-27 17:04:49	Microsoft-Windows-Security-Auditing	4648: A logon was attempted using explicit credentials. Subject: Security ID: S-1-5-18 Account Name: LTRANPHD$ Account Domain: WORKGROUP Logon ID: 0x3e7 Logon GUID: {00000000-0000-0000-0000-000000000000} Account Whose Credentials Were Used: Account Name: DWM-1 Account Domain: Window Manager Logon GUID: {00000000-0000-0000-0000-000000000000} Target Server: Target Server Name: localhost Additional Information: localhost Process Information: Process ID: 0x204 Process Name: C:\Windows\System32\winlogon.exe Network Information: Network Address: - Port: - This event is generated when a process attempts to log on an account by explicitly specifying that account's credentials. This most commonly occurs in batch-type configurations such as scheduled tasks, or when using the RUNAS command.
Security	Audit Success	12544	2015-04-27 17:04:49	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: LTRANPHD$ Account Domain: WORKGROUP Logon ID: 0x3e7 Logon Type: 2 Impersonation Level: %%1833 New Logon: Security ID: S-1-5-90-1 Account Name: DWM-1 Account Domain: Window Manager Logon ID: 0xdc09 Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x204 Process Name: C:\Windows\System32\winlogon.exe Network Information: Workstation Name: Source Network Address: - Source Port: - Detailed Authentication Information: Logon Process: Advapi Authentication Package: Negotiate Transited Services: - Package Name (NTLM only): - Key Length: 0 This event is generated when a logon session is created. It is generated on the computer that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service such as the Server service, or a local process such as Winlogon.exe or Services.exe. The logon type field indicates the kind of logon that occurred. The most common types are 2 (interactive) and 3 (network). The New Logon fields indicate the account for whom the new logon was created, i.e. the account that was logged on. The network fields indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impersonation level field indicates the extent to which a process in the logon session can impersonate. The authentication information fields provide detailed information about this specific logon request. - Logon GUID is a unique identifier that can be used to correlate this event with a KDC event. - Transited services indicate which intermediate services have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indicates the length of the generated session key. This will be 0 if no session key was requested.

Security	Audit Success	12544	2015-04-27 17:04:49	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: LTRANPHD$ Account Domain: WORKGROUP Logon ID: 0x3e7 Logon Type: 2 Impersonation Level: %%1833 New Logon: Security ID: S-1-5-90-1 Account Name: DWM-1 Account Domain: Window Manager Logon ID: 0xdc22 Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x204 Process Name: C:\Windows\System32\winlogon.exe Network Information: Workstation Name: Source Network Address: - Source Port: - Detailed Authentication Information: Logon Process: Advapi Authentication Package: Negotiate Transited Services: - Package Name (NTLM only): - Key Length: 0 This event is generated when a logon session is created. It is generated on the computer that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service such as the Server service, or a local process such as Winlogon.exe or Services.exe. The logon type field indicates the kind of logon that occurred. The most common types are 2 (interactive) and 3 (network). The New Logon fields indicate the account for whom the new logon was created, i.e. the account that was logged on. The network fields indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impersonation level field indicates the extent to which a process in the logon session can impersonate. The authentication information fields provide detailed information about this specific logon request. - Logon GUID is a unique identifier that can be used to correlate this event with a KDC event. - Transited services indicate which intermediate services have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indicates the length of the generated session key. This will be 0 if no session key was requested.
Security	Audit Success	12544	2015-04-27 17:04:49	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: LTRANPHD$ Account Domain: WORKGROUP Logon ID: 0x3e7 Logon Type: 5 Impersonation Level: %%1833 New Logon: Security ID: S-1-5-19 Account Name: LOCAL SERVICE Account Domain: NT AUTHORITY Logon ID: 0x3e5 Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x234 Process Name: C:\Windows\System32\services.exe Network Information: Workstation Name: Source Network Address: - Source Port: - Detailed Authentication Information: Logon Process: Advapi Authentication Package: Negotiate Transited Services: - Package Name (NTLM only): - Key Length: 0 This event is generated when a logon session is created. It is generated on the computer that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service such as the Server service, or a local process such as Winlogon.exe or Services.exe. The logon type field indicates the kind of logon that occurred. The most common types are 2 (interactive) and 3 (network). The New Logon fields indicate the account for whom the new logon was created, i.e. the account that was logged on. The network fields indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impersonation level field indicates the extent to which a process in the logon session can impersonate. The authentication information fields provide detailed information about this specific logon request. - Logon GUID is a unique identifier that can be used to correlate this event with a KDC event. - Transited services indicate which intermediate services have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indicates the length of the generated session key. This will be 0 if no session key was requested.
Security	Audit Success	12544	2015-04-27 17:04:49	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: LTRANPHD$ Account Domain: WORKGROUP Logon ID: 0x3e7 Logon Type: 5 Impersonation Level: %%1833 New Logon: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Logon ID: 0x3e7 Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x234 Process Name: C:\Windows\System32\services.exe Network Information: Workstation Name: Source Network Address: - Source Port: - Detailed Authentication Information: Logon Process: Advapi Authentication Package: Negotiate Transited Services: - Package Name (NTLM only): - Key Length: 0 This event is generated when a logon session is created. It is generated on the computer that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service such as the Server service, or a local process such as Winlogon.exe or Services.exe. The logon type field indicates the kind of logon that occurred. The most common types are 2 (interactive) and 3 (network). The New Logon fields indicate the account for whom the new logon was created, i.e. the account that was logged on. The network fields indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impersonation level field indicates the extent to which a process in the logon session can impersonate. The authentication information fields provide detailed information about this specific logon request. - Logon GUID is a unique identifier that can be used to correlate this event with a KDC event. - Transited services indicate which intermediate services have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indicates the length of the generated session key. This will be 0 if no session key was requested.
Security	Audit	12544	2015-04-27	Microsoft-Windows-Security-	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: LTRANPHD$ Account Domain: WORKGROUP Logon ID: 0x3e7 Logon Type: 5 Impersonation Level: %%1833 New Logon: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Logon ID: 0x3e7 Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x234 Process Name: C:\Windows\System32\services.exe Network Information: Workstation Name: Source Network Address: - Source Port: - Detailed Authentication Information: Logon Process: Advapi Authentication Package: Negotiate Transited Services: - Package Name (NTLM only): - Key Length: 0 This event is generated when a logon session is created. It is generated on the computer that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service such as the Server service, or a local process such as Winlogon.exe or Services.exe. The logon type field indicates the kind of logon that occurred.

	Success		17:04:49	Auditing	The most common types are 2 (interactive) and 3 (network). The New Logon fields indicate the account for whom the new logon was created, i.e. the account that was logged on. The network fields indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impersonation level field indicates the extent to which a process in the logon session can impersonate. The authentication information fields provide detailed information about this specific logon request. - Logon GUID is a unique identifier that can be used to correlate this event with a KDC event. - Transited services indicate which intermediate services have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indicates the length of the generated session key. This will be 0 if no session key was requested.
Security	Audit Success	12544	2015-04-27 17:04:49	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: LTRANPHD$ Account Domain: WORKGROUP Logon ID: 0x3e7 Logon Type: 5 Impersonation Level: %%1833 New Logon: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Logon ID: 0x3e7 Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x234 Process Name: C:\Windows\System32\services.exe Network Information: Workstation Name: Source Network Address: - Source Port: - Detailed Authentication Information: Logon Process: Advapi Authentication Package: Negotiate Transited Services: - Package Name (NTLM only): - Key Length: 0 This event is generated when a logon session is created. It is generated on the computer that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service such as the Server service, or a local process such as Winlogon.exe or Services.exe. The logon type field indicates the kind of logon that occurred. The most common types are 2 (interactive) and 3 (network). The New Logon fields indicate the account for whom the new logon was created, i.e. the account that was logged on. The network fields indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impersonation level field indicates the extent to which a process in the logon session can impersonate. The authentication information fields provide detailed information about this specific logon request. - Logon GUID is a unique identifier that can be used to correlate this event with a KDC event. - Transited services indicate which intermediate services have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indicates the length of the generated session key. This will be 0 if no session key was requested.
Security	Audit Success	12548	2015-04-27 17:04:49	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Logon ID: 0x3e7 Privileges: SeAssignPrimaryTokenPrivilege SeTcbPrivilege SeSecurityPrivilege SeTakeOwnershipPrivilege SeLoadDriverPrivilege SeBackupPrivilege SeRestorePrivilege SeDebugPrivilege SeAuditPrivilege SeSystemEnvironmentPrivilege SeImpersonatePrivilege
Security	Audit Success	12548	2015-04-27 17:04:49	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-20 Account Name: NETWORK SERVICE Account Domain: NT AUTHORITY Logon ID: 0x3e4 Privileges: SeAssignPrimaryTokenPrivilege SeAuditPrivilege SeImpersonatePrivilege
Security	Audit Success	12548	2015-04-27 17:04:49	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-90-1 Account Name: DWM-1 Account Domain: Window Manager Logon ID: 0xdc09 Privileges: SeAssignPrimaryTokenPrivilege SeAuditPrivilege SeImpersonatePrivilege
Security	Audit Success	12548	2015-04-27 17:04:49	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-90-1 Account Name: DWM-1 Account Domain: Window Manager Logon ID: 0xdc22 Privileges: SeAssignPrimaryTokenPrivilege SeAuditPrivilege
Security	Audit Success	12548	2015-04-27 17:04:49	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-19 Account Name: LOCAL SERVICE Account Domain: NT AUTHORITY Logon ID: 0x3e5 Privileges: SeAssignPrimaryTokenPrivilege SeAuditPrivilege SeImpersonatePrivilege
Security	Audit Success	12548	2015-04-27 17:04:49	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Logon ID: 0x3e7 Privileges: SeAssignPrimaryTokenPrivilege SeTcbPrivilege SeSecurityPrivilege SeTakeOwnershipPrivilege SeLoadDriverPrivilege SeBackupPrivilege SeRestorePrivilege SeDebugPrivilege SeAuditPrivilege SeSystemEnvironmentPrivilege SeImpersonatePrivilege
Security	Audit Success	12548	2015-04-27 17:04:49	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Logon ID: 0x3e7 Privileges: SeAssignPrimaryTokenPrivilege SeTcbPrivilege SeSecurityPrivilege SeTakeOwnershipPrivilege SeLoadDriverPrivilege SeBackupPrivilege SeRestorePrivilege SeDebugPrivilege SeAuditPrivilege SeSystemEnvironmentPrivilege SeImpersonatePrivilege
Security	Audit Success	12548	2015-04-27 17:04:49	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Logon ID: 0x3e7 Privileges: SeAssignPrimaryTokenPrivilege SeTcbPrivilege SeSecurityPrivilege SeTakeOwnershipPrivilege SeLoadDriverPrivilege SeBackupPrivilege SeRestorePrivilege SeDebugPrivilege SeAuditPrivilege SeSystemEnvironmentPrivilege SeImpersonatePrivilege
Security	Audit Success	13568	2015-04-27 17:04:49	Microsoft-Windows-Security-Auditing	4902: The Per-user audit policy table was created. Number of Elements: 0 Policy ID: 0x8cb6
Security	Audit Success	101	2015-04-27 17:04:50	Microsoft-Windows-Eventlog	1101: Audit events have been dropped by the transport. 0
Security	Audit Success	12292	2015-04-27	Microsoft-Windows-Security-Auditing	5024: The Windows Firewall service started successfully.

			17:04:50		
Security	Audit Success	12544	2015-04-27 17:04:50	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: LTRANPHD$ Account Domain: WORKGROUP Logon ID: 0x3e7 Logon Type: 5 Impersonation Level: %%1833 New Logon: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Logon ID: 0x3e7 Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x234 Process Name: C:\Windows\System32\services.exe Network Information: Workstation Name: Source Network Address: - Source Port: - Detailed Authentication Information: Logon Process: Advapi Authentication Package: Negotiate Transited Services: - Package Name (NTLM only): - Key Length: 0 This event is generated when a logon session is created. It is generated on the computer that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service such as the Server service, or a local process such as Winlogon.exe or Services.exe. The logon type field indicates the kind of logon that occurred. The most common types are 2 (interactive) and 3 (network). The New Logon fields indicate the account for whom the new logon was created, i.e. the account that was logged on. The network fields indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impersonation level field indicates the extent to which a process in the logon session can impersonate. The authentication information fields provide detailed information about this specific logon request. - Logon GUID is a unique identifier that can be used to correlate this event with a KDC event. - Transited services indicate which intermediate services have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indicates the length of the generated session key. This will be 0 if no session key was requested.
Security	Audit Success	12544	2015-04-27 17:04:50	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: LTRANPHD$ Account Domain: WORKGROUP Logon ID: 0x3e7 Logon Type: 5 Impersonation Level: %%1833 New Logon: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Logon ID: 0x3e7 Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x234 Process Name: C:\Windows\System32\services.exe Network Information: Workstation Name: Source Network Address: - Source Port: - Detailed Authentication Information: Logon Process: Advapi Authentication Package: Negotiate Transited Services: - Package Name (NTLM only): - Key Length: 0 This event is generated when a logon session is created. It is generated on the computer that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service such as the Server service, or a local process such as Winlogon.exe or Services.exe. The logon type field indicates the kind of logon that occurred. The most common types are 2 (interactive) and 3 (network). The New Logon fields indicate the account for whom the new logon was created, i.e. the account that was logged on. The network fields indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impersonation level field indicates the extent to which a process in the logon session can impersonate. The authentication information fields provide detailed information about this specific logon request. - Logon GUID is a unique identifier that can be used to correlate this event with a KDC event. - Transited services indicate which intermediate services have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indicates the length of the generated session key. This will be 0 if no session key was requested.
Security	Audit Success	12544	2015-04-27 17:04:50	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-0-0 Account Name: - Account Domain: - Logon ID: 0x0 Logon Type: 3 Impersonation Level: %%1833 New Logon: Security ID: S-1-5-7 Account Name: ANONYMOUS LOGON Account Domain: NT AUTHORITY Logon ID: 0x187e8 Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x0 Process Name: - Network Information: Workstation Name: Source Network Address: - Source Port: - Detailed Authentication Information: Logon Process: NtLmSsp Authentication Package: NTLM Transited Services: - Package Name (NTLM only): NTLM V1 Key Length: 0 This event is generated when a logon session is created. It is generated on the computer that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service such as the Server service, or a local process such as Winlogon.exe or Services.exe. The logon type field indicates the kind of logon that occurred. The most common types are 2 (interactive) and 3 (network). The New Logon fields indicate the account for whom the new logon was created, i.e. the account that was logged on. The network fields indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impersonation level field indicates the extent to which a process in the logon session can impersonate. The authentication information fields provide detailed information about this specific logon request. - Logon GUID is a unique identifier that can be used to correlate this event with a KDC event. - Transited services indicate which intermediate services have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indicates the length of the generated session key. This will be 0 if no session key was requested.
Security	Audit Success	12548	2015-04-27 17:04:50	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Logon ID: 0x3e7 Privileges: SeAssignPrimaryTokenPrivilege SeTcbPrivilege SeSecurityPrivilege SeTakeOwnershipPrivilege SeLoadDriverPrivilege SeBackupPrivilege SeRestorePrivilege SeDebugPrivilege SeAuditPrivilege SeSystemEnvironmentPrivilege SeImpersonatePrivilege
Security	Audit Success	12548	2015-04-27 17:04:50	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Logon ID: 0x3e7 Privileges: SeAssignPrimaryTokenPrivilege SeTcbPrivilege SeSecurityPrivilege SeTakeOwnershipPrivilege SeLoadDriverPrivilege SeBackupPrivilege SeRestorePrivilege SeDebugPrivilege SeAuditPrivilege SeSystemEnvironmentPrivilege SeImpersonatePrivilege
					4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: LTRANPHD$

Security	Audit Success	12544	2015-04-27 17:04:54	Microsoft-Windows-Security-Auditing	Account Domain: WORKGROUP Logon ID: 0x3e7 Logon Type: 5 Impersonation Level: %%1833 New Logon: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Logon ID: 0x3e7 Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x234 Process Name: C:\Windows\System32\services.exe Network Information: Workstation Name: Source Network Address: - Source Port: - Detailed Authentication Information: Logon Process: Advapi Authentication Package: Negotiate Transited Services: - Package Name (NTLM only): - Key Length: 0 This event is generated when a logon session is created. It is generated on the computer that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service such as the Server service, or a local process such as Winlogon.exe or Services.exe. The logon type field indicates the kind of logon that occurred. The most common types are 2 (interactive) and 3 (network). The New Logon fields indicate the account for whom the new logon was created, i.e. the account that was logged on. The network fields indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impersonation level field indicates the extent to which a process in the logon session can impersonate. The authentication information fields provide detailed information about this specific logon request. - Logon GUID is a unique identifier that can be used to correlate this event with a KDC event. - Transited services indicate which intermediate services have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indicates the length of the generated session key. This will be 0 if no session key was requested.
Security	Audit Success	12548	2015-04-27 17:04:54	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Logon ID: 0x3e7 Privileges: SeAssignPrimaryTokenPrivilege SeTcbPrivilege SeSecurityPrivilege SeTakeOwnershipPrivilege SeLoadDriverPrivilege SeBackupPrivilege SeRestorePrivilege SeDebugPrivilege SeAuditPrivilege SeSystemEnvironmentPrivilege SeImpersonatePrivilege
Security	Audit Success	12544	2015-04-27 17:04:55	Microsoft-Windows-Security-Auditing	4648: A logon was attempted using explicit credentials. Subject: Security ID: S-1-5-18 Account Name: LTRANPHD$ Account Domain: WORKGROUP Logon ID: 0x3e7 Logon GUID: {00000000-0000-0000-0000-000000000000} Account Whose Credentials Were Used: Account Name: Liem Account Domain: LTRANPHD Logon GUID: {00000000-0000-0000-0000-000000000000} Target Server: Target Server Name: localhost Additional Information: localhost Process Information: Process ID: 0x204 Process Name: C:\Windows\System32\winlogon.exe Network Information: Network Address: 127.0.0.1 Port: 0 This event is generated when a process attempts to log on an account by explicitly specifying that account's credentials. This most commonly occurs in batch-type configurations such as scheduled tasks, or when using the RUNAS command.
Security	Audit Success	12544	2015-04-27 17:04:55	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: LTRANPHD$ Account Domain: WORKGROUP Logon ID: 0x3e7 Logon Type: 2 Impersonation Level: %%1833 New Logon: Security ID: S-1-5-21-1888849264-3803429180-4108621888-1001 Account Name: Liem Account Domain: LTRANPHD Logon ID: 0x264a8 Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x204 Process Name: C:\Windows\System32\winlogon.exe Network Information: Workstation Name: LTRANPHD Source Network Address: 127.0.0.1 Source Port: 0 Detailed Authentication Information: Logon Process: User32 Authentication Package: Negotiate Transited Services: - Package Name (NTLM only): - Key Length: 0 This event is generated when a logon session is created. It is generated on the computer that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service such as the Server service, or a local process such as Winlogon.exe or Services.exe. The logon type field indicates the kind of logon that occurred. The most common types are 2 (interactive) and 3 (network). The New Logon fields indicate the account for whom the new logon was created, i.e. the account that was logged on. The network fields indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impersonation level field indicates the extent to which a process in the logon session can impersonate. The authentication information fields provide detailed information about this specific logon request. - Logon GUID is a unique identifier that can be used to correlate this event with a KDC event. - Transited services indicate which intermediate services have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indicates the length of the generated session key. This will be 0 if no session key was requested.
Security	Audit Success	12544	2015-04-27 17:04:55	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: LTRANPHD$ Account Domain: WORKGROUP Logon ID: 0x3e7 Logon Type: 2 Impersonation Level: %%1833 New Logon: Security ID: S-1-5-21-1888849264-3803429180-4108621888-1001 Account Name: Liem Account Domain: LTRANPHD Logon ID: 0x264d2 Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x204 Process Name: C:\Windows\System32\winlogon.exe Network Information: Workstation Name: LTRANPHD Source Network Address: 127.0.0.1 Source Port: 0 Detailed Authentication Information: Logon Process: User32 Authentication Package: Negotiate Transited Services: - Package Name (NTLM only): - Key Length: 0 This event is generated when a logon session is created. It is generated on the computer that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service such as the Server service, or a local process such as Winlogon.exe or Services.exe. The logon type field indicates the kind of logon that occurred. The most common types are 2 (interactive) and 3 (network). The New Logon fields indicate the account for whom the new logon was created, i.e. the account that was logged on. The network fields indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impersonation level field indicates the extent to which a process in the logon session can impersonate. The authentication information fields provide detailed information about this specific logon request. - Logon GUID is a unique identifier that can be used to correlate this event with a KDC event. - Transited services indicate which intermediate services have participated in this

					logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indicates the length of the generated session key. This will be 0 if no session key was requested.
	Security	Audit Success	12548	2015-04-27 17:04:55	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-21-1888849264-3803429180-4108621888-1001 Account Name: Liem Account Domain: LTRANPHD Logon ID: 0x264a8 Privileges: SeSecurityPrivilege SeTakeOwnershipPrivilege SeLoadDriverPrivilege SeBackupPrivilege SeRestorePrivilege SeDebugPrivilege SeSystemEnvironmentPrivilege SeImpersonatePrivilege
	Security	Audit Success	12544	2015-04-27 17:04:56	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: LTRANPHD$ Account Domain: WORKGROUP Logon ID: 0x3e7 Logon Type: 5 Impersonation Level: %%1833 New Logon: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Logon ID: 0x3e7 Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x234 Process Name: C:\Windows\System32\services.exe Network Information: Workstation Name: Source Network Address: - Source Port: - Detailed Authentication Information: Logon Process: Advapi Authentication Package: Negotiate Transited Services: - Package Name (NTLM only): - Key Length: 0 This event is generated when a logon session is created. It is generated on the computer that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service such as the Server service, or a local process such as Winlogon.exe or Services.exe. The logon type field indicates the kind of logon that occurred. The most common types are 2 (interactive) and 3 (network). The New Logon fields indicate the account for whom the new logon was created, i.e. the account that was logged on. The network fields indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impersonation level field indicates the extent to which a process in the logon session can impersonate. The authentication information fields provide detailed information about this specific logon request. - Logon GUID is a unique identifier that can be used to correlate this event with a KDC event. - Transited services indicate which intermediate services have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indicates the length of the generated session key. This will be 0 if no session key was requested.
	Security	Audit Success	12544	2015-04-27 17:04:56	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: LTRANPHD$ Account Domain: WORKGROUP Logon ID: 0x3e7 Logon Type: 5 Impersonation Level: %%1833 New Logon: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Logon ID: 0x3e7 Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x234 Process Name: C:\Windows\System32\services.exe Network Information: Workstation Name: Source Network Address: - Source Port: - Detailed Authentication Information: Logon Process: Advapi Authentication Package: Negotiate Transited Services: - Package Name (NTLM only): - Key Length: 0 This event is generated when a logon session is created. It is generated on the computer that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service such as the Server service, or a local process such as Winlogon.exe or Services.exe. The logon type field indicates the kind of logon that occurred. The most common types are 2 (interactive) and 3 (network). The New Logon fields indicate the account for whom the new logon was created, i.e. the account that was logged on. The network fields indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impersonation level field indicates the extent to which a process in the logon session can impersonate. The authentication information fields provide detailed information about this specific logon request. - Logon GUID is a unique identifier that can be used to correlate this event with a KDC event. - Transited services indicate which intermediate services have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indicates the length of the generated session key. This will be 0 if no session key was requested.
	Security	Audit Success	12548	2015-04-27 17:04:56	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Logon ID: 0x3e7 Privileges: SeAssignPrimaryTokenPrivilege SeTcbPrivilege SeSecurityPrivilege SeTakeOwnershipPrivilege SeLoadDriverPrivilege SeBackupPrivilege SeRestorePrivilege SeDebugPrivilege SeAuditPrivilege SeSystemEnvironmentPrivilege SeImpersonatePrivilege
	Security	Audit Success	12548	2015-04-27 17:04:56	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Logon ID: 0x3e7 Privileges: SeAssignPrimaryTokenPrivilege SeTcbPrivilege SeSecurityPrivilege SeTakeOwnershipPrivilege SeLoadDriverPrivilege SeBackupPrivilege SeRestorePrivilege SeDebugPrivilege SeAuditPrivilege SeSystemEnvironmentPrivilege SeImpersonatePrivilege
	Security	Audit Success	13824	2015-04-27 17:04:58	Microsoft-Windows-Security-Auditing	4797: An attempt was made to query the existence of a blank password for an account. Subject: Security ID: S-1-5-21-1888849264-3803429180-4108621888-1001 Account Name: Liem Account Domain: LTRANPHD Logon ID: 0x264d2 Additional Information: Caller Workstation: LTRANPHD Target Account Name: Administrator Target Account Domain: LTRANPHD
	Security	Audit Success	13824	2015-04-27 17:04:58	Microsoft-Windows-Security-Auditing	4797: An attempt was made to query the existence of a blank password for an account. Subject: Security ID: S-1-5-21-1888849264-3803429180-4108621888-1001 Account Name: Liem Account Domain: LTRANPHD Logon ID: 0x264d2 Additional Information: Caller Workstation: LTRANPHD Target Account Name: Guest Target Account Domain: LTRANPHD
	Security	Audit Success	13824	2015-04-27 17:04:58	Microsoft-Windows-Security-Auditing	4797: An attempt was made to query the existence of a blank password for an account. Subject: Security ID: S-1-5-21-1888849264-3803429180-4108621888-1001 Account Name: Liem Account Domain: LTRANPHD Logon ID: 0x264d2 Additional Information: Caller Workstation: LTRANPHD Target Account Name: Administrator Target Account Domain: LTRANPHD
				2015-04-		4797: An attempt was made to query the existence of a blank password for an account. Subject: Security ID:

Security	Audit Success	13824	27 17:04:58	Microsoft-Windows-Security-Auditing	S-1-5-21-1888849264-3803429180-4108621888-1001 Account Name: Liem Account Domain: LTRANPHD Logon ID: 0x264d2 Additional Information: Caller Workstation: LTRANPHD Target Account Name: Guest Target Account Domain: LTRANPHD
Security	Audit Success	13824	2015-04-27 17:04:58	Microsoft-Windows-Security-Auditing	4797: An attempt was made to query the existence of a blank password for an account. Subject: Security ID: S-1-5-19 Account Name: LOCAL SERVICE Account Domain: NT AUTHORITY Logon ID: 0x3e5 Additional Information: Caller Workstation: LTRANPHD Target Account Name: Administrator Target Account Domain: LTRANPHD
Security	Audit Success	13824	2015-04-27 17:04:58	Microsoft-Windows-Security-Auditing	4797: An attempt was made to query the existence of a blank password for an account. Subject: Security ID: S-1-5-19 Account Name: LOCAL SERVICE Account Domain: NT AUTHORITY Logon ID: 0x3e5 Additional Information: Caller Workstation: LTRANPHD Target Account Name: Administrator Target Account Domain: LTRANPHD
Security	Audit Success	13824	2015-04-27 17:04:58	Microsoft-Windows-Security-Auditing	4797: An attempt was made to query the existence of a blank password for an account. Subject: Security ID: S-1-5-19 Account Name: LOCAL SERVICE Account Domain: NT AUTHORITY Logon ID: 0x3e5 Additional Information: Caller Workstation: LTRANPHD Target Account Name: Guest Target Account Domain: LTRANPHD
Security	Audit Success	13824	2015-04-27 17:04:58	Microsoft-Windows-Security-Auditing	4797: An attempt was made to query the existence of a blank password for an account. Subject: Security ID: S-1-5-19 Account Name: LOCAL SERVICE Account Domain: NT AUTHORITY Logon ID: 0x3e5 Additional Information: Caller Workstation: LTRANPHD Target Account Name: Guest Target Account Domain: LTRANPHD
Security	Audit Success	13824	2015-04-27 17:04:58	Microsoft-Windows-Security-Auditing	4797: An attempt was made to query the existence of a blank password for an account. Subject: Security ID: S-1-5-19 Account Name: LOCAL SERVICE Account Domain: NT AUTHORITY Logon ID: 0x3e5 Additional Information: Caller Workstation: LTRANPHD Target Account Name: Liem Target Account Domain: LTRANPHD
Security	Audit Success	13824	2015-04-27 17:04:58	Microsoft-Windows-Security-Auditing	4797: An attempt was made to query the existence of a blank password for an account. Subject: Security ID: S-1-5-19 Account Name: LOCAL SERVICE Account Domain: NT AUTHORITY Logon ID: 0x3e5 Additional Information: Caller Workstation: LTRANPHD Target Account Name: Liem Target Account Domain: LTRANPHD
Security	Audit Success	13824	2015-04-27 17:04:58	Microsoft-Windows-Security-Auditing	4797: An attempt was made to query the existence of a blank password for an account. Subject: Security ID: S-1-5-19 Account Name: LOCAL SERVICE Account Domain: NT AUTHORITY Logon ID: 0x3e5 Additional Information: Caller Workstation: LTRANPHD Target Account Name: Liem Target Account Domain: LTRANPHD
Security	Audit Success	13824	2015-04-27 17:04:58	Microsoft-Windows-Security-Auditing	4797: An attempt was made to query the existence of a blank password for an account. Subject: Security ID: S-1-5-19 Account Name: LOCAL SERVICE Account Domain: NT AUTHORITY Logon ID: 0x3e5 Additional Information: Caller Workstation: LTRANPHD Target Account Name: Liem Target Account Domain: LTRANPHD
Security	Audit Success	13824	2015-04-27 17:06:23	Microsoft-Windows-Security-Auditing	4797: An attempt was made to query the existence of a blank password for an account. Subject: Security ID: S-1-5-21-1888849264-3803429180-4108621888-1001 Account Name: Liem Account Domain: LTRANPHD Logon ID: 0x264d2 Additional Information: Caller Workstation: LTRANPHD Target Account Name: Administrator Target Account Domain: LTRANPHD
Security	Audit Success	13824	2015-04-27 17:06:23	Microsoft-Windows-Security-Auditing	4797: An attempt was made to query the existence of a blank password for an account. Subject: Security ID: S-1-5-21-1888849264-3803429180-4108621888-1001 Account Name: Liem Account Domain: LTRANPHD Logon ID: 0x264d2 Additional Information: Caller Workstation: LTRANPHD Target Account Name: Guest Target Account Domain: LTRANPHD
Security	Audit Success	13824	2015-04-27 17:06:23	Microsoft-Windows-Security-Auditing	4797: An attempt was made to query the existence of a blank password for an account. Subject: Security ID: S-1-5-21-1888849264-3803429180-4108621888-1001 Account Name: Liem Account Domain: LTRANPHD Logon ID: 0x264d2 Additional Information: Caller Workstation: LTRANPHD Target Account Name: Administrator Target Account Domain: LTRANPHD
Security	Audit Success	13824	2015-04-27 17:06:23	Microsoft-Windows-Security-Auditing	4797: An attempt was made to query the existence of a blank password for an account. Subject: Security ID: S-1-5-21-1888849264-3803429180-4108621888-1001 Account Name: Liem Account Domain: LTRANPHD Logon ID: 0x264d2 Additional Information: Caller Workstation: LTRANPHD Target Account Name: Guest Target Account Domain: LTRANPHD
Security	Audit Success	13824	2015-04-27 17:27:32	Microsoft-Windows-Security-Auditing	4797: An attempt was made to query the existence of a blank password for an account. Subject: Security ID: S-1-5-21-1888849264-3803429180-4108621888-1001 Account Name: Liem Account Domain: LTRANPHD Logon ID: 0x264d2 Additional Information: Caller Workstation: LTRANPHD Target Account Name: Administrator Target Account Domain: LTRANPHD
Security	Audit Success	13824	2015-04-27 17:27:32	Microsoft-Windows-Security-Auditing	4797: An attempt was made to query the existence of a blank password for an account. Subject: Security ID: S-1-5-21-1888849264-3803429180-4108621888-1001 Account Name: Liem Account Domain: LTRANPHD Logon ID: 0x264d2 Additional Information: Caller Workstation: LTRANPHD Target Account Name: Guest Target Account Domain: LTRANPHD
Security	Audit Success	13824	2015-04-27 17:27:35	Microsoft-Windows-Security-Auditing	4797: An attempt was made to query the existence of a blank password for an account. Subject: Security ID: S-1-5-21-1888849264-3803429180-4108621888-1001 Account Name: Liem Account Domain: LTRANPHD Logon ID: 0x264d2 Additional Information: Caller Workstation: LTRANPHD Target Account Name: Administrator Target Account Domain: LTRANPHD
Security	Audit Success	13824	2015-04-27 17:27:35	Microsoft-Windows-Security-Auditing	4797: An attempt was made to query the existence of a blank password for an account. Subject: Security ID: S-1-5-21-1888849264-3803429180-4108621888-1001 Account Name: Liem Account Domain: LTRANPHD Logon ID: 0x264d2 Additional Information: Caller Workstation: LTRANPHD Target Account Name: Guest Target Account Domain: LTRANPHD
Security	Audit	13824	2015-04-27	Microsoft-Windows-Security-	4797: An attempt was made to query the existence of a blank password for an account. Subject: Security ID: S-1-5-21-1888849264-3803429180-4108621888-1001 Account Name: Liem Account Domain: LTRANPHD Logon

	Success		17:27:44	Auditing	ID: 0x264d2 Additional Information: Caller Workstation: LTRANPHD Target Account Name: Guest Target Account Domain: LTRANPHD
Security	Audit Success	13824	2015-04-27 17:27:50	Microsoft-Windows-Security-Auditing	4797: An attempt was made to query the existence of a blank password for an account. Subject: Security ID: S-1-5-21-1888849264-3803429180-4108621888-1001 Account Name: Liem Account Domain: LTRANPHD Logon ID: 0x264d2 Additional Information: Caller Workstation: LTRANPHD Target Account Name: Administrator Target Account Domain: LTRANPHD
Security	Audit Success	13824	2015-04-27 17:27:50	Microsoft-Windows-Security-Auditing	4797: An attempt was made to query the existence of a blank password for an account. Subject: Security ID: S-1-5-21-1888849264-3803429180-4108621888-1001 Account Name: Liem Account Domain: LTRANPHD Logon ID: 0x264d2 Additional Information: Caller Workstation: LTRANPHD Target Account Name: Guest Target Account Domain: LTRANPHD
Security	Audit Success	13824	2015-04-27 17:28:01	Microsoft-Windows-Security-Auditing	4797: An attempt was made to query the existence of a blank password for an account. Subject: Security ID: S-1-5-21-1888849264-3803429180-4108621888-1001 Account Name: Liem Account Domain: LTRANPHD Logon ID: 0x264d2 Additional Information: Caller Workstation: LTRANPHD Target Account Name: Administrator Target Account Domain: LTRANPHD
Security	Audit Success	13824	2015-04-27 17:28:01	Microsoft-Windows-Security-Auditing	4797: An attempt was made to query the existence of a blank password for an account. Subject: Security ID: S-1-5-21-1888849264-3803429180-4108621888-1001 Account Name: Liem Account Domain: LTRANPHD Logon ID: 0x264d2 Additional Information: Caller Workstation: LTRANPHD Target Account Name: Guest Target Account Domain: LTRANPHD
Security	Audit Success	12288	2015-04-27 17:35:01	Microsoft-Windows-Security-Auditing	4608: Windows is starting up. This event is logged when LSASS.EXE starts and the auditing subsystem is initialized.
Security	Audit Success	12544	2015-04-27 17:35:01	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-0-0 Account Name: - Account Domain: - Logon ID: 0x0 Logon Type: 0 Impersonation Level: - New Logon: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Logon ID: 0x3e7 Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x4 Process Name: Network Information: Workstation Name: - Source Network Address: - Source Port: - Detailed Authentication Information: Logon Process: - Authentication Package: - Transited Services: - Package Name (NTLM only): - Key Length: 0 This event is generated when a logon session is created. It is generated on the computer that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service such as the Server service, or a local process such as Winlogon.exe or Services.exe. The logon type field indicates the kind of logon that occurred. The most common types are 2 (interactive) and 3 (network). The New Logon fields indicate the account for whom the new logon was created, i.e. the account that was logged on. The network fields indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impersonation level field indicates the extent to which a process in the logon session can impersonate. The authentication information fields provide detailed information about this specific logon request. - Logon GUID is a unique identifier that can be used to correlate this event with a KDC event. - Transited services indicate which intermediate services have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indicates the length of the generated session key. This will be 0 if no session key was requested.
Security	Audit Success	12544	2015-04-27 17:35:01	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: LTRANPHD$ Account Domain: WORKGROUP Logon ID: 0x3e7 Logon Type: 5 Impersonation Level: %%1833 New Logon: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Logon ID: 0x3e7 Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x238 Process Name: C:\Windows\System32\services.exe Network Information: Workstation Name: Source Network Address: - Source Port: - Detailed Authentication Information: Logon Process: Advapi Authentication Package: Negotiate Transited Services: - Package Name (NTLM only): - Key Length: 0 This event is generated when a logon session is created. It is generated on the computer that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service such as the Server service, or a local process such as Winlogon.exe or Services.exe. The logon type field indicates the kind of logon that occurred. The most common types are 2 (interactive) and 3 (network). The New Logon fields indicate the account for whom the new logon was created, i.e. the account that was logged on. The network fields indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impersonation level field indicates the extent to which a process in the logon session can impersonate. The authentication information fields provide detailed information about this specific logon request. - Logon GUID is a unique identifier that can be used to correlate this event with a KDC event. - Transited services indicate which intermediate services have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indicates the length of the generated session key. This will be 0 if no session key was requested.
					4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: LTRANPHD$ Account Domain: WORKGROUP Logon ID: 0x3e7 Logon Type: 5 Impersonation Level: %%1833 New Logon: Security ID: S-1-5-20 Account Name: NETWORK SERVICE Account Domain: NT AUTHORITY Logon ID: 0x3e4 Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x238 Process Name: C:\Windows\System32\services.exe Network Information: Workstation Name: Source Network Address: - Source Port: - Detailed Authentication Information: Logon Process: Advapi Authentication Package: Negotiate Transited Services: - Package Name (NTLM only): - Key Length: 0 This event is generated when a logon session is created. It is generated on the computer that was accessed. The subject fields indicate the account on the

Security	Audit Success	12544	2015-04-27 17:35:01	Microsoft-Windows-Security-Auditing	local system which requested the logon. This is most commonly a service such as the Server service, or a local process such as Winlogon.exe or Services.exe. The logon type field indicates the kind of logon that occurred. The most common types are 2 (interactive) and 3 (network). The New Logon fields indicate the account for whom the new logon was created, i.e. the account that was logged on. The network fields indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impersonation level field indicates the extent to which a process in the logon session can impersonate. The authentication information fields provide detailed information about this specific logon request. - Logon GUID is a unique identifier that can be used to correlate this event with a KDC event. - Transited services indicate which intermediate services have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indicates the length of the generated session key. This will be 0 if no session key was requested.
Security	Audit Success	12544	2015-04-27 17:35:01	Microsoft-Windows-Security-Auditing	4648: A logon was attempted using explicit credentials. Subject: Security ID: S-1-5-18 Account Name: LTRANPHD$ Account Domain: WORKGROUP Logon ID: 0x3e7 Logon GUID: {00000000-0000-0000-0000-000000000000} Account Whose Credentials Were Used: Account Name: DWM-1 Account Domain: Window Manager Logon GUID: {00000000-0000-0000-0000-000000000000} Target Server: Target Server Name: localhost Additional Information: localhost Process Information: Process ID: 0x218 Process Name: C:\Windows\System32\winlogon.exe Network Information: Network Address: - Port: - This event is generated when a process attempts to log on an account by explicitly specifying that account's credentials. This most commonly occurs in batch-type configurations such as scheduled tasks, or when using the RUNAS command.
Security	Audit Success	12544	2015-04-27 17:35:01	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: LTRANPHD$ Account Domain: WORKGROUP Logon ID: 0x3e7 Logon Type: 2 Impersonation Level: %%1833 New Logon: Security ID: S-1-5-90-1 Account Name: DWM-1 Account Domain: Window Manager Logon ID: 0xd8ac Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x218 Process Name: C:\Windows\System32\winlogon.exe Network Information: Workstation Name: Source Network Address: - Source Port: - Detailed Authentication Information: Logon Process: Advapi Authentication Package: Negotiate Transited Services: - Package Name (NTLM only): - Key Length: 0 This event is generated when a logon session is created. It is generated on the computer that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service such as the Server service, or a local process such as Winlogon.exe or Services.exe. The logon type field indicates the kind of logon that occurred. The most common types are 2 (interactive) and 3 (network). The New Logon fields indicate the account for whom the new logon was created, i.e. the account that was logged on. The network fields indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impersonation level field indicates the extent to which a process in the logon session can impersonate. The authentication information fields provide detailed information about this specific logon request. - Logon GUID is a unique identifier that can be used to correlate this event with a KDC event. - Transited services indicate which intermediate services have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indicates the length of the generated session key. This will be 0 if no session key was requested.
Security	Audit Success	12544	2015-04-27 17:35:01	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: LTRANPHD$ Account Domain: WORKGROUP Logon ID: 0x3e7 Logon Type: 2 Impersonation Level: %%1833 New Logon: Security ID: S-1-5-90-1 Account Name: DWM-1 Account Domain: Window Manager Logon ID: 0xd8d9 Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x218 Process Name: C:\Windows\System32\winlogon.exe Network Information: Workstation Name: Source Network Address: - Source Port: - Detailed Authentication Information: Logon Process: Advapi Authentication Package: Negotiate Transited Services: - Package Name (NTLM only): - Key Length: 0 This event is generated when a logon session is created. It is generated on the computer that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service such as the Server service, or a local process such as Winlogon.exe or Services.exe. The logon type field indicates the kind of logon that occurred. The most common types are 2 (interactive) and 3 (network). The New Logon fields indicate the account for whom the new logon was created, i.e. the account that was logged on. The network fields indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impersonation level field indicates the extent to which a process in the logon session can impersonate. The authentication information fields provide detailed information about this specific logon request. - Logon GUID is a unique identifier that can be used to correlate this event with a KDC event. - Transited services indicate which intermediate services have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indicates the length of the generated session key. This will be 0 if no session key was requested.
Security	Audit	12544	2015-04-27	Microsoft-Windows-Security-	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: LTRANPHD$ Account Domain: WORKGROUP Logon ID: 0x3e7 Logon Type: 5 Impersonation Level: %%1833 New Logon: Security ID: S-1-5-19 Account Name: LOCAL SERVICE Account Domain: NT AUTHORITY Logon ID: 0x3e5 Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x238 Process Name: C:\Windows\System32\services.exe Network Information: Workstation Name: Source Network Address: - Source Port: - Detailed Authentication Information: Logon Process: Advapi Authentication Package: Negotiate Transited Services: - Package Name (NTLM only): - Key Length: 0 This event is generated when a logon session is created. It is generated on the computer that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service such as the Server service, or a local process such as Winlogon.exe or Services.exe. The logon type field indicates the kind of logon that occurred.

	Success		17:35:01	Auditing	The most common types are 2 (interactive) and 3 (network). The New Logon fields indicate the account for whom the new logon was created, i.e. the account that was logged on. The network fields indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impersonation level field indicates the extent to which a process in the logon session can impersonate. The authentication information fields provide detailed information about this specific logon request. - Logon GUID is a unique identifier that can be used to correlate this event with a KDC event. - Transited services indicate which intermediate services have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indicates the length of the generated session key. This will be 0 if no session key was requested.
Security	Audit Success	12544	2015-04-27 17:35:01	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: LTRANPHD$ Account Domain: WORKGROUP Logon ID: 0x3e7 Logon Type: 5 Impersonation Level: %%1833 New Logon: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Logon ID: 0x3e7 Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x238 Process Name: C:\Windows\System32\services.exe Network Information: Workstation Name: Source Network Address: - Source Port: - Detailed Authentication Information: Logon Process: Advapi Authentication Package: Negotiate Transited Services: - Package Name (NTLM only): - Key Length: 0 This event is generated when a logon session is created. It is generated on the computer that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service such as the Server service, or a local process such as Winlogon.exe or Services.exe. The logon type field indicates the kind of logon that occurred. The most common types are 2 (interactive) and 3 (network). The New Logon fields indicate the account for whom the new logon was created, i.e. the account that was logged on. The network fields indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impersonation level field indicates the extent to which a process in the logon session can impersonate. The authentication information fields provide detailed information about this specific logon request. - Logon GUID is a unique identifier that can be used to correlate this event with a KDC event. - Transited services indicate which intermediate services have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indicates the length of the generated session key. This will be 0 if no session key was requested.
Security	Audit Success	12544	2015-04-27 17:35:01	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: LTRANPHD$ Account Domain: WORKGROUP Logon ID: 0x3e7 Logon Type: 5 Impersonation Level: %%1833 New Logon: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Logon ID: 0x3e7 Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x238 Process Name: C:\Windows\System32\services.exe Network Information: Workstation Name: Source Network Address: - Source Port: - Detailed Authentication Information: Logon Process: Advapi Authentication Package: Negotiate Transited Services: - Package Name (NTLM only): - Key Length: 0 This event is generated when a logon session is created. It is generated on the computer that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service such as the Server service, or a local process such as Winlogon.exe or Services.exe. The logon type field indicates the kind of logon that occurred. The most common types are 2 (interactive) and 3 (network). The New Logon fields indicate the account for whom the new logon was created, i.e. the account that was logged on. The network fields indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impersonation level field indicates the extent to which a process in the logon session can impersonate. The authentication information fields provide detailed information about this specific logon request. - Logon GUID is a unique identifier that can be used to correlate this event with a KDC event. - Transited services indicate which intermediate services have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indicates the length of the generated session key. This will be 0 if no session key was requested.
Security	Audit Success	12548	2015-04-27 17:35:01	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Logon ID: 0x3e7 Privileges: SeAssignPrimaryTokenPrivilege SeTcbPrivilege SeSecurityPrivilege SeTakeOwnershipPrivilege SeLoadDriverPrivilege SeBackupPrivilege SeRestorePrivilege SeDebugPrivilege SeAuditPrivilege SeSystemEnvironmentPrivilege SeImpersonatePrivilege
Security	Audit Success	12548	2015-04-27 17:35:01	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-20 Account Name: NETWORK SERVICE Account Domain: NT AUTHORITY Logon ID: 0x3e4 Privileges: SeAssignPrimaryTokenPrivilege SeAuditPrivilege SeImpersonatePrivilege
Security	Audit Success	12548	2015-04-27 17:35:01	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-90-1 Account Name: DWM-1 Account Domain: Window Manager Logon ID: 0xd8ac Privileges: SeAssignPrimaryTokenPrivilege SeAuditPrivilege SeImpersonatePrivilege
Security	Audit Success	12548	2015-04-27 17:35:01	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-90-1 Account Name: DWM-1 Account Domain: Window Manager Logon ID: 0xd8d9 Privileges: SeAssignPrimaryTokenPrivilege SeAuditPrivilege
Security	Audit Success	12548	2015-04-27 17:35:01	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-19 Account Name: LOCAL SERVICE Account Domain: NT AUTHORITY Logon ID: 0x3e5 Privileges: SeAssignPrimaryTokenPrivilege SeAuditPrivilege SeImpersonatePrivilege
Security	Audit	12548	2015-04-27	Microsoft-Windows-Security-	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Logon ID: 0x3e7 Privileges: SeAssignPrimaryTokenPrivilege SeTcbPrivilege

	Success		17:35:01	Auditing	SeSecurityPrivilege SeTakeOwnershipPrivilege SeLoadDriverPrivilege SeBackupPrivilege SeRestorePrivilege SeDebugPrivilege SeAuditPrivilege SeSystemEnvironmentPrivilege SeImpersonatePrivilege
Security	Audit Success	12548	2015-04-27 17:35:01	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Logon ID: 0x3e7 Privileges: SeAssignPrimaryTokenPrivilege SeTcbPrivilege SeSecurityPrivilege SeTakeOwnershipPrivilege SeLoadDriverPrivilege SeBackupPrivilege SeRestorePrivilege SeDebugPrivilege SeAuditPrivilege SeSystemEnvironmentPrivilege SeImpersonatePrivilege
Security	Audit Success	13568	2015-04-27 17:35:01	Microsoft-Windows-Security-Auditing	4902: The Per-user audit policy table was created. Number of Elements: 0 Policy ID: 0xa054
Security	Audit Success	101	2015-04-27 17:35:02	Microsoft-Windows-Eventlog	1101: Audit events have been dropped by the transport. 0
Security	Audit Success	12292	2015-04-27 17:35:02	Microsoft-Windows-Security-Auditing	5033: The Windows Firewall Driver started successfully.
Security	Audit Success	12544	2015-04-27 17:35:02	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: LTRANPHD$ Account Domain: WORKGROUP Logon ID: 0x3e7 Logon Type: 5 Impersonation Level: %%1833 New Logon: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Logon ID: 0x3e7 Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x238 Process Name: C:\Windows\System32\services.exe Network Information: Workstation Name: Source Network Address: - Source Port: - Detailed Authentication Information: Logon Process: Advapi Authentication Package: Negotiate Transited Services: - Package Name (NTLM only): - Key Length: 0 This event is generated when a logon session is created. It is generated on the computer that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service such as the Server service, or a local process such as Winlogon.exe or Services.exe. The logon type field indicates the kind of logon that occurred. The most common types are 2 (interactive) and 3 (network). The New Logon fields indicate the account for whom the new logon was created, i.e. the account that was logged on. The network fields indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impersonation level field indicates the extent to which a process in the logon session can impersonate. The authentication information fields provide detailed information about this specific logon request. - Logon GUID is a unique identifier that can be used to correlate this event with a KDC event. - Transited services indicate which intermediate services have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indicates the length of the generated session key. This will be 0 if no session key was requested.
Security	Audit Success	12544	2015-04-27 17:35:02	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: LTRANPHD$ Account Domain: WORKGROUP Logon ID: 0x3e7 Logon Type: 5 Impersonation Level: %%1833 New Logon: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Logon ID: 0x3e7 Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x238 Process Name: C:\Windows\System32\services.exe Network Information: Workstation Name: Source Network Address: - Source Port: - Detailed Authentication Information: Logon Process: Advapi Authentication Package: Negotiate Transited Services: - Package Name (NTLM only): - Key Length: 0 This event is generated when a logon session is created. It is generated on the computer that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service such as the Server service, or a local process such as Winlogon.exe or Services.exe. The logon type field indicates the kind of logon that occurred. The most common types are 2 (interactive) and 3 (network). The New Logon fields indicate the account for whom the new logon was created, i.e. the account that was logged on. The network fields indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impersonation level field indicates the extent to which a process in the logon session can impersonate. The authentication information fields provide detailed information about this specific logon request. - Logon GUID is a unique identifier that can be used to correlate this event with a KDC event. - Transited services indicate which intermediate services have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indicates the length of the generated session key. This will be 0 if no session key was requested.
Security	Audit Success	12548	2015-04-27 17:35:02	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Logon ID: 0x3e7 Privileges: SeAssignPrimaryTokenPrivilege SeTcbPrivilege SeSecurityPrivilege SeTakeOwnershipPrivilege SeLoadDriverPrivilege SeBackupPrivilege SeRestorePrivilege SeDebugPrivilege SeAuditPrivilege SeSystemEnvironmentPrivilege SeImpersonatePrivilege
Security	Audit Success	12548	2015-04-27 17:35:02	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Logon ID: 0x3e7 Privileges: SeAssignPrimaryTokenPrivilege SeTcbPrivilege SeSecurityPrivilege SeTakeOwnershipPrivilege SeLoadDriverPrivilege SeBackupPrivilege SeRestorePrivilege SeDebugPrivilege SeAuditPrivilege SeSystemEnvironmentPrivilege SeImpersonatePrivilege
Security	Audit Success	12292	2015-04-27 17:35:03	Microsoft-Windows-Security-Auditing	5024: The Windows Firewall service started successfully.
					4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: LTRANPHD$

Security	Audit Success	12544	2015-04-27 17:35:03	Microsoft-Windows-Security-Auditing	Account Domain: WORKGROUP Logon ID: 0x3e7 Logon Type: 5 Impersonation Level: %%1833 New Logon: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Logon ID: 0x3e7 Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x238 Process Name: C:\Windows\System32\services.exe Network Information: Workstation Name: Source Network Address: - Source Port: - Detailed Authentication Information: Logon Process: Advapi Authentication Package: Negotiate Transited Services: - Package Name (NTLM only): - Key Length: 0 This event is generated when a logon session is created. It is generated on the computer that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service such as the Server service, or a local process such as Winlogon.exe or Services.exe. The logon type field indicates the kind of logon that occurred. The most common types are 2 (interactive) and 3 (network). The New Logon fields indicate the account for whom the new logon was created, i.e. the account that was logged on. The network fields indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impersonation level field indicates the extent to which a process in the logon session can impersonate. The authentication information fields provide detailed information about this specific logon request. - Logon GUID is a unique identifier that can be used to correlate this event with a KDC event. - Transited services indicate which intermediate services have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indicates the length of the generated session key. This will be 0 if no session key was requested.
Security	Audit Success	12544	2015-04-27 17:35:03	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-0-0 Account Name: - Account Domain: - Logon ID: 0x0 Logon Type: 3 Impersonation Level: %%1833 New Logon: Security ID: S-1-5-7 Account Name: ANONYMOUS LOGON Account Domain: NT AUTHORITY Logon ID: 0x1a182 Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x0 Process Name: - Network Information: Workstation Name: Source Network Address: - Source Port: - Detailed Authentication Information: Logon Process: NtLmSsp Authentication Package: NTLM Transited Services: - Package Name (NTLM only): NTLM V1 Key Length: 0 This event is generated when a logon session is created. It is generated on the computer that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service such as the Server service, or a local process such as Winlogon.exe or Services.exe. The logon type field indicates the kind of logon that occurred. The most common types are 2 (interactive) and 3 (network). The New Logon fields indicate the account for whom the new logon was created, i.e. the account that was logged on. The network fields indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impersonation level field indicates the extent to which a process in the logon session can impersonate. The authentication information fields provide detailed information about this specific logon request. - Logon GUID is a unique identifier that can be used to correlate this event with a KDC event. - Transited services indicate which intermediate services have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indicates the length of the generated session key. This will be 0 if no session key was requested.
Security	Audit Success	12548	2015-04-27 17:35:03	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Logon ID: 0x3e7 Privileges: SeAssignPrimaryTokenPrivilege SeTcbPrivilege SeSecurityPrivilege SeTakeOwnershipPrivilege SeLoadDriverPrivilege SeBackupPrivilege SeRestorePrivilege SeDebugPrivilege SeAuditPrivilege SeSystemEnvironmentPrivilege SeImpersonatePrivilege
Security	Audit Success	12544	2015-04-27 17:35:06	Microsoft-Windows-Security-Auditing	4648: A logon was attempted using explicit credentials. Subject: Security ID: S-1-5-18 Account Name: LTRANPHD$ Account Domain: WORKGROUP Logon ID: 0x3e7 Logon GUID: {00000000-0000-0000-0000-000000000000} Account Whose Credentials Were Used: Account Name: Liem Account Domain: LTRANPHD Logon GUID: {00000000-0000-0000-0000-000000000000} Target Server: Target Server Name: localhost Additional Information: localhost Process Information: Process ID: 0x218 Process Name: C:\Windows\System32\winlogon.exe Network Information: Network Address: 127.0.0.1 Port: 0 This event is generated when a process attempts to log on an account by explicitly specifying that account's credentials. This most commonly occurs in batch-type configurations such as scheduled tasks, or when using the RUNAS command.
Security	Audit Success	12544	2015-04-27 17:35:06	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: LTRANPHD$ Account Domain: WORKGROUP Logon ID: 0x3e7 Logon Type: 2 Impersonation Level: %%1833 New Logon: Security ID: S-1-5-21-1888849264-3803429180-4108621888-1001 Account Name: Liem Account Domain: LTRANPHD Logon ID: 0x1cbd5 Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x218 Process Name: C:\Windows\System32\winlogon.exe Network Information: Workstation Name: LTRANPHD Source Network Address: 127.0.0.1 Source Port: 0 Detailed Authentication Information: Logon Process: User32 Authentication Package: Negotiate Transited Services: - Package Name (NTLM only): - Key Length: 0 This event is generated when a logon session is created. It is generated on the computer that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service such as the Server service, or a local process such as Winlogon.exe or Services.exe. The logon type field indicates the kind of logon that occurred. The most common types are 2 (interactive) and 3 (network). The New Logon fields indicate the account for whom the new logon was created, i.e. the account that was logged on. The network fields indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impersonation level field indicates the extent to which a process in the logon session can impersonate. The authentication information fields provide detailed information about this specific logon request. - Logon GUID is a unique identifier that can be used to correlate this event with a KDC event. - Transited services indicate which intermediate services have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length

					indicates the length of the generated session key. This will be 0 if no session key was requested.
Security	Audit Success	12544	2015-04-27 17:35:06	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: LTRANPHD$ Account Domain: WORKGROUP Logon ID: 0x3e7 Logon Type: 2 Impersonation Level: %%1833 New Logon: Security ID: S-1-5-21-1888849264-3803429180-4108621888-1001 Account Name: Liem Account Domain: LTRANPHD Logon ID: 0x1cc08 Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x218 Process Name: C:\Windows\System32\winlogon.exe Network Information: Workstation Name: LTRANPHD Source Network Address: 127.0.0.1 Source Port: 0 Detailed Authentication Information: Logon Process: User32 Authentication Package: Negotiate Transited Services: - Package Name (NTLM only): - Key Length: 0 This event is generated when a logon session is created. It is generated on the computer that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service such as the Server service, or a local process such as Winlogon.exe or Services.exe. The logon type field indicates the kind of logon that occurred. The most common types are 2 (interactive) and 3 (network). The New Logon fields indicate the account for whom the new logon was created, i.e. the account that was logged on. The network fields indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impersonation level field indicates the extent to which a process in the logon session can impersonate. The authentication information fields provide detailed information about this specific logon request. - Logon GUID is a unique identifier that can be used to correlate this event with a KDC event. - Transited services indicate which intermediate services have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indicates the length of the generated session key. This will be 0 if no session key was requested.
Security	Audit Success	12548	2015-04-27 17:35:06	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-21-1888849264-3803429180-4108621888-1001 Account Name: Liem Account Domain: LTRANPHD Logon ID: 0x1cbd5 Privileges: SeSecurityPrivilege SeTakeOwnershipPrivilege SeLoadDriverPrivilege SeBackupPrivilege SeRestorePrivilege SeDebugPrivilege SeSystemEnvironmentPrivilege SeImpersonatePrivilege
Security	Audit Success	12544	2015-04-27 17:35:08	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: LTRANPHD$ Account Domain: WORKGROUP Logon ID: 0x3e7 Logon Type: 5 Impersonation Level: %%1833 New Logon: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Logon ID: 0x3e7 Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x238 Process Name: C:\Windows\System32\services.exe Network Information: Workstation Name: Source Network Address: - Source Port: - Detailed Authentication Information: Logon Process: Advapi Authentication Package: Negotiate Transited Services: - Package Name (NTLM only): - Key Length: 0 This event is generated when a logon session is created. It is generated on the computer that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service such as the Server service, or a local process such as Winlogon.exe or Services.exe. The logon type field indicates the kind of logon that occurred. The most common types are 2 (interactive) and 3 (network). The New Logon fields indicate the account for whom the new logon was created, i.e. the account that was logged on. The network fields indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impersonation level field indicates the extent to which a process in the logon session can impersonate. The authentication information fields provide detailed information about this specific logon request. - Logon GUID is a unique identifier that can be used to correlate this event with a KDC event. - Transited services indicate which intermediate services have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indicates the length of the generated session key. This will be 0 if no session key was requested.
Security	Audit Success	12548	2015-04-27 17:35:08	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Logon ID: 0x3e7 Privileges: SeAssignPrimaryTokenPrivilege SeTcbPrivilege SeSecurityPrivilege SeTakeOwnershipPrivilege SeLoadDriverPrivilege SeBackupPrivilege SeRestorePrivilege SeDebugPrivilege SeAuditPrivilege SeSystemEnvironmentPrivilege SeImpersonatePrivilege
Security	Audit Success	13824	2015-04-27 17:35:10	Microsoft-Windows-Security-Auditing	4797: An attempt was made to query the existence of a blank password for an account. Subject: Security ID: S-1-5-21-1888849264-3803429180-4108621888-1001 Account Name: Liem Account Domain: LTRANPHD Logon ID: 0x1cc08 Additional Information: Caller Workstation: LTRANPHD Target Account Name: Administrator Target Account Domain: LTRANPHD
Security	Audit Success	13824	2015-04-27 17:35:10	Microsoft-Windows-Security-Auditing	4797: An attempt was made to query the existence of a blank password for an account. Subject: Security ID: S-1-5-21-1888849264-3803429180-4108621888-1001 Account Name: Liem Account Domain: LTRANPHD Logon ID: 0x1cc08 Additional Information: Caller Workstation: LTRANPHD Target Account Name: Guest Target Account Domain: LTRANPHD
Security	Audit Success	13824	2015-04-27 17:35:10	Microsoft-Windows-Security-Auditing	4797: An attempt was made to query the existence of a blank password for an account. Subject: Security ID: S-1-5-21-1888849264-3803429180-4108621888-1001 Account Name: Liem Account Domain: LTRANPHD Logon ID: 0x1cc08 Additional Information: Caller Workstation: LTRANPHD Target Account Name: Administrator Target Account Domain: LTRANPHD
Security	Audit Success	13824	2015-04-27 17:35:10	Microsoft-Windows-Security-Auditing	4797: An attempt was made to query the existence of a blank password for an account. Subject: Security ID: S-1-5-21-1888849264-3803429180-4108621888-1001 Account Name: Liem Account Domain: LTRANPHD Logon ID: 0x1cc08 Additional Information: Caller Workstation: LTRANPHD Target Account Name: Guest Target Account Domain: LTRANPHD
Security	Audit	13824	2015-04-27	Microsoft-Windows-Security-	4797: An attempt was made to query the existence of a blank password for an account. Subject: Security ID: S-1-5-19 Account Name: LOCAL SERVICE Account Domain: NT AUTHORITY Logon ID: 0x3e5 Additional

	Success		17:35:12	Auditing	Information: Caller Workstation: LTRANPHD Target Account Name: Administrator Target Account Domain: LTRANPHD
Security	Audit Success	13824	2015-04-27 17:35:12	Microsoft-Windows-Security-Auditing	4797: An attempt was made to query the existence of a blank password for an account. Subject: Security ID: S-1-5-19 Account Name: LOCAL SERVICE Account Domain: NT AUTHORITY Logon ID: 0x3e5 Additional Information: Caller Workstation: LTRANPHD Target Account Name: Guest Target Account Domain: LTRANPHD
Security	Audit Success	13824	2015-04-27 17:35:12	Microsoft-Windows-Security-Auditing	4797: An attempt was made to query the existence of a blank password for an account. Subject: Security ID: S-1-5-19 Account Name: LOCAL SERVICE Account Domain: NT AUTHORITY Logon ID: 0x3e5 Additional Information: Caller Workstation: LTRANPHD Target Account Name: Liem Target Account Domain: LTRANPHD
Security	Audit Success	13824	2015-04-27 17:35:12	Microsoft-Windows-Security-Auditing	4797: An attempt was made to query the existence of a blank password for an account. Subject: Security ID: S-1-5-19 Account Name: LOCAL SERVICE Account Domain: NT AUTHORITY Logon ID: 0x3e5 Additional Information: Caller Workstation: LTRANPHD Target Account Name: Administrator Target Account Domain: LTRANPHD
Security	Audit Success	13824	2015-04-27 17:35:12	Microsoft-Windows-Security-Auditing	4797: An attempt was made to query the existence of a blank password for an account. Subject: Security ID: S-1-5-19 Account Name: LOCAL SERVICE Account Domain: NT AUTHORITY Logon ID: 0x3e5 Additional Information: Caller Workstation: LTRANPHD Target Account Name: Liem Target Account Domain: LTRANPHD
Security	Audit Success	13824	2015-04-27 17:35:12	Microsoft-Windows-Security-Auditing	4797: An attempt was made to query the existence of a blank password for an account. Subject: Security ID: S-1-5-19 Account Name: LOCAL SERVICE Account Domain: NT AUTHORITY Logon ID: 0x3e5 Additional Information: Caller Workstation: LTRANPHD Target Account Name: Guest Target Account Domain: LTRANPHD
Security	Audit Success	13824	2015-04-27 17:35:12	Microsoft-Windows-Security-Auditing	4797: An attempt was made to query the existence of a blank password for an account. Subject: Security ID: S-1-5-19 Account Name: LOCAL SERVICE Account Domain: NT AUTHORITY Logon ID: 0x3e5 Additional Information: Caller Workstation: LTRANPHD Target Account Name: Liem Target Account Domain: LTRANPHD
Security	Audit Success	13824	2015-04-27 17:35:12	Microsoft-Windows-Security-Auditing	4797: An attempt was made to query the existence of a blank password for an account. Subject: Security ID: S-1-5-19 Account Name: LOCAL SERVICE Account Domain: NT AUTHORITY Logon ID: 0x3e5 Additional Information: Caller Workstation: LTRANPHD Target Account Name: Liem Target Account Domain: LTRANPHD
Security	Audit Success	12544	2015-04-27 18:02:00	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: LTRANPHD$ Account Domain: WORKGROUP Logon ID: 0x3e7 Logon Type: 5 Impersonation Level: %%1833 New Logon: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Logon ID: 0x3e7 Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x238 Process Name: C:\Windows\System32\services.exe Network Information: Workstation Name: Source Network Address: - Source Port: - Detailed Authentication Information: Logon Process: Advapi Authentication Package: Negotiate Transited Services: - Package Name (NTLM only): - Key Length: 0 This event is generated when a logon session is created. It is generated on the computer that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service such as the Server service, or a local process such as Winlogon.exe or Services.exe. The logon type field indicates the kind of logon that occurred. The most common types are 2 (interactive) and 3 (network). The New Logon fields indicate the account for whom the new logon was created, i.e. the account that was logged on. The network fields indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impersonation level field indicates the extent to which a process in the logon session can impersonate. The authentication information fields provide detailed information about this specific logon request. - Logon GUID is a unique identifier that can be used to correlate this event with a KDC event. - Transited services indicate which intermediate services have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indicates the length of the generated session key. This will be 0 if no session key was requested.
Security	Audit Success	12548	2015-04-27 18:02:00	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Logon ID: 0x3e7 Privileges: SeAssignPrimaryTokenPrivilege SeTcbPrivilege SeSecurityPrivilege SeTakeOwnershipPrivilege SeLoadDriverPrivilege SeBackupPrivilege SeRestorePrivilege SeDebugPrivilege SeAuditPrivilege SeSystemEnvironmentPrivilege SeImpersonatePrivilege
Security	Audit Success	12544	2015-04-27 18:02:01	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: LTRANPHD$ Account Domain: WORKGROUP Logon ID: 0x3e7 Logon Type: 5 Impersonation Level: %%1833 New Logon: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Logon ID: 0x3e7 Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x238 Process Name: C:\Windows\System32\services.exe Network Information: Workstation Name: Source Network Address: - Source Port: - Detailed Authentication Information: Logon Process: Advapi Authentication Package: Negotiate Transited Services: - Package Name (NTLM only): - Key Length: 0 This event is generated when a logon session is created. It is generated on the computer that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service such as the Server service, or a local process such as Winlogon.exe or Services.exe. The logon type field indicates the kind of logon that occurred. The most common types are 2 (interactive) and 3 (network). The New Logon fields indicate the account for whom the new logon was created, i.e. the account that was logged on. The network fields indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impersonation level field indicates the extent to which a process in the logon session can impersonate. The authentication information fields provide detailed information about this specific logon request. - Logon GUID is a unique identifier that can be used to correlate this event with a KDC event. - Transited services indicate which intermediate services have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indicates the length of the generated

					session key. This will be 0 if no session key was requested.
Security	Audit Success	12548	2015-04-27 18:02:01	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Logon ID: 0x3e7 Privileges: SeAssignPrimaryTokenPrivilege SeTcbPrivilege SeSecurityPrivilege SeTakeOwnershipPrivilege SeLoadDriverPrivilege SeBackupPrivilege SeRestorePrivilege SeDebugPrivilege SeAuditPrivilege SeSystemEnvironmentPrivilege SeImpersonatePrivilege
Security	Audit Success	12288	2015-04-27 18:02:19	Microsoft-Windows-Security-Auditing	4616: The system time was changed. Subject: Security ID: S-1-5-19 Account Name: LOCAL SERVICE Account Domain: NT AUTHORITY Logon ID: 0x3e5 Process Information: Process ID: 0x3d8 Name: C:\Windows\System32\svchost.exe Previous Time: 2015-04-28T01:02:19.036091600Z New Time: 2015-04-28T01:02:19.035000000Z This event is generated when the system time is changed. It is normal for the Windows Time Service, which runs with System privilege, to change the system time on a regular basis. Other system time changes may be indicative of attempts to tamper with the computer.
Security	Audit Success	12288	2015-04-27 18:32:23	Microsoft-Windows-Security-Auditing	4608: Windows is starting up. This event is logged when LSASS.EXE starts and the auditing subsystem is initialized.
Security	Audit Success	12544	2015-04-27 18:32:23	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-0-0 Account Name: - Account Domain: - Logon ID: 0x0 Logon Type: 0 Impersonation Level: - New Logon: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Logon ID: 0x3e7 Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x4 Process Name: Network Information: Workstation Name: - Source Network Address: - Source Port: - Detailed Authentication Information: Logon Process: - Authentication Package: - Transited Services: - Package Name (NTLM only): - Key Length: 0 This event is generated when a logon session is created. It is generated on the computer that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service such as the Server service, or a local process such as Winlogon.exe or Services.exe. The logon type field indicates the kind of logon that occurred. The most common types are 2 (interactive) and 3 (network). The New Logon fields indicate the account for whom the new logon was created, i.e. the account that was logged on. The network fields indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impersonation level field indicates the extent to which a process in the logon session can impersonate. The authentication information fields provide detailed information about this specific logon request. - Logon GUID is a unique identifier that can be used to correlate this event with a KDC event. - Transited services indicate which intermediate services have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indicates the length of the generated session key. This will be 0 if no session key was requested.
Security	Audit Success	12544	2015-04-27 18:32:23	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: LTRANPHD$ Account Domain: WORKGROUP Logon ID: 0x3e7 Logon Type: 5 Impersonation Level: %%1833 New Logon: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Logon ID: 0x3e7 Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x230 Process Name: C:\Windows\System32\services.exe Network Information: Workstation Name: Source Network Address: - Source Port: - Detailed Authentication Information: Logon Process: Advapi Authentication Package: Negotiate Transited Services: - Package Name (NTLM only): - Key Length: 0 This event is generated when a logon session is created. It is generated on the computer that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service such as the Server service, or a local process such as Winlogon.exe or Services.exe. The logon type field indicates the kind of logon that occurred. The most common types are 2 (interactive) and 3 (network). The New Logon fields indicate the account for whom the new logon was created, i.e. the account that was logged on. The network fields indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impersonation level field indicates the extent to which a process in the logon session can impersonate. The authentication information fields provide detailed information about this specific logon request. - Logon GUID is a unique identifier that can be used to correlate this event with a KDC event. - Transited services indicate which intermediate services have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indicates the length of the generated session key. This will be 0 if no session key was requested.
Security	Audit Success	12544	2015-04-27 18:32:23	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: LTRANPHD$ Account Domain: WORKGROUP Logon ID: 0x3e7 Logon Type: 5 Impersonation Level: %%1833 New Logon: Security ID: S-1-5-20 Account Name: NETWORK SERVICE Account Domain: NT AUTHORITY Logon ID: 0x3e4 Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x230 Process Name: C:\Windows\System32\services.exe Network Information: Workstation Name: Source Network Address: - Source Port: - Detailed Authentication Information: Logon Process: Advapi Authentication Package: Negotiate Transited Services: - Package Name (NTLM only): - Key Length: 0 This event is generated when a logon session is created. It is generated on the computer that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service such as the Server service, or a local process such as Winlogon.exe or Services.exe. The logon type field indicates the kind of logon that occurred. The most common types are 2 (interactive) and 3 (network). The New Logon fields indicate the account for whom the new logon was created, i.e. the account that was logged on. The network fields indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impersonation level field indicates the extent to which a process in the logon session can impersonate. The authentication information fields provide detailed information about this specific logon request.

					- Logon GUID is a unique identifier that can be used to correlate this event with a KDC event. - Transited services indicate which intermediate services have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indicates the length of the generated session key. This will be 0 if no session key was requested.
Security	Audit Success	12544	2015-04-27 18:32:23	Microsoft-Windows-Security-Auditing	4648: A logon was attempted using explicit credentials. Subject: Security ID: S-1-5-18 Account Name: LTRANPHD$ Account Domain: WORKGROUP Logon ID: 0x3e7 Logon GUID: {00000000-0000-0000-0000-000000000000} Account Whose Credentials Were Used: Account Name: DWM-1 Account Domain: Window Manager Logon GUID: {00000000-0000-0000-0000-000000000000} Target Server: Target Server Name: localhost Additional Information: localhost Process Information: Process ID: 0x208 Process Name: C:\Windows\System32\winlogon.exe Network Information: Network Address: - Port: - This event is generated when a process attempts to log on an account by explicitly specifying that account's credentials. This most commonly occurs in batch-type configurations such as scheduled tasks, or when using the RUNAS command.
Security	Audit Success	12544	2015-04-27 18:32:23	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: LTRANPHD$ Account Domain: WORKGROUP Logon ID: 0x3e7 Logon Type: 2 Impersonation Level: %%1833 New Logon: Security ID: S-1-5-90-1 Account Name: DWM-1 Account Domain: Window Manager Logon ID: 0xdbb4 Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x208 Process Name: C:\Windows\System32\winlogon.exe Network Information: Workstation Name: Source Network Address: - Source Port: - Detailed Authentication Information: Logon Process: Advapi Authentication Package: Negotiate Transited Services: - Package Name (NTLM only): - Key Length: 0 This event is generated when a logon session is created. It is generated on the computer that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service such as the Server service, or a local process such as Winlogon.exe or Services.exe. The logon type field indicates the kind of logon that occurred. The most common types are 2 (interactive) and 3 (network). The New Logon fields indicate the account for whom the new logon was created, i.e. the account that was logged on. The network fields indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impersonation level field indicates the extent to which a process in the logon session can impersonate. The authentication information fields provide detailed information about this specific logon request. - Logon GUID is a unique identifier that can be used to correlate this event with a KDC event. - Transited services indicate which intermediate services have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indicates the length of the generated session key. This will be 0 if no session key was requested.
Security	Audit Success	12544	2015-04-27 18:32:23	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: LTRANPHD$ Account Domain: WORKGROUP Logon ID: 0x3e7 Logon Type: 2 Impersonation Level: %%1833 New Logon: Security ID: S-1-5-90-1 Account Name: DWM-1 Account Domain: Window Manager Logon ID: 0xdbc6 Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x208 Process Name: C:\Windows\System32\winlogon.exe Network Information: Workstation Name: Source Network Address: - Source Port: - Detailed Authentication Information: Logon Process: Advapi Authentication Package: Negotiate Transited Services: - Package Name (NTLM only): - Key Length: 0 This event is generated when a logon session is created. It is generated on the computer that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service such as the Server service, or a local process such as Winlogon.exe or Services.exe. The logon type field indicates the kind of logon that occurred. The most common types are 2 (interactive) and 3 (network). The New Logon fields indicate the account for whom the new logon was created, i.e. the account that was logged on. The network fields indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impersonation level field indicates the extent to which a process in the logon session can impersonate. The authentication information fields provide detailed information about this specific logon request. - Logon GUID is a unique identifier that can be used to correlate this event with a KDC event. - Transited services indicate which intermediate services have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indicates the length of the generated session key. This will be 0 if no session key was requested.
Security	Audit Success	12544	2015-04-27 18:32:23	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: LTRANPHD$ Account Domain: WORKGROUP Logon ID: 0x3e7 Logon Type: 5 Impersonation Level: %%1833 New Logon: Security ID: S-1-5-19 Account Name: LOCAL SERVICE Account Domain: NT AUTHORITY Logon ID: 0x3e5 Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x230 Process Name: C:\Windows\System32\services.exe Network Information: Workstation Name: Source Network Address: - Source Port: - Detailed Authentication Information: Logon Process: Advapi Authentication Package: Negotiate Transited Services: - Package Name (NTLM only): - Key Length: 0 This event is generated when a logon session is created. It is generated on the computer that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service such as the Server service, or a local process such as Winlogon.exe or Services.exe. The logon type field indicates the kind of logon that occurred. The most common types are 2 (interactive) and 3 (network). The New Logon fields indicate the account for whom the new logon was created, i.e. the account that was logged on. The network fields indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impersonation level field indicates the extent to which a process in the logon session can impersonate. The authentication information fields provide detailed information about this specific logon request. - Logon GUID is a unique identifier that can be used to correlate this event with a KDC event. - Transited services indicate which intermediate services have participated in this logon request. - Package name indicates

					which sub-protocol was used among the NTLM protocols. - Key length indicates the length of the generated session key. This will be 0 if no session key was requested.
Security	Audit Success	12544	2015-04-27 18:32:23	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: LTRANPHD$ Account Domain: WORKGROUP Logon ID: 0x3e7 Logon Type: 5 Impersonation Level: %%1833 New Logon: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Logon ID: 0x3e7 Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x230 Process Name: C:\Windows\System32\services.exe Network Information: Workstation Name: Source Network Address: - Source Port: - Detailed Authentication Information: Logon Process: Advapi Authentication Package: Negotiate Transited Services: - Package Name (NTLM only): - Key Length: 0 This event is generated when a logon session is created. It is generated on the computer that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service such as the Server service, or a local process such as Winlogon.exe or Services.exe. The logon type field indicates the kind of logon that occurred. The most common types are 2 (interactive) and 3 (network). The New Logon fields indicate the account for whom the new logon was created, i.e. the account that was logged on. The network fields indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impersonation level field indicates the extent to which a process in the logon session can impersonate. The authentication information fields provide detailed information about this specific logon request. - Logon GUID is a unique identifier that can be used to correlate this event with a KDC event. - Transited services indicate which intermediate services have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indicates the length of the generated session key. This will be 0 if no session key was requested.
Security	Audit Success	12544	2015-04-27 18:32:23	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: LTRANPHD$ Account Domain: WORKGROUP Logon ID: 0x3e7 Logon Type: 5 Impersonation Level: %%1833 New Logon: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Logon ID: 0x3e7 Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x230 Process Name: C:\Windows\System32\services.exe Network Information: Workstation Name: Source Network Address: - Source Port: - Detailed Authentication Information: Logon Process: Advapi Authentication Package: Negotiate Transited Services: - Package Name (NTLM only): - Key Length: 0 This event is generated when a logon session is created. It is generated on the computer that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service such as the Server service, or a local process such as Winlogon.exe or Services.exe. The logon type field indicates the kind of logon that occurred. The most common types are 2 (interactive) and 3 (network). The New Logon fields indicate the account for whom the new logon was created, i.e. the account that was logged on. The network fields indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impersonation level field indicates the extent to which a process in the logon session can impersonate. The authentication information fields provide detailed information about this specific logon request. - Logon GUID is a unique identifier that can be used to correlate this event with a KDC event. - Transited services indicate which intermediate services have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indicates the length of the generated session key. This will be 0 if no session key was requested.
Security	Audit Success	12548	2015-04-27 18:32:23	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Logon ID: 0x3e7 Privileges: SeAssignPrimaryTokenPrivilege SeTcbPrivilege SeSecurityPrivilege SeTakeOwnershipPrivilege SeLoadDriverPrivilege SeBackupPrivilege SeRestorePrivilege SeDebugPrivilege SeAuditPrivilege SeSystemEnvironmentPrivilege SeImpersonatePrivilege
Security	Audit Success	12548	2015-04-27 18:32:23	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-20 Account Name: NETWORK SERVICE Account Domain: NT AUTHORITY Logon ID: 0x3e4 Privileges: SeAssignPrimaryTokenPrivilege SeAuditPrivilege SeImpersonatePrivilege
Security	Audit Success	12548	2015-04-27 18:32:23	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-90-1 Account Name: DWM-1 Account Domain: Window Manager Logon ID: 0xdbb4 Privileges: SeAssignPrimaryTokenPrivilege SeAuditPrivilege SeImpersonatePrivilege
Security	Audit Success	12548	2015-04-27 18:32:23	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-90-1 Account Name: DWM-1 Account Domain: Window Manager Logon ID: 0xdbc6 Privileges: SeAssignPrimaryTokenPrivilege SeAuditPrivilege
Security	Audit Success	12548	2015-04-27 18:32:23	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-19 Account Name: LOCAL SERVICE Account Domain: NT AUTHORITY Logon ID: 0x3e5 Privileges: SeAssignPrimaryTokenPrivilege SeAuditPrivilege SeImpersonatePrivilege
Security	Audit Success	12548	2015-04-27 18:32:23	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Logon ID: 0x3e7 Privileges: SeAssignPrimaryTokenPrivilege SeTcbPrivilege SeSecurityPrivilege SeTakeOwnershipPrivilege SeLoadDriverPrivilege SeBackupPrivilege SeRestorePrivilege SeDebugPrivilege SeAuditPrivilege SeSystemEnvironmentPrivilege SeImpersonatePrivilege
Security	Audit Success	12548	2015-04-27 18:32:23	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Logon ID: 0x3e7 Privileges: SeAssignPrimaryTokenPrivilege SeTcbPrivilege SeSecurityPrivilege SeTakeOwnershipPrivilege SeLoadDriverPrivilege SeBackupPrivilege SeRestorePrivilege SeDebugPrivilege SeAuditPrivilege SeSystemEnvironmentPrivilege SeImpersonatePrivilege
	Audit		2015-04-	Microsoft-Windows-Security-	

Security	Success	13568	27 18:32:23	Auditing	4902: The Per-user audit policy table was created. Number of Elements: 0 Policy ID: 0x8cf2
Security	Audit Success	101	2015-04-27 18:32:24	Microsoft-Windows-Eventlog	1101: Audit events have been dropped by the transport. 0
Security	Audit Success	12292	2015-04-27 18:32:25	Microsoft-Windows-Security-Auditing	5033: The Windows Firewall Driver started successfully.
Security	Audit Success	12292	2015-04-27 18:32:25	Microsoft-Windows-Security-Auditing	5024: The Windows Firewall service started successfully.
Security	Audit Success	12544	2015-04-27 18:32:25	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: LTRANPHD$ Account Domain: WORKGROUP Logon ID: 0x3e7 Logon Type: 5 Impersonation Level: %%1833 New Logon: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Logon ID: 0x3e7 Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x230 Process Name: C:\Windows\System32\services.exe Network Information: Workstation Name: Source Network Address: - Source Port: - Detailed Authentication Information: Logon Process: Advapi Authentication Package: Negotiate Transited Services: - Package Name (NTLM only): - Key Length: 0 This event is generated when a logon session is created. It is generated on the computer that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service such as the Server service, or a local process such as Winlogon.exe or Services.exe. The logon type field indicates the kind of logon that occurred. The most common types are 2 (interactive) and 3 (network). The New Logon fields indicate the account for whom the new logon was created, i.e. the account that was logged on. The network fields indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impersonation level field indicates the extent to which a process in the logon session can impersonate. The authentication information fields provide detailed information about this specific logon request. - Logon GUID is a unique identifier that can be used to correlate this event with a KDC event. - Transited services indicate which intermediate services have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indicates the length of the generated session key. This will be 0 if no session key was requested.
Security	Audit Success	12544	2015-04-27 18:32:25	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: LTRANPHD$ Account Domain: WORKGROUP Logon ID: 0x3e7 Logon Type: 5 Impersonation Level: %%1833 New Logon: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Logon ID: 0x3e7 Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x230 Process Name: C:\Windows\System32\services.exe Network Information: Workstation Name: Source Network Address: - Source Port: - Detailed Authentication Information: Logon Process: Advapi Authentication Package: Negotiate Transited Services: - Package Name (NTLM only): - Key Length: 0 This event is generated when a logon session is created. It is generated on the computer that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service such as the Server service, or a local process such as Winlogon.exe or Services.exe. The logon type field indicates the kind of logon that occurred. The most common types are 2 (interactive) and 3 (network). The New Logon fields indicate the account for whom the new logon was created, i.e. the account that was logged on. The network fields indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impersonation level field indicates the extent to which a process in the logon session can impersonate. The authentication information fields provide detailed information about this specific logon request. - Logon GUID is a unique identifier that can be used to correlate this event with a KDC event. - Transited services indicate which intermediate services have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indicates the length of the generated session key. This will be 0 if no session key was requested.
Security	Audit Success	12544	2015-04-27 18:32:25	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: LTRANPHD$ Account Domain: WORKGROUP Logon ID: 0x3e7 Logon Type: 5 Impersonation Level: %%1833 New Logon: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Logon ID: 0x3e7 Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x230 Process Name: C:\Windows\System32\services.exe Network Information: Workstation Name: Source Network Address: - Source Port: - Detailed Authentication Information: Logon Process: Advapi Authentication Package: Negotiate Transited Services: - Package Name (NTLM only): - Key Length: 0 This event is generated when a logon session is created. It is generated on the computer that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service such as the Server service, or a local process such as Winlogon.exe or Services.exe. The logon type field indicates the kind of logon that occurred. The most common types are 2 (interactive) and 3 (network). The New Logon fields indicate the account for whom the new logon was created, i.e. the account that was logged on. The network fields indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impersonation level field indicates the extent to which a process in the logon session can impersonate. The authentication information fields provide detailed information about this specific logon request. - Logon GUID is a unique identifier that can be used to correlate this event with a KDC event. - Transited services indicate which intermediate services have participated in this logon request. - Package name indicates

					which sub-protocol was used among the NTLM protocols. - Key length indicates the length of the generated session key. This will be 0 if no session key was requested.
Security	Audit Success	12544	2015-04-27 18:32:25	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-0-0 Account Name: - Account Domain: - Logon ID: 0x0 Logon Type: 3 Impersonation Level: %%1833 New Logon: Security ID: S-1-5-7 Account Name: ANONYMOUS LOGON Account Domain: NT AUTHORITY Logon ID: 0x192ee Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x0 Process Name: - Network Information: Workstation Name: Source Network Address: - Source Port: - Detailed Authentication Information: Logon Process: NtLmSsp Authentication Package: NTLM Transited Services: - Package Name (NTLM only): NTLM V1 Key Length: 0 This event is generated when a logon session is created. It is generated on the computer that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service such as the Server service, or a local process such as Winlogon.exe or Services.exe. The logon type field indicates the kind of logon that occurred. The most common types are 2 (interactive) and 3 (network). The New Logon fields indicate the account for whom the new logon was created, i.e. the account that was logged on. The network fields indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impersonation level field indicates the extent to which a process in the logon session can impersonate. The authentication information fields provide detailed information about this specific logon request. - Logon GUID is a unique identifier that can be used to correlate this event with a KDC event. - Transited services indicate which intermediate services have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indicates the length of the generated session key. This will be 0 if no session key was requested.
Security	Audit Success	12548	2015-04-27 18:32:25	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Logon ID: 0x3e7 Privileges: SeAssignPrimaryTokenPrivilege SeTcbPrivilege SeSecurityPrivilege SeTakeOwnershipPrivilege SeLoadDriverPrivilege SeBackupPrivilege SeRestorePrivilege SeDebugPrivilege SeAuditPrivilege SeSystemEnvironmentPrivilege SeImpersonatePrivilege
Security	Audit Success	12548	2015-04-27 18:32:25	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Logon ID: 0x3e7 Privileges: SeAssignPrimaryTokenPrivilege SeTcbPrivilege SeSecurityPrivilege SeTakeOwnershipPrivilege SeLoadDriverPrivilege SeBackupPrivilege SeRestorePrivilege SeDebugPrivilege SeAuditPrivilege SeSystemEnvironmentPrivilege SeImpersonatePrivilege
Security	Audit Success	12548	2015-04-27 18:32:25	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Logon ID: 0x3e7 Privileges: SeAssignPrimaryTokenPrivilege SeTcbPrivilege SeSecurityPrivilege SeTakeOwnershipPrivilege SeLoadDriverPrivilege SeBackupPrivilege SeRestorePrivilege SeDebugPrivilege SeAuditPrivilege SeSystemEnvironmentPrivilege SeImpersonatePrivilege
Security	Audit Success	12544	2015-04-27 18:32:27	Microsoft-Windows-Security-Auditing	4648: A logon was attempted using explicit credentials. Subject: Security ID: S-1-5-18 Account Name: LTRANPHD$ Account Domain: WORKGROUP Logon ID: 0x3e7 Logon GUID: {00000000-0000-0000-0000-000000000000} Account Whose Credentials Were Used: Account Name: Liem Account Domain: LTRANPHD Logon GUID: {00000000-0000-0000-0000-000000000000} Target Server: Target Server Name: localhost Additional Information: localhost Process Information: Process ID: 0x208 Process Name: C:\Windows\System32\winlogon.exe Network Information: Network Address: 127.0.0.1 Port: 0 This event is generated when a process attempts to log on an account by explicitly specifying that account's credentials. This most commonly occurs in batch-type configurations such as scheduled tasks, or when using the RUNAS command.
Security	Audit Success	12544	2015-04-27 18:32:27	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: LTRANPHD$ Account Domain: WORKGROUP Logon ID: 0x3e7 Logon Type: 2 Impersonation Level: %%1833 New Logon: Security ID: S-1-5-21-1888849264-3803429180-4108621888-1001 Account Name: Liem Account Domain: LTRANPHD Logon ID: 0x1acd0 Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x208 Process Name: C:\Windows\System32\winlogon.exe Network Information: Workstation Name: LTRANPHD Source Network Address: 127.0.0.1 Source Port: 0 Detailed Authentication Information: Logon Process: User32 Authentication Package: Negotiate Transited Services: - Package Name (NTLM only): - Key Length: 0 This event is generated when a logon session is created. It is generated on the computer that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service such as the Server service, or a local process such as Winlogon.exe or Services.exe. The logon type field indicates the kind of logon that occurred. The most common types are 2 (interactive) and 3 (network). The New Logon fields indicate the account for whom the new logon was created, i.e. the account that was logged on. The network fields indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impersonation level field indicates the extent to which a process in the logon session can impersonate. The authentication information fields provide detailed information about this specific logon request. - Logon GUID is a unique identifier that can be used to correlate this event with a KDC event. - Transited services indicate which intermediate services have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indicates the length of the generated session key. This will be 0 if no session key was requested.
					4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: LTRANPHD$ Account Domain: WORKGROUP Logon ID: 0x3e7 Logon Type: 2 Impersonation Level: %%1833 New Logon: Security ID: S-1-5-21-1888849264-3803429180-4108621888-1001 Account Name: Liem Account Domain: LTRANPHD Logon ID: 0x1acff Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x208 Process Name: C:\Windows\System32\winlogon.exe Network Information: Workstation Name: LTRANPHD Source Network Address: 127.0.0.1 Source Port: 0 Detailed Authentication Information:

Security	Audit Success	12544	2015-04-27 18:32:27	Microsoft-Windows-Security-Auditing	Logon Process: User32 Authentication Package: Negotiate Transited Services: - Package Name (NTLM only): - Key Length: 0 This event is generated when a logon session is created. It is generated on the computer that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service such as the Server service, or a local process such as Winlogon.exe or Services.exe. The logon type field indicates the kind of logon that occurred. The most common types are 2 (interactive) and 3 (network). The New Logon fields indicate the account for whom the new logon was created, i.e. the account that was logged on. The network fields indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impersonation level field indicates the extent to which a process in the logon session can impersonate. The authentication information fields provide detailed information about this specific logon request. - Logon GUID is a unique identifier that can be used to correlate this event with a KDC event. - Transited services indicate which intermediate services have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indicates the length of the generated session key. This will be 0 if no session key was requested.
Security	Audit Success	12548	2015-04-27 18:32:27	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-21-1888849264-3803429180-4108621888-1001 Account Name: Liem Account Domain: LTRANPHD Logon ID: 0x1acd0 Privileges: SeSecurityPrivilege SeTakeOwnershipPrivilege SeLoadDriverPrivilege SeBackupPrivilege SeRestorePrivilege SeDebugPrivilege SeSystemEnvironmentPrivilege SeImpersonatePrivilege
Security	Audit Success	12544	2015-04-27 18:32:28	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: LTRANPHD$ Account Domain: WORKGROUP Logon ID: 0x3e7 Logon Type: 5 Impersonation Level: %%1833 New Logon: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Logon ID: 0x3e7 Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x230 Process Name: C:\Windows\System32\services.exe Network Information: Workstation Name: Source Network Address: - Source Port: - Detailed Authentication Information: Logon Process: Advapi Authentication Package: Negotiate Transited Services: - Package Name (NTLM only): - Key Length: 0 This event is generated when a logon session is created. It is generated on the computer that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service such as the Server service, or a local process such as Winlogon.exe or Services.exe. The logon type field indicates the kind of logon that occurred. The most common types are 2 (interactive) and 3 (network). The New Logon fields indicate the account for whom the new logon was created, i.e. the account that was logged on. The network fields indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impersonation level field indicates the extent to which a process in the logon session can impersonate. The authentication information fields provide detailed information about this specific logon request. - Logon GUID is a unique identifier that can be used to correlate this event with a KDC event. - Transited services indicate which intermediate services have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indicates the length of the generated session key. This will be 0 if no session key was requested.
Security	Audit Success	12548	2015-04-27 18:32:28	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Logon ID: 0x3e7 Privileges: SeAssignPrimaryTokenPrivilege SeTcbPrivilege SeSecurityPrivilege SeTakeOwnershipPrivilege SeLoadDriverPrivilege SeBackupPrivilege SeRestorePrivilege SeDebugPrivilege SeAuditPrivilege SeSystemEnvironmentPrivilege SeImpersonatePrivilege
Security	Audit Success	13824	2015-04-27 18:32:29	Microsoft-Windows-Security-Auditing	4797: An attempt was made to query the existence of a blank password for an account. Subject: Security ID: S-1-5-21-1888849264-3803429180-4108621888-1001 Account Name: Liem Account Domain: LTRANPHD Logon ID: 0x1acff Additional Information: Caller Workstation: LTRANPHD Target Account Name: Administrator Target Account Domain: LTRANPHD
Security	Audit Success	13824	2015-04-27 18:32:29	Microsoft-Windows-Security-Auditing	4797: An attempt was made to query the existence of a blank password for an account. Subject: Security ID: S-1-5-21-1888849264-3803429180-4108621888-1001 Account Name: Liem Account Domain: LTRANPHD Logon ID: 0x1acff Additional Information: Caller Workstation: LTRANPHD Target Account Name: Guest Target Account Domain: LTRANPHD
Security	Audit Success	13824	2015-04-27 18:32:29	Microsoft-Windows-Security-Auditing	4797: An attempt was made to query the existence of a blank password for an account. Subject: Security ID: S-1-5-21-1888849264-3803429180-4108621888-1001 Account Name: Liem Account Domain: LTRANPHD Logon ID: 0x1acff Additional Information: Caller Workstation: LTRANPHD Target Account Name: Administrator Target Account Domain: LTRANPHD
Security	Audit Success	13824	2015-04-27 18:32:29	Microsoft-Windows-Security-Auditing	4797: An attempt was made to query the existence of a blank password for an account. Subject: Security ID: S-1-5-21-1888849264-3803429180-4108621888-1001 Account Name: Liem Account Domain: LTRANPHD Logon ID: 0x1acff Additional Information: Caller Workstation: LTRANPHD Target Account Name: Guest Target Account Domain: LTRANPHD
Security	Audit Success	13824	2015-04-27 18:32:32	Microsoft-Windows-Security-Auditing	4797: An attempt was made to query the existence of a blank password for an account. Subject: Security ID: S-1-5-19 Account Name: LOCAL SERVICE Account Domain: NT AUTHORITY Logon ID: 0x3e5 Additional Information: Caller Workstation: LTRANPHD Target Account Name: Administrator Target Account Domain: LTRANPHD
Security	Audit Success	13824	2015-04-27 18:32:32	Microsoft-Windows-Security-Auditing	4797: An attempt was made to query the existence of a blank password for an account. Subject: Security ID: S-1-5-19 Account Name: LOCAL SERVICE Account Domain: NT AUTHORITY Logon ID: 0x3e5 Additional Information: Caller Workstation: LTRANPHD Target Account Name: Administrator Target Account Domain: LTRANPHD
	Audit		2015-04-	Microsoft-Windows-Security-	4797: An attempt was made to query the existence of a blank password for an account. Subject: Security ID:

Security	Success	13824	27 18:32:32	Auditing	S-1-5-19 Account Name: LOCAL SERVICE Account Domain: NT AUTHORITY Logon ID: 0x3e5 Additional Information: Caller Workstation: LTRANPHD Target Account Name: Guest Target Account Domain: LTRANPHD
Security	Audit Success	13824	2015-04-27 18:32:32	Microsoft-Windows-Security-Auditing	4797: An attempt was made to query the existence of a blank password for an account. Subject: Security ID: S-1-5-19 Account Name: LOCAL SERVICE Account Domain: NT AUTHORITY Logon ID: 0x3e5 Additional Information: Caller Workstation: LTRANPHD Target Account Name: Guest Target Account Domain: LTRANPHD
Security	Audit Success	13824	2015-04-27 18:32:32	Microsoft-Windows-Security-Auditing	4797: An attempt was made to query the existence of a blank password for an account. Subject: Security ID: S-1-5-19 Account Name: LOCAL SERVICE Account Domain: NT AUTHORITY Logon ID: 0x3e5 Additional Information: Caller Workstation: LTRANPHD Target Account Name: Liem Target Account Domain: LTRANPHD
Security	Audit Success	13824	2015-04-27 18:32:32	Microsoft-Windows-Security-Auditing	4797: An attempt was made to query the existence of a blank password for an account. Subject: Security ID: S-1-5-19 Account Name: LOCAL SERVICE Account Domain: NT AUTHORITY Logon ID: 0x3e5 Additional Information: Caller Workstation: LTRANPHD Target Account Name: Liem Target Account Domain: LTRANPHD
Security	Audit Success	13824	2015-04-27 18:32:32	Microsoft-Windows-Security-Auditing	4797: An attempt was made to query the existence of a blank password for an account. Subject: Security ID: S-1-5-19 Account Name: LOCAL SERVICE Account Domain: NT AUTHORITY Logon ID: 0x3e5 Additional Information: Caller Workstation: LTRANPHD Target Account Name: Liem Target Account Domain: LTRANPHD
Security	Audit Success	13824	2015-04-27 18:32:32	Microsoft-Windows-Security-Auditing	4797: An attempt was made to query the existence of a blank password for an account. Subject: Security ID: S-1-5-19 Account Name: LOCAL SERVICE Account Domain: NT AUTHORITY Logon ID: 0x3e5 Additional Information: Caller Workstation: LTRANPHD Target Account Name: Liem Target Account Domain: LTRANPHD
Security	Audit Success	12288	2015-04-28 18:36:22	Microsoft-Windows-Security-Auditing	4608: Windows is starting up. This event is logged when LSASS.EXE starts and the auditing subsystem is initialized.
Security	Audit Success	12544	2015-04-28 18:36:22	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-0-0 Account Name: - Account Domain: - Logon ID: 0x0 Logon Type: 0 Impersonation Level: - New Logon: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Logon ID: 0x3e7 Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x4 Process Name: Network Information: Workstation Name: - Source Network Address: - Source Port: - Detailed Authentication Information: Logon Process: - Authentication Package: - Transited Services: - Package Name (NTLM only): - Key Length: 0 This event is generated when a logon session is created. It is generated on the computer that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service such as the Server service, or a local process such as Winlogon.exe or Services.exe. The logon type field indicates the kind of logon that occurred. The most common types are 2 (interactive) and 3 (network). The New Logon fields indicate the account for whom the new logon was created, i.e. the account that was logged on. The network fields indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impersonation level field indicates the extent to which a process in the logon session can impersonate. The authentication information fields provide detailed information about this specific logon request. - Logon GUID is a unique identifier that can be used to correlate this event with a KDC event. - Transited services indicate which intermediate services have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indicates the length of the generated session key. This will be 0 if no session key was requested.
Security	Audit Success	12544	2015-04-28 18:36:22	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: LTRANPHD$ Account Domain: WORKGROUP Logon ID: 0x3e7 Logon Type: 5 Impersonation Level: %%1833 New Logon: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Logon ID: 0x3e7 Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x22c Process Name: C:\Windows\System32\services.exe Network Information: Workstation Name: Source Network Address: - Source Port: - Detailed Authentication Information: Logon Process: Advapi Authentication Package: Negotiate Transited Services: - Package Name (NTLM only): - Key Length: 0 This event is generated when a logon session is created. It is generated on the computer that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service such as the Server service, or a local process such as Winlogon.exe or Services.exe. The logon type field indicates the kind of logon that occurred. The most common types are 2 (interactive) and 3 (network). The New Logon fields indicate the account for whom the new logon was created, i.e. the account that was logged on. The network fields indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impersonation level field indicates the extent to which a process in the logon session can impersonate. The authentication information fields provide detailed information about this specific logon request. - Logon GUID is a unique identifier that can be used to correlate this event with a KDC event. - Transited services indicate which intermediate services have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indicates the length of the generated session key. This will be 0 if no session key was requested.
					4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: LTRANPHD$ Account Domain: WORKGROUP Logon ID: 0x3e7 Logon Type: 5 Impersonation Level: %%1833 New Logon: Security ID: S-1-5-20 Account Name: NETWORK SERVICE Account Domain: NT AUTHORITY Logon ID: 0x3e4 Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x22c Process Name: C:\Windows\System32\services.exe Network Information: Workstation Name: Source Network Address: - Source Port: - Detailed Authentication Information: Logon Process: Advapi Authentication Package: Negotiate Transited Services: - Package Name (NTLM only): - Key Length: 0 This event is generated when a logon session is created. It is generated on the computer that was accessed. The subject fields indicate the account on the

Security	Audit Success	12544	2015-04-28 18:36:22	Microsoft-Windows-Security-Auditing	local system which requested the logon. This is most commonly a service such as the Server service, or a local process such as Winlogon.exe or Services.exe. The logon type field indicates the kind of logon that occurred. The most common types are 2 (interactive) and 3 (network). The New Logon fields indicate the account for whom the new logon was created, i.e. the account that was logged on. The network fields indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impersonation level field indicates the extent to which a process in the logon session can impersonate. The authentication information fields provide detailed information about this specific logon request. - Logon GUID is a unique identifier that can be used to correlate this event with a KDC event. - Transited services indicate which intermediate services have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indicates the length of the generated session key. This will be 0 if no session key was requested.
Security	Audit Success	12544	2015-04-28 18:36:22	Microsoft-Windows-Security-Auditing	4648: A logon was attempted using explicit credentials. Subject: Security ID: S-1-5-18 Account Name: LTRANPHD$ Account Domain: WORKGROUP Logon ID: 0x3e7 Logon GUID: {00000000-0000-0000-0000-000000000000} Account Whose Credentials Were Used: Account Name: DWM-1 Account Domain: Window Manager Logon GUID: {00000000-0000-0000-0000-000000000000} Target Server: Target Server Name: localhost Additional Information: localhost Process Information: Process ID: 0x204 Process Name: C:\Windows\System32\winlogon.exe Network Information: Network Address: - Port: - This event is generated when a process attempts to log on an account by explicitly specifying that account's credentials. This most commonly occurs in batch-type configurations such as scheduled tasks, or when using the RUNAS command.
Security	Audit Success	12544	2015-04-28 18:36:22	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: LTRANPHD$ Account Domain: WORKGROUP Logon ID: 0x3e7 Logon Type: 2 Impersonation Level: %%1833 New Logon: Security ID: S-1-5-90-1 Account Name: DWM-1 Account Domain: Window Manager Logon ID: 0xe0fd Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x204 Process Name: C:\Windows\System32\winlogon.exe Network Information: Workstation Name: Source Network Address: - Source Port: - Detailed Authentication Information: Logon Process: Advapi Authentication Package: Negotiate Transited Services: - Package Name (NTLM only): - Key Length: 0 This event is generated when a logon session is created. It is generated on the computer that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service such as the Server service, or a local process such as Winlogon.exe or Services.exe. The logon type field indicates the kind of logon that occurred. The most common types are 2 (interactive) and 3 (network). The New Logon fields indicate the account for whom the new logon was created, i.e. the account that was logged on. The network fields indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impersonation level field indicates the extent to which a process in the logon session can impersonate. The authentication information fields provide detailed information about this specific logon request. - Logon GUID is a unique identifier that can be used to correlate this event with a KDC event. - Transited services indicate which intermediate services have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indicates the length of the generated session key. This will be 0 if no session key was requested.
Security	Audit Success	12544	2015-04-28 18:36:22	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: LTRANPHD$ Account Domain: WORKGROUP Logon ID: 0x3e7 Logon Type: 2 Impersonation Level: %%1833 New Logon: Security ID: S-1-5-90-1 Account Name: DWM-1 Account Domain: Window Manager Logon ID: 0xe113 Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x204 Process Name: C:\Windows\System32\winlogon.exe Network Information: Workstation Name: Source Network Address: - Source Port: - Detailed Authentication Information: Logon Process: Advapi Authentication Package: Negotiate Transited Services: - Package Name (NTLM only): - Key Length: 0 This event is generated when a logon session is created. It is generated on the computer that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service such as the Server service, or a local process such as Winlogon.exe or Services.exe. The logon type field indicates the kind of logon that occurred. The most common types are 2 (interactive) and 3 (network). The New Logon fields indicate the account for whom the new logon was created, i.e. the account that was logged on. The network fields indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impersonation level field indicates the extent to which a process in the logon session can impersonate. The authentication information fields provide detailed information about this specific logon request. - Logon GUID is a unique identifier that can be used to correlate this event with a KDC event. - Transited services indicate which intermediate services have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indicates the length of the generated session key. This will be 0 if no session key was requested.
Security	Audit	12544	2015-04-28	Microsoft-Windows-Security-	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: LTRANPHD$ Account Domain: WORKGROUP Logon ID: 0x3e7 Logon Type: 5 Impersonation Level: %%1833 New Logon: Security ID: S-1-5-19 Account Name: LOCAL SERVICE Account Domain: NT AUTHORITY Logon ID: 0x3e5 Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x22c Process Name: C:\Windows\System32\services.exe Network Information: Workstation Name: Source Network Address: - Source Port: - Detailed Authentication Information: Logon Process: Advapi Authentication Package: Negotiate Transited Services: - Package Name (NTLM only): - Key Length: 0 This event is generated when a logon session is created. It is generated on the computer that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service such as the Server service, or a local process such as Winlogon.exe or Services.exe. The logon type field indicates the kind of logon that occurred.

	Success		18:36:22	Auditing	The most common types are 2 (interactive) and 3 (network). The New Logon fields indicate the account for whom the new logon was created, i.e. the account that was logged on. The network fields indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impersonation level field indicates the extent to which a process in the logon session can impersonate. The authentication information fields provide detailed information about this specific logon request. - Logon GUID is a unique identifier that can be used to correlate this event with a KDC event. - Transited services indicate which intermediate services have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indicates the length of the generated session key. This will be 0 if no session key was requested.
Security	Audit Success	12544	2015-04-28 18:36:22	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: LTRANPHD$ Account Domain: WORKGROUP Logon ID: 0x3e7 Logon Type: 5 Impersonation Level: %%1833 New Logon: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Logon ID: 0x3e7 Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x22c Process Name: C:\Windows\System32\services.exe Network Information: Workstation Name: Source Network Address: - Source Port: - Detailed Authentication Information: Logon Process: Advapi Authentication Package: Negotiate Transited Services: - Package Name (NTLM only): - Key Length: 0 This event is generated when a logon session is created. It is generated on the computer that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service such as the Server service, or a local process such as Winlogon.exe or Services.exe. The logon type field indicates the kind of logon that occurred. The most common types are 2 (interactive) and 3 (network). The New Logon fields indicate the account for whom the new logon was created, i.e. the account that was logged on. The network fields indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impersonation level field indicates the extent to which a process in the logon session can impersonate. The authentication information fields provide detailed information about this specific logon request. - Logon GUID is a unique identifier that can be used to correlate this event with a KDC event. - Transited services indicate which intermediate services have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indicates the length of the generated session key. This will be 0 if no session key was requested.
Security	Audit Success	12544	2015-04-28 18:36:22	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: LTRANPHD$ Account Domain: WORKGROUP Logon ID: 0x3e7 Logon Type: 5 Impersonation Level: %%1833 New Logon: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Logon ID: 0x3e7 Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x22c Process Name: C:\Windows\System32\services.exe Network Information: Workstation Name: Source Network Address: - Source Port: - Detailed Authentication Information: Logon Process: Advapi Authentication Package: Negotiate Transited Services: - Package Name (NTLM only): - Key Length: 0 This event is generated when a logon session is created. It is generated on the computer that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service such as the Server service, or a local process such as Winlogon.exe or Services.exe. The logon type field indicates the kind of logon that occurred. The most common types are 2 (interactive) and 3 (network). The New Logon fields indicate the account for whom the new logon was created, i.e. the account that was logged on. The network fields indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impersonation level field indicates the extent to which a process in the logon session can impersonate. The authentication information fields provide detailed information about this specific logon request. - Logon GUID is a unique identifier that can be used to correlate this event with a KDC event. - Transited services indicate which intermediate services have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indicates the length of the generated session key. This will be 0 if no session key was requested.
Security	Audit Success	12548	2015-04-28 18:36:22	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Logon ID: 0x3e7 Privileges: SeAssignPrimaryTokenPrivilege SeTcbPrivilege SeSecurityPrivilege SeTakeOwnershipPrivilege SeLoadDriverPrivilege SeBackupPrivilege SeRestorePrivilege SeDebugPrivilege SeAuditPrivilege SeSystemEnvironmentPrivilege SeImpersonatePrivilege
Security	Audit Success	12548	2015-04-28 18:36:22	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-20 Account Name: NETWORK SERVICE Account Domain: NT AUTHORITY Logon ID: 0x3e4 Privileges: SeAssignPrimaryTokenPrivilege SeAuditPrivilege SeImpersonatePrivilege
Security	Audit Success	12548	2015-04-28 18:36:22	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-90-1 Account Name: DWM-1 Account Domain: Window Manager Logon ID: 0xe0fd Privileges: SeAssignPrimaryTokenPrivilege SeAuditPrivilege SeImpersonatePrivilege
Security	Audit Success	12548	2015-04-28 18:36:22	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-90-1 Account Name: DWM-1 Account Domain: Window Manager Logon ID: 0xe113 Privileges: SeAssignPrimaryTokenPrivilege SeAuditPrivilege
Security	Audit Success	12548	2015-04-28 18:36:22	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-19 Account Name: LOCAL SERVICE Account Domain: NT AUTHORITY Logon ID: 0x3e5 Privileges: SeAssignPrimaryTokenPrivilege SeAuditPrivilege SeImpersonatePrivilege
Security	Audit	12548	2015-04-28	Microsoft-Windows-Security-	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Logon ID: 0x3e7 Privileges: SeAssignPrimaryTokenPrivilege SeTcbPrivilege

	Success		18:36:22	Auditing	SeSecurityPrivilege SeTakeOwnershipPrivilege SeLoadDriverPrivilege SeBackupPrivilege SeRestorePrivilege SeDebugPrivilege SeAuditPrivilege SeSystemEnvironmentPrivilege SeImpersonatePrivilege
Security	Audit Success	12548	2015-04-28 18:36:22	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Logon ID: 0x3e7 Privileges: SeAssignPrimaryTokenPrivilege SeTcbPrivilege SeSecurityPrivilege SeTakeOwnershipPrivilege SeLoadDriverPrivilege SeBackupPrivilege SeRestorePrivilege SeDebugPrivilege SeAuditPrivilege SeSystemEnvironmentPrivilege SeImpersonatePrivilege
Security	Audit Success	13568	2015-04-28 18:36:22	Microsoft-Windows-Security-Auditing	4902: The Per-user audit policy table was created. Number of Elements: 0 Policy ID: 0x90b0
Security	Audit Success	101	2015-04-28 18:36:23	Microsoft-Windows-Eventlog	1101: Audit events have been dropped by the transport. 0
Security	Audit Success	12292	2015-04-28 18:36:23	Microsoft-Windows-Security-Auditing	5033: The Windows Firewall Driver started successfully.
Security	Audit Success	12544	2015-04-28 18:36:23	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: LTRANPHD$ Account Domain: WORKGROUP Logon ID: 0x3e7 Logon Type: 5 Impersonation Level: %%1833 New Logon: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Logon ID: 0x3e7 Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x22c Process Name: C:\Windows\System32\services.exe Network Information: Workstation Name: Source Network Address: - Source Port: - Detailed Authentication Information: Logon Process: Advapi Authentication Package: Negotiate Transited Services: - Package Name (NTLM only): - Key Length: 0 This event is generated when a logon session is created. It is generated on the computer that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service such as the Server service, or a local process such as Winlogon.exe or Services.exe. The logon type field indicates the kind of logon that occurred. The most common types are 2 (interactive) and 3 (network). The New Logon fields indicate the account for whom the new logon was created, i.e. the account that was logged on. The network fields indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impersonation level field indicates the extent to which a process in the logon session can impersonate. The authentication information fields provide detailed information about this specific logon request. - Logon GUID is a unique identifier that can be used to correlate this event with a KDC event. - Transited services indicate which intermediate services have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indicates the length of the generated session key. This will be 0 if no session key was requested.
Security	Audit Success	12544	2015-04-28 18:36:23	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: LTRANPHD$ Account Domain: WORKGROUP Logon ID: 0x3e7 Logon Type: 5 Impersonation Level: %%1833 New Logon: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Logon ID: 0x3e7 Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x22c Process Name: C:\Windows\System32\services.exe Network Information: Workstation Name: Source Network Address: - Source Port: - Detailed Authentication Information: Logon Process: Advapi Authentication Package: Negotiate Transited Services: - Package Name (NTLM only): - Key Length: 0 This event is generated when a logon session is created. It is generated on the computer that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service such as the Server service, or a local process such as Winlogon.exe or Services.exe. The logon type field indicates the kind of logon that occurred. The most common types are 2 (interactive) and 3 (network). The New Logon fields indicate the account for whom the new logon was created, i.e. the account that was logged on. The network fields indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impersonation level field indicates the extent to which a process in the logon session can impersonate. The authentication information fields provide detailed information about this specific logon request. - Logon GUID is a unique identifier that can be used to correlate this event with a KDC event. - Transited services indicate which intermediate services have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indicates the length of the generated session key. This will be 0 if no session key was requested.
Security	Audit Success	12548	2015-04-28 18:36:23	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Logon ID: 0x3e7 Privileges: SeAssignPrimaryTokenPrivilege SeTcbPrivilege SeSecurityPrivilege SeTakeOwnershipPrivilege SeLoadDriverPrivilege SeBackupPrivilege SeRestorePrivilege SeDebugPrivilege SeAuditPrivilege SeSystemEnvironmentPrivilege SeImpersonatePrivilege
Security	Audit Success	12548	2015-04-28 18:36:23	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Logon ID: 0x3e7 Privileges: SeAssignPrimaryTokenPrivilege SeTcbPrivilege SeSecurityPrivilege SeTakeOwnershipPrivilege SeLoadDriverPrivilege SeBackupPrivilege SeRestorePrivilege SeDebugPrivilege SeAuditPrivilege SeSystemEnvironmentPrivilege SeImpersonatePrivilege
Security	Audit Success	12292	2015-04-28 18:36:24	Microsoft-Windows-Security-Auditing	5024: The Windows Firewall service started successfully.
					4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: LTRANPHD$

Security	Audit Success	12544	2015-04-28 18:36:24	Microsoft-Windows-Security-Auditing	Account Domain: WORKGROUP Logon ID: 0x3e7 Logon Type: 5 Impersonation Level: %%1833 New Logon: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Logon ID: 0x3e7 Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x22c Process Name: C:\Windows\System32\services.exe Network Information: Workstation Name: Source Network Address: - Source Port: - Detailed Authentication Information: Logon Process: Advapi Authentication Package: Negotiate Transited Services: - Package Name (NTLM only): - Key Length: 0 This event is generated when a logon session is created. It is generated on the computer that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service such as the Server service, or a local process such as Winlogon.exe or Services.exe. The logon type field indicates the kind of logon that occurred. The most common types are 2 (interactive) and 3 (network). The New Logon fields indicate the account for whom the new logon was created, i.e. the account that was logged on. The network fields indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impersonation level field indicates the extent to which a process in the logon session can impersonate. The authentication information fields provide detailed information about this specific logon request. - Logon GUID is a unique identifier that can be used to correlate this event with a KDC event. - Transited services indicate which intermediate services have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indicates the length of the generated session key. This will be 0 if no session key was requested.
Security	Audit Success	12544	2015-04-28 18:36:24	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-0-0 Account Name: - Account Domain: - Logon ID: 0x0 Logon Type: 3 Impersonation Level: %%1833 New Logon: Security ID: S-1-5-7 Account Name: ANONYMOUS LOGON Account Domain: NT AUTHORITY Logon ID: 0x19d1b Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x0 Process Name: - Network Information: Workstation Name: Source Network Address: - Source Port: - Detailed Authentication Information: Logon Process: NtLmSsp Authentication Package: NTLM Transited Services: - Package Name (NTLM only): NTLM V1 Key Length: 0 This event is generated when a logon session is created. It is generated on the computer that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service such as the Server service, or a local process such as Winlogon.exe or Services.exe. The logon type field indicates the kind of logon that occurred. The most common types are 2 (interactive) and 3 (network). The New Logon fields indicate the account for whom the new logon was created, i.e. the account that was logged on. The network fields indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impersonation level field indicates the extent to which a process in the logon session can impersonate. The authentication information fields provide detailed information about this specific logon request. - Logon GUID is a unique identifier that can be used to correlate this event with a KDC event. - Transited services indicate which intermediate services have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indicates the length of the generated session key. This will be 0 if no session key was requested.
Security	Audit Success	12548	2015-04-28 18:36:24	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Logon ID: 0x3e7 Privileges: SeAssignPrimaryTokenPrivilege SeTcbPrivilege SeSecurityPrivilege SeTakeOwnershipPrivilege SeLoadDriverPrivilege SeBackupPrivilege SeRestorePrivilege SeDebugPrivilege SeAuditPrivilege SeSystemEnvironmentPrivilege SeImpersonatePrivilege
Security	Audit Success	12544	2015-04-28 18:36:25	Microsoft-Windows-Security-Auditing	4648: A logon was attempted using explicit credentials. Subject: Security ID: S-1-5-18 Account Name: LTRANPHD$ Account Domain: WORKGROUP Logon ID: 0x3e7 Logon GUID: {00000000-0000-0000-0000-000000000000} Account Whose Credentials Were Used: Account Name: Liem Account Domain: LTRANPHD Logon GUID: {00000000-0000-0000-0000-000000000000} Target Server: Target Server Name: localhost Additional Information: localhost Process Information: Process ID: 0x204 Process Name: C:\Windows\System32\winlogon.exe Network Information: Network Address: 127.0.0.1 Port: 0 This event is generated when a process attempts to log on an account by explicitly specifying that account's credentials. This most commonly occurs in batch-type configurations such as scheduled tasks, or when using the RUNAS command.
Security	Audit Success	12544	2015-04-28 18:36:25	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: LTRANPHD$ Account Domain: WORKGROUP Logon ID: 0x3e7 Logon Type: 2 Impersonation Level: %%1833 New Logon: Security ID: S-1-5-21-1888849264-3803429180-4108621888-1001 Account Name: Liem Account Domain: LTRANPHD Logon ID: 0x1bf47 Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x204 Process Name: C:\Windows\System32\winlogon.exe Network Information: Workstation Name: LTRANPHD Source Network Address: 127.0.0.1 Source Port: 0 Detailed Authentication Information: Logon Process: User32 Authentication Package: Negotiate Transited Services: - Package Name (NTLM only): - Key Length: 0 This event is generated when a logon session is created. It is generated on the computer that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service such as the Server service, or a local process such as Winlogon.exe or Services.exe. The logon type field indicates the kind of logon that occurred. The most common types are 2 (interactive) and 3 (network). The New Logon fields indicate the account for whom the new logon was created, i.e. the account that was logged on. The network fields indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impersonation level field indicates the extent to which a process in the logon session can impersonate. The authentication information fields provide detailed information about this specific logon request. - Logon GUID is a unique identifier that can be used to correlate this event with a KDC event. - Transited services indicate which intermediate services have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length

					indicates the length of the generated session key. This will be 0 if no session key was requested.
Security	Audit Success	12544	2015-04-28 18:36:25	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: LTRANPHD$ Account Domain: WORKGROUP Logon ID: 0x3e7 Logon Type: 2 Impersonation Level: %%1833 New Logon: Security ID: S-1-5-21-1888849264-3803429180-4108621888-1001 Account Name: Liem Account Domain: LTRANPHD Logon ID: 0x1bf76 Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x204 Process Name: C:\Windows\System32\winlogon.exe Network Information: Workstation Name: LTRANPHD Source Network Address: 127.0.0.1 Source Port: 0 Detailed Authentication Information: Logon Process: User32 Authentication Package: Negotiate Transited Services: - Package Name (NTLM only): - Key Length: 0 This event is generated when a logon session is created. It is generated on the computer that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service such as the Server service, or a local process such as Winlogon.exe or Services.exe. The logon type field indicates the kind of logon that occurred. The most common types are 2 (interactive) and 3 (network). The New Logon fields indicate the account for whom the new logon was created, i.e. the account that was logged on. The network fields indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impersonation level field indicates the extent to which a process in the logon session can impersonate. The authentication information fields provide detailed information about this specific logon request. - Logon GUID is a unique identifier that can be used to correlate this event with a KDC event. - Transited services indicate which intermediate services have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indicates the length of the generated session key. This will be 0 if no session key was requested.
Security	Audit Success	12548	2015-04-28 18:36:25	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-21-1888849264-3803429180-4108621888-1001 Account Name: Liem Account Domain: LTRANPHD Logon ID: 0x1bf47 Privileges: SeSecurityPrivilege SeTakeOwnershipPrivilege SeLoadDriverPrivilege SeBackupPrivilege SeRestorePrivilege SeDebugPrivilege SeSystemEnvironmentPrivilege SeImpersonatePrivilege
Security	Audit Success	12544	2015-04-28 18:36:28	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: LTRANPHD$ Account Domain: WORKGROUP Logon ID: 0x3e7 Logon Type: 5 Impersonation Level: %%1833 New Logon: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Logon ID: 0x3e7 Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x22c Process Name: C:\Windows\System32\services.exe Network Information: Workstation Name: Source Network Address: - Source Port: - Detailed Authentication Information: Logon Process: Advapi Authentication Package: Negotiate Transited Services: - Package Name (NTLM only): - Key Length: 0 This event is generated when a logon session is created. It is generated on the computer that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service such as the Server service, or a local process such as Winlogon.exe or Services.exe. The logon type field indicates the kind of logon that occurred. The most common types are 2 (interactive) and 3 (network). The New Logon fields indicate the account for whom the new logon was created, i.e. the account that was logged on. The network fields indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impersonation level field indicates the extent to which a process in the logon session can impersonate. The authentication information fields provide detailed information about this specific logon request. - Logon GUID is a unique identifier that can be used to correlate this event with a KDC event. - Transited services indicate which intermediate services have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indicates the length of the generated session key. This will be 0 if no session key was requested.
Security	Audit Success	12548	2015-04-28 18:36:28	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Logon ID: 0x3e7 Privileges: SeAssignPrimaryTokenPrivilege SeTcbPrivilege SeSecurityPrivilege SeTakeOwnershipPrivilege SeLoadDriverPrivilege SeBackupPrivilege SeRestorePrivilege SeDebugPrivilege SeAuditPrivilege SeSystemEnvironmentPrivilege SeImpersonatePrivilege
Security	Audit Success	13824	2015-04-28 18:36:30	Microsoft-Windows-Security-Auditing	4797: An attempt was made to query the existence of a blank password for an account. Subject: Security ID: S-1-5-21-1888849264-3803429180-4108621888-1001 Account Name: Liem Account Domain: LTRANPHD Logon ID: 0x1bf76 Additional Information: Caller Workstation: LTRANPHD Target Account Name: Administrator Target Account Domain: LTRANPHD
Security	Audit Success	13824	2015-04-28 18:36:30	Microsoft-Windows-Security-Auditing	4797: An attempt was made to query the existence of a blank password for an account. Subject: Security ID: S-1-5-21-1888849264-3803429180-4108621888-1001 Account Name: Liem Account Domain: LTRANPHD Logon ID: 0x1bf76 Additional Information: Caller Workstation: LTRANPHD Target Account Name: Guest Target Account Domain: LTRANPHD
Security	Audit Success	13824	2015-04-28 18:36:30	Microsoft-Windows-Security-Auditing	4797: An attempt was made to query the existence of a blank password for an account. Subject: Security ID: S-1-5-21-1888849264-3803429180-4108621888-1001 Account Name: Liem Account Domain: LTRANPHD Logon ID: 0x1bf76 Additional Information: Caller Workstation: LTRANPHD Target Account Name: Administrator Target Account Domain: LTRANPHD
Security	Audit Success	13824	2015-04-28 18:36:30	Microsoft-Windows-Security-Auditing	4797: An attempt was made to query the existence of a blank password for an account. Subject: Security ID: S-1-5-21-1888849264-3803429180-4108621888-1001 Account Name: Liem Account Domain: LTRANPHD Logon ID: 0x1bf76 Additional Information: Caller Workstation: LTRANPHD Target Account Name: Guest Target Account Domain: LTRANPHD
Security	Audit	13824	2015-04-28	Microsoft-Windows-Security-	4797: An attempt was made to query the existence of a blank password for an account. Subject: Security ID: S-1-5-19 Account Name: LOCAL SERVICE Account Domain: NT AUTHORITY Logon ID: 0x3e5 Additional

	Success		18:36:31	Auditing	Information: Caller Workstation: LTRANPHD Target Account Name: Administrator Target Account Domain: LTRANPHD
Security	Audit Success	13824	2015-04-28 18:36:31	Microsoft-Windows-Security-Auditing	4797: An attempt was made to query the existence of a blank password for an account. Subject: Security ID: S-1-5-19 Account Name: LOCAL SERVICE Account Domain: NT AUTHORITY Logon ID: 0x3e5 Additional Information: Caller Workstation: LTRANPHD Target Account Name: Guest Target Account Domain: LTRANPHD
Security	Audit Success	13824	2015-04-28 18:36:31	Microsoft-Windows-Security-Auditing	4797: An attempt was made to query the existence of a blank password for an account. Subject: Security ID: S-1-5-19 Account Name: LOCAL SERVICE Account Domain: NT AUTHORITY Logon ID: 0x3e5 Additional Information: Caller Workstation: LTRANPHD Target Account Name: Liem Target Account Domain: LTRANPHD
Security	Audit Success	13824	2015-04-28 18:36:31	Microsoft-Windows-Security-Auditing	4797: An attempt was made to query the existence of a blank password for an account. Subject: Security ID: S-1-5-19 Account Name: LOCAL SERVICE Account Domain: NT AUTHORITY Logon ID: 0x3e5 Additional Information: Caller Workstation: LTRANPHD Target Account Name: Liem Target Account Domain: LTRANPHD
Security	Audit Success	12544	2015-04-28 18:45:25	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: LTRANPHD$ Account Domain: WORKGROUP Logon ID: 0x3e7 Logon Type: 5 Impersonation Level: %%1833 New Logon: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Logon ID: 0x3e7 Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x22c Process Name: C:\Windows\System32\services.exe Network Information: Workstation Name: Source Network Address: - Source Port: - Detailed Authentication Information: Logon Process: Advapi Authentication Package: Negotiate Transited Services: - Package Name (NTLM only): - Key Length: 0 This event is generated when a logon session is created. It is generated on the computer that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service such as the Server service, or a local process such as Winlogon.exe or Services.exe. The logon type field indicates the kind of logon that occurred. The most common types are 2 (interactive) and 3 (network). The New Logon fields indicate the account for whom the new logon was created, i.e. the account that was logged on. The network fields indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impersonation level field indicates the extent to which a process in the logon session can impersonate. The authentication information fields provide detailed information about this specific logon request. - Logon GUID is a unique identifier that can be used to correlate this event with a KDC event. - Transited services indicate which intermediate services have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indicates the length of the generated session key. This will be 0 if no session key was requested.
Security	Audit Success	12544	2015-04-28 18:45:25	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: LTRANPHD$ Account Domain: WORKGROUP Logon ID: 0x3e7 Logon Type: 5 Impersonation Level: %%1833 New Logon: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Logon ID: 0x3e7 Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x22c Process Name: C:\Windows\System32\services.exe Network Information: Workstation Name: Source Network Address: - Source Port: - Detailed Authentication Information: Logon Process: Advapi Authentication Package: Negotiate Transited Services: - Package Name (NTLM only): - Key Length: 0 This event is generated when a logon session is created. It is generated on the computer that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service such as the Server service, or a local process such as Winlogon.exe or Services.exe. The logon type field indicates the kind of logon that occurred. The most common types are 2 (interactive) and 3 (network). The New Logon fields indicate the account for whom the new logon was created, i.e. the account that was logged on. The network fields indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impersonation level field indicates the extent to which a process in the logon session can impersonate. The authentication information fields provide detailed information about this specific logon request. - Logon GUID is a unique identifier that can be used to correlate this event with a KDC event. - Transited services indicate which intermediate services have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indicates the length of the generated session key. This will be 0 if no session key was requested.
Security	Audit Success	12548	2015-04-28 18:45:25	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Logon ID: 0x3e7 Privileges: SeAssignPrimaryTokenPrivilege SeTcbPrivilege SeSecurityPrivilege SeTakeOwnershipPrivilege SeLoadDriverPrivilege SeBackupPrivilege SeRestorePrivilege SeDebugPrivilege SeAuditPrivilege SeSystemEnvironmentPrivilege SeImpersonatePrivilege
Security	Audit Success	12548	2015-04-28 18:45:25	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Logon ID: 0x3e7 Privileges: SeAssignPrimaryTokenPrivilege SeTcbPrivilege SeSecurityPrivilege SeTakeOwnershipPrivilege SeLoadDriverPrivilege SeBackupPrivilege SeRestorePrivilege SeDebugPrivilege SeAuditPrivilege SeSystemEnvironmentPrivilege SeImpersonatePrivilege
Security	Audit Success	12288	2015-04-28 19:06:35	Microsoft-Windows-Security-Auditing	4608: Windows is starting up. This event is logged when LSASS.EXE starts and the auditing subsystem is initialized.
					4624: An account was successfully logged on. Subject: Security ID: S-1-0-0 Account Name: - Account Domain: - Logon ID: 0x0 Logon Type: 0 Impersonation Level: - New Logon: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Logon ID: 0x3e7 Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x4 Process Name: Network Information: Workstation Name: - Source Network Address: - Source Port: - Detailed Authentication Information: Logon Process: -

	Security	Audit Success	12544	2015-04-28 19:06:35	Microsoft-Windows-Security-Auditing	Authentication Package: - Transited Services: - Package Name (NTLM only): - Key Length: 0 This event is generated when a logon session is created. It is generated on the computer that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service such as the Server service, or a local process such as Winlogon.exe or Services.exe. The logon type field indicates the kind of logon that occurred. The most common types are 2 (interactive) and 3 (network). The New Logon fields indicate the account for whom the new logon was created, i.e. the account that was logged on. The network fields indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impersonation level field indicates the extent to which a process in the logon session can impersonate. The authentication information fields provide detailed information about this specific logon request. - Logon GUID is a unique identifier that can be used to correlate this event with a KDC event. - Transited services indicate which intermediate services have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indicates the length of the generated session key. This will be 0 if no session key was requested.
	Security	Audit Success	12544	2015-04-28 19:06:35	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: LTRANPHD$ Account Domain: WORKGROUP Logon ID: 0x3e7 Logon Type: 5 Impersonation Level: %%1833 New Logon: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Logon ID: 0x3e7 Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x230 Process Name: C:\Windows\System32\services.exe Network Information: Workstation Name: Source Network Address: - Source Port: - Detailed Authentication Information: Logon Process: Advapi Authentication Package: Negotiate Transited Services: - Package Name (NTLM only): - Key Length: 0 This event is generated when a logon session is created. It is generated on the computer that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service such as the Server service, or a local process such as Winlogon.exe or Services.exe. The logon type field indicates the kind of logon that occurred. The most common types are 2 (interactive) and 3 (network). The New Logon fields indicate the account for whom the new logon was created, i.e. the account that was logged on. The network fields indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impersonation level field indicates the extent to which a process in the logon session can impersonate. The authentication information fields provide detailed information about this specific logon request. - Logon GUID is a unique identifier that can be used to correlate this event with a KDC event. - Transited services indicate which intermediate services have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indicates the length of the generated session key. This will be 0 if no session key was requested.
	Security	Audit Success	12544	2015-04-28 19:06:35	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: LTRANPHD$ Account Domain: WORKGROUP Logon ID: 0x3e7 Logon Type: 5 Impersonation Level: %%1833 New Logon: Security ID: S-1-5-20 Account Name: NETWORK SERVICE Account Domain: NT AUTHORITY Logon ID: 0x3e4 Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x230 Process Name: C:\Windows\System32\services.exe Network Information: Workstation Name: Source Network Address: - Source Port: - Detailed Authentication Information: Logon Process: Advapi Authentication Package: Negotiate Transited Services: - Package Name (NTLM only): - Key Length: 0 This event is generated when a logon session is created. It is generated on the computer that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service such as the Server service, or a local process such as Winlogon.exe or Services.exe. The logon type field indicates the kind of logon that occurred. The most common types are 2 (interactive) and 3 (network). The New Logon fields indicate the account for whom the new logon was created, i.e. the account that was logged on. The network fields indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impersonation level field indicates the extent to which a process in the logon session can impersonate. The authentication information fields provide detailed information about this specific logon request. - Logon GUID is a unique identifier that can be used to correlate this event with a KDC event. - Transited services indicate which intermediate services have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indicates the length of the generated session key. This will be 0 if no session key was requested.
	Security	Audit Success	12544	2015-04-28 19:06:35	Microsoft-Windows-Security-Auditing	4648: A logon was attempted using explicit credentials. Subject: Security ID: S-1-5-18 Account Name: LTRANPHD$ Account Domain: WORKGROUP Logon ID: 0x3e7 Logon GUID: {00000000-0000-0000-0000-000000000000} Account Whose Credentials Were Used: Account Name: DWM-1 Account Domain: Window Manager Logon GUID: {00000000-0000-0000-0000-000000000000} Target Server: Target Server Name: localhost Additional Information: localhost Process Information: Process ID: 0x218 Process Name: C:\Windows\System32\winlogon.exe Network Information: Network Address: - Port: - This event is generated when a process attempts to log on an account by explicitly specifying that account's credentials. This most commonly occurs in batch-type configurations such as scheduled tasks, or when using the RUNAS command.
						4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: LTRANPHD$ Account Domain: WORKGROUP Logon ID: 0x3e7 Logon Type: 2 Impersonation Level: %%1833 New Logon: Security ID: S-1-5-90-1 Account Name: DWM-1 Account Domain: Window Manager Logon ID: 0xdc8e Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x218 Process Name: C:\Windows\System32\winlogon.exe Network Information: Workstation Name: Source Network Address: - Source Port: - Detailed Authentication Information: Logon Process: Advapi Authentication Package: Negotiate Transited Services: - Package Name (NTLM only): - Key Length: 0 This event is generated when a logon session is created. It is generated on the computer that was accessed. The subject fields indicate the account on the

Security	Audit Success	12544	2015-04-28 19:06:35	Microsoft-Windows-Security-Auditing	local system which requested the logon. This is most commonly a service such as the Server service, or a local process such as Winlogon.exe or Services.exe. The logon type field indicates the kind of logon that occurred. The most common types are 2 (interactive) and 3 (network). The New Logon fields indicate the account for whom the new logon was created, i.e. the account that was logged on. The network fields indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impersonation level field indicates the extent to which a process in the logon session can impersonate. The authentication information fields provide detailed information about this specific logon request. - Logon GUID is a unique identifier that can be used to correlate this event with a KDC event. - Transited services indicate which intermediate services have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indicates the length of the generated session key. This will be 0 if no session key was requested.
Security	Audit Success	12544	2015-04-28 19:06:35	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: LTRANPHD$ Account Domain: WORKGROUP Logon ID: 0x3e7 Logon Type: 2 Impersonation Level: %%1833 New Logon: Security ID: S-1-5-90-1 Account Name: DWM-1 Account Domain: Window Manager Logon ID: 0xdca9 Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x218 Process Name: C:\Windows\System32\winlogon.exe Network Information: Workstation Name: Source Network Address: - Source Port: - Detailed Authentication Information: Logon Process: Advapi Authentication Package: Negotiate Transited Services: - Package Name (NTLM only): - Key Length: 0 This event is generated when a logon session is created. It is generated on the computer that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service such as the Server service, or a local process such as Winlogon.exe or Services.exe. The logon type field indicates the kind of logon that occurred. The most common types are 2 (interactive) and 3 (network). The New Logon fields indicate the account for whom the new logon was created, i.e. the account that was logged on. The network fields indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impersonation level field indicates the extent to which a process in the logon session can impersonate. The authentication information fields provide detailed information about this specific logon request. - Logon GUID is a unique identifier that can be used to correlate this event with a KDC event. - Transited services indicate which intermediate services have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indicates the length of the generated session key. This will be 0 if no session key was requested.
Security	Audit Success	12544	2015-04-28 19:06:35	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: LTRANPHD$ Account Domain: WORKGROUP Logon ID: 0x3e7 Logon Type: 5 Impersonation Level: %%1833 New Logon: Security ID: S-1-5-19 Account Name: LOCAL SERVICE Account Domain: NT AUTHORITY Logon ID: 0x3e5 Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x230 Process Name: C:\Windows\System32\services.exe Network Information: Workstation Name: Source Network Address: - Source Port: - Detailed Authentication Information: Logon Process: Advapi Authentication Package: Negotiate Transited Services: - Package Name (NTLM only): - Key Length: 0 This event is generated when a logon session is created. It is generated on the computer that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service such as the Server service, or a local process such as Winlogon.exe or Services.exe. The logon type field indicates the kind of logon that occurred. The most common types are 2 (interactive) and 3 (network). The New Logon fields indicate the account for whom the new logon was created, i.e. the account that was logged on. The network fields indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impersonation level field indicates the extent to which a process in the logon session can impersonate. The authentication information fields provide detailed information about this specific logon request. - Logon GUID is a unique identifier that can be used to correlate this event with a KDC event. - Transited services indicate which intermediate services have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indicates the length of the generated session key. This will be 0 if no session key was requested.
Security	Audit Success	12544	2015-04-28 19:06:35	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: LTRANPHD$ Account Domain: WORKGROUP Logon ID: 0x3e7 Logon Type: 5 Impersonation Level: %%1833 New Logon: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Logon ID: 0x3e7 Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x230 Process Name: C:\Windows\System32\services.exe Network Information: Workstation Name: Source Network Address: - Source Port: - Detailed Authentication Information: Logon Process: Advapi Authentication Package: Negotiate Transited Services: - Package Name (NTLM only): - Key Length: 0 This event is generated when a logon session is created. It is generated on the computer that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service such as the Server service, or a local process such as Winlogon.exe or Services.exe. The logon type field indicates the kind of logon that occurred. The most common types are 2 (interactive) and 3 (network). The New Logon fields indicate the account for whom the new logon was created, i.e. the account that was logged on. The network fields indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impersonation level field indicates the extent to which a process in the logon session can impersonate. The authentication information fields provide detailed information about this specific logon request. - Logon GUID is a unique identifier that can be used to correlate this event with a KDC event. - Transited services indicate which intermediate services have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indicates the length of the generated

					session key. This will be 0 if no session key was requested.
Security	Audit Success	12544	2015-04-28 19:06:35	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: LTRANPHD$ Account Domain: WORKGROUP Logon ID: 0x3e7 Logon Type: 5 Impersonation Level: %%1833 New Logon: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Logon ID: 0x3e7 Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x230 Process Name: C:\Windows\System32\services.exe Network Information: Workstation Name: Source Network Address: - Source Port: - Detailed Authentication Information: Logon Process: Advapi Authentication Package: Negotiate Transited Services: - Package Name (NTLM only): - Key Length: 0 This event is generated when a logon session is created. It is generated on the computer that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service such as the Server service, or a local process such as Winlogon.exe or Services.exe. The logon type field indicates the kind of logon that occurred. The most common types are 2 (interactive) and 3 (network). The New Logon fields indicate the account for whom the new logon was created, i.e. the account that was logged on. The network fields indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impersonation level field indicates the extent to which a process in the logon session can impersonate. The authentication information fields provide detailed information about this specific logon request. - Logon GUID is a unique identifier that can be used to correlate this event with a KDC event. - Transited services indicate which intermediate services have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indicates the length of the generated session key. This will be 0 if no session key was requested.
Security	Audit Success	12548	2015-04-28 19:06:35	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Logon ID: 0x3e7 Privileges: SeAssignPrimaryTokenPrivilege SeTcbPrivilege SeSecurityPrivilege SeTakeOwnershipPrivilege SeLoadDriverPrivilege SeBackupPrivilege SeRestorePrivilege SeDebugPrivilege SeAuditPrivilege SeSystemEnvironmentPrivilege SeImpersonatePrivilege
Security	Audit Success	12548	2015-04-28 19:06:35	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-20 Account Name: NETWORK SERVICE Account Domain: NT AUTHORITY Logon ID: 0x3e4 Privileges: SeAssignPrimaryTokenPrivilege SeAuditPrivilege SeImpersonatePrivilege
Security	Audit Success	12548	2015-04-28 19:06:35	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-90-1 Account Name: DWM-1 Account Domain: Window Manager Logon ID: 0xdc8e Privileges: SeAssignPrimaryTokenPrivilege SeAuditPrivilege SeImpersonatePrivilege
Security	Audit Success	12548	2015-04-28 19:06:35	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-90-1 Account Name: DWM-1 Account Domain: Window Manager Logon ID: 0xdca9 Privileges: SeAssignPrimaryTokenPrivilege SeAuditPrivilege
Security	Audit Success	12548	2015-04-28 19:06:35	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-19 Account Name: LOCAL SERVICE Account Domain: NT AUTHORITY Logon ID: 0x3e5 Privileges: SeAssignPrimaryTokenPrivilege SeAuditPrivilege SeImpersonatePrivilege
Security	Audit Success	12548	2015-04-28 19:06:35	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Logon ID: 0x3e7 Privileges: SeAssignPrimaryTokenPrivilege SeTcbPrivilege SeSecurityPrivilege SeTakeOwnershipPrivilege SeLoadDriverPrivilege SeBackupPrivilege SeRestorePrivilege SeDebugPrivilege SeAuditPrivilege SeSystemEnvironmentPrivilege SeImpersonatePrivilege
Security	Audit Success	12548	2015-04-28 19:06:35	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Logon ID: 0x3e7 Privileges: SeAssignPrimaryTokenPrivilege SeTcbPrivilege SeSecurityPrivilege SeTakeOwnershipPrivilege SeLoadDriverPrivilege SeBackupPrivilege SeRestorePrivilege SeDebugPrivilege SeAuditPrivilege SeSystemEnvironmentPrivilege SeImpersonatePrivilege
Security	Audit Success	13568	2015-04-28 19:06:35	Microsoft-Windows-Security-Auditing	4902: The Per-user audit policy table was created. Number of Elements: 0 Policy ID: 0xa3e5
Security	Audit Success	101	2015-04-28 19:06:36	Microsoft-Windows-Eventlog	1101: Audit events have been dropped by the transport. 0
Security	Audit Success	12292	2015-04-28 19:06:36	Microsoft-Windows-Security-Auditing	5033: The Windows Firewall Driver started successfully.
Security	Audit Success	12544	2015-04-28 19:06:36	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: LTRANPHD$ Account Domain: WORKGROUP Logon ID: 0x3e7 Logon Type: 5 Impersonation Level: %%1833 New Logon: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Logon ID: 0x3e7 Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x230 Process Name: C:\Windows\System32\services.exe Network Information: Workstation Name: Source Network Address: - Source Port: - Detailed Authentication Information: Logon Process: Advapi Authentication Package: Negotiate Transited Services: - Package Name (NTLM only): - Key Length: 0 This event is generated when a logon session is created. It is generated on the computer that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service such as the Server service, or a local process such as Winlogon.exe or Services.exe. The logon type field indicates the kind of logon that occurred. The most common types are 2 (interactive) and 3 (network). The New Logon fields indicate the account for whom the new logon was created, i.e. the account that was logged on. The network fields indicate where a

					remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impersonation level field indicates the extent to which a process in the logon session can impersonate. The authentication information fields provide detailed information about this specific logon request. - Logon GUID is a unique identifier that can be used to correlate this event with a KDC event. - Transited services indicate which intermediate services have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indicates the length of the generated session key. This will be 0 if no session key was requested.
Security	Audit Success	12544	2015-04-28 19:06:36	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: LTRANPHD$ Account Domain: WORKGROUP Logon ID: 0x3e7 Logon Type: 5 Impersonation Level: %%1833 New Logon: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Logon ID: 0x3e7 Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x230 Process Name: C:\Windows\System32\services.exe Network Information: Workstation Name: Source Network Address: - Source Port: - Detailed Authentication Information: Logon Process: Advapi Authentication Package: Negotiate Transited Services: - Package Name (NTLM only): - Key Length: 0 This event is generated when a logon session is created. It is generated on the computer that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service such as the Server service, or a local process such as Winlogon.exe or Services.exe. The logon type field indicates the kind of logon that occurred. The most common types are 2 (interactive) and 3 (network). The New Logon fields indicate the account for whom the new logon was created, i.e. the account that was logged on. The network fields indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impersonation level field indicates the extent to which a process in the logon session can impersonate. The authentication information fields provide detailed information about this specific logon request. - Logon GUID is a unique identifier that can be used to correlate this event with a KDC event. - Transited services indicate which intermediate services have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indicates the length of the generated session key. This will be 0 if no session key was requested.
Security	Audit Success	12548	2015-04-28 19:06:36	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Logon ID: 0x3e7 Privileges: SeAssignPrimaryTokenPrivilege SeTcbPrivilege SeSecurityPrivilege SeTakeOwnershipPrivilege SeLoadDriverPrivilege SeBackupPrivilege SeRestorePrivilege SeDebugPrivilege SeAuditPrivilege SeSystemEnvironmentPrivilege SeImpersonatePrivilege
Security	Audit Success	12548	2015-04-28 19:06:36	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Logon ID: 0x3e7 Privileges: SeAssignPrimaryTokenPrivilege SeTcbPrivilege SeSecurityPrivilege SeTakeOwnershipPrivilege SeLoadDriverPrivilege SeBackupPrivilege SeRestorePrivilege SeDebugPrivilege SeAuditPrivilege SeSystemEnvironmentPrivilege SeImpersonatePrivilege
Security	Audit Success	12292	2015-04-28 19:06:37	Microsoft-Windows-Security-Auditing	5024: The Windows Firewall service started successfully.
Security	Audit Success	12544	2015-04-28 19:06:37	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: LTRANPHD$ Account Domain: WORKGROUP Logon ID: 0x3e7 Logon Type: 5 Impersonation Level: %%1833 New Logon: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Logon ID: 0x3e7 Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x230 Process Name: C:\Windows\System32\services.exe Network Information: Workstation Name: Source Network Address: - Source Port: - Detailed Authentication Information: Logon Process: Advapi Authentication Package: Negotiate Transited Services: - Package Name (NTLM only): - Key Length: 0 This event is generated when a logon session is created. It is generated on the computer that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service such as the Server service, or a local process such as Winlogon.exe or Services.exe. The logon type field indicates the kind of logon that occurred. The most common types are 2 (interactive) and 3 (network). The New Logon fields indicate the account for whom the new logon was created, i.e. the account that was logged on. The network fields indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impersonation level field indicates the extent to which a process in the logon session can impersonate. The authentication information fields provide detailed information about this specific logon request. - Logon GUID is a unique identifier that can be used to correlate this event with a KDC event. - Transited services indicate which intermediate services have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indicates the length of the generated session key. This will be 0 if no session key was requested.
Security	Audit Success	12544	2015-04-28 19:06:37	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-0-0 Account Name: - Account Domain: - Logon ID: 0x0 Logon Type: 3 Impersonation Level: %%1833 New Logon: Security ID: S-1-5-7 Account Name: ANONYMOUS LOGON Account Domain: NT AUTHORITY Logon ID: 0x1a17f Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x0 Process Name: - Network Information: Workstation Name: Source Network Address: - Source Port: - Detailed Authentication Information: Logon Process: NtLmSsp Authentication Package: NTLM Transited Services: - Package Name (NTLM only): NTLM V1 Key Length: 0 This event is generated when a logon session is created. It is generated on the computer that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service such as the Server service, or a local process such as Winlogon.exe or Services.exe. The logon type field indicates the kind of logon that occurred. The most common types are 2 (interactive) and 3

					(network). The New Logon fields indicate the account for whom the new logon was created, i.e. the account that was logged on. The network fields indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impersonation level field indicates the extent to which a process in the logon session can impersonate. The authentication information fields provide detailed information about this specific logon request. - Logon GUID is a unique identifier that can be used to correlate this event with a KDC event. - Transited services indicate which intermediate services have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indicates the length of the generated session key. This will be 0 if no session key was requested.
Security	Audit Success	12548	2015-04-28 19:06:37	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Logon ID: 0x3e7 Privileges: SeAssignPrimaryTokenPrivilege SeTcbPrivilege SeSecurityPrivilege SeTakeOwnershipPrivilege SeLoadDriverPrivilege SeBackupPrivilege SeRestorePrivilege SeDebugPrivilege SeAuditPrivilege SeSystemEnvironmentPrivilege SeImpersonatePrivilege
Security	Audit Success	12544	2015-04-28 19:08:38	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: LTRANPHD$ Account Domain: WORKGROUP Logon ID: 0x3e7 Logon Type: 5 Impersonation Level: %%1833 New Logon: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Logon ID: 0x3e7 Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x230 Process Name: C:\Windows\System32\services.exe Network Information: Workstation Name: Source Network Address: - Source Port: - Detailed Authentication Information: Logon Process: Advapi Authentication Package: Negotiate Transited Services: - Package Name (NTLM only): - Key Length: 0 This event is generated when a logon session is created. It is generated on the computer that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service such as the Server service, or a local process such as Winlogon.exe or Services.exe. The logon type field indicates the kind of logon that occurred. The most common types are 2 (interactive) and 3 (network). The New Logon fields indicate the account for whom the new logon was created, i.e. the account that was logged on. The network fields indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impersonation level field indicates the extent to which a process in the logon session can impersonate. The authentication information fields provide detailed information about this specific logon request. - Logon GUID is a unique identifier that can be used to correlate this event with a KDC event. - Transited services indicate which intermediate services have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indicates the length of the generated session key. This will be 0 if no session key was requested.
Security	Audit Success	12548	2015-04-28 19:08:38	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Logon ID: 0x3e7 Privileges: SeAssignPrimaryTokenPrivilege SeTcbPrivilege SeSecurityPrivilege SeTakeOwnershipPrivilege SeLoadDriverPrivilege SeBackupPrivilege SeRestorePrivilege SeDebugPrivilege SeAuditPrivilege SeSystemEnvironmentPrivilege SeImpersonatePrivilege
Security	Audit Success	12544	2015-04-28 19:17:06	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: LTRANPHD$ Account Domain: WORKGROUP Logon ID: 0x3e7 Logon Type: 5 Impersonation Level: %%1833 New Logon: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Logon ID: 0x3e7 Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x230 Process Name: C:\Windows\System32\services.exe Network Information: Workstation Name: Source Network Address: - Source Port: - Detailed Authentication Information: Logon Process: Advapi Authentication Package: Negotiate Transited Services: - Package Name (NTLM only): - Key Length: 0 This event is generated when a logon session is created. It is generated on the computer that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service such as the Server service, or a local process such as Winlogon.exe or Services.exe. The logon type field indicates the kind of logon that occurred. The most common types are 2 (interactive) and 3 (network). The New Logon fields indicate the account for whom the new logon was created, i.e. the account that was logged on. The network fields indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impersonation level field indicates the extent to which a process in the logon session can impersonate. The authentication information fields provide detailed information about this specific logon request. - Logon GUID is a unique identifier that can be used to correlate this event with a KDC event. - Transited services indicate which intermediate services have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indicates the length of the generated session key. This will be 0 if no session key was requested.
Security	Audit Success	12548	2015-04-28 19:17:06	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Logon ID: 0x3e7 Privileges: SeAssignPrimaryTokenPrivilege SeTcbPrivilege SeSecurityPrivilege SeTakeOwnershipPrivilege SeLoadDriverPrivilege SeBackupPrivilege SeRestorePrivilege SeDebugPrivilege SeAuditPrivilege SeSystemEnvironmentPrivilege SeImpersonatePrivilege
Security	Audit Success	12288	2015-04-28 19:37:42	Microsoft-Windows-Security-Auditing	4608: Windows is starting up. This event is logged when LSASS.EXE starts and the auditing subsystem is initialized.
					4624: An account was successfully logged on. Subject: Security ID: S-1-0-0 Account Name: - Account Domain: - Logon ID: 0x0 Logon Type: 0 Impersonation Level: - New Logon: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Logon ID: 0x3e7 Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x4 Process Name: Network Information: Workstation Name: - Source Network Address: - Source Port: - Detailed Authentication Information: Logon Process: -

	Security	Audit Success	12544	2015-04-28 19:37:42	Microsoft-Windows-Security-Auditing	Authentication Package: - Transited Services: - Package Name (NTLM only): - Key Length: 0 This event is generated when a logon session is created. It is generated on the computer that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service such as the Server service, or a local process such as Winlogon.exe or Services.exe. The logon type field indicates the kind of logon that occurred. The most common types are 2 (interactive) and 3 (network). The New Logon fields indicate the account for whom the new logon was created, i.e. the account that was logged on. The network fields indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impersonation level field indicates the extent to which a process in the logon session can impersonate. The authentication information fields provide detailed information about this specific logon request. - Logon GUID is a unique identifier that can be used to correlate this event with a KDC event. - Transited services indicate which intermediate services have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indicates the length of the generated session key. This will be 0 if no session key was requested.
	Security	Audit Success	12544	2015-04-28 19:37:42	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: LTRANPHD$ Account Domain: WORKGROUP Logon ID: 0x3e7 Logon Type: 5 Impersonation Level: %%1833 New Logon: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Logon ID: 0x3e7 Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x238 Process Name: C:\Windows\System32\services.exe Network Information: Workstation Name: Source Network Address: - Source Port: - Detailed Authentication Information: Logon Process: Advapi Authentication Package: Negotiate Transited Services: - Package Name (NTLM only): - Key Length: 0 This event is generated when a logon session is created. It is generated on the computer that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service such as the Server service, or a local process such as Winlogon.exe or Services.exe. The logon type field indicates the kind of logon that occurred. The most common types are 2 (interactive) and 3 (network). The New Logon fields indicate the account for whom the new logon was created, i.e. the account that was logged on. The network fields indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impersonation level field indicates the extent to which a process in the logon session can impersonate. The authentication information fields provide detailed information about this specific logon request. - Logon GUID is a unique identifier that can be used to correlate this event with a KDC event. - Transited services indicate which intermediate services have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indicates the length of the generated session key. This will be 0 if no session key was requested.
	Security	Audit Success	12544	2015-04-28 19:37:42	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: LTRANPHD$ Account Domain: WORKGROUP Logon ID: 0x3e7 Logon Type: 5 Impersonation Level: %%1833 New Logon: Security ID: S-1-5-20 Account Name: NETWORK SERVICE Account Domain: NT AUTHORITY Logon ID: 0x3e4 Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x238 Process Name: C:\Windows\System32\services.exe Network Information: Workstation Name: Source Network Address: - Source Port: - Detailed Authentication Information: Logon Process: Advapi Authentication Package: Negotiate Transited Services: - Package Name (NTLM only): - Key Length: 0 This event is generated when a logon session is created. It is generated on the computer that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service such as the Server service, or a local process such as Winlogon.exe or Services.exe. The logon type field indicates the kind of logon that occurred. The most common types are 2 (interactive) and 3 (network). The New Logon fields indicate the account for whom the new logon was created, i.e. the account that was logged on. The network fields indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impersonation level field indicates the extent to which a process in the logon session can impersonate. The authentication information fields provide detailed information about this specific logon request. - Logon GUID is a unique identifier that can be used to correlate this event with a KDC event. - Transited services indicate which intermediate services have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indicates the length of the generated session key. This will be 0 if no session key was requested.
	Security	Audit Success	12544	2015-04-28 19:37:42	Microsoft-Windows-Security-Auditing	4648: A logon was attempted using explicit credentials. Subject: Security ID: S-1-5-18 Account Name: LTRANPHD$ Account Domain: WORKGROUP Logon ID: 0x3e7 Logon GUID: {00000000-0000-0000-0000-000000000000} Account Whose Credentials Were Used: Account Name: DWM-1 Account Domain: Window Manager Logon GUID: {00000000-0000-0000-0000-000000000000} Target Server: Target Server Name: localhost Additional Information: localhost Process Information: Process ID: 0x210 Process Name: C:\Windows\System32\winlogon.exe Network Information: Network Address: - Port: - This event is generated when a process attempts to log on an account by explicitly specifying that account's credentials. This most commonly occurs in batch-type configurations such as scheduled tasks, or when using the RUNAS command.
						4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: LTRANPHD$ Account Domain: WORKGROUP Logon ID: 0x3e7 Logon Type: 2 Impersonation Level: %%1833 New Logon: Security ID: S-1-5-90-1 Account Name: DWM-1 Account Domain: Window Manager Logon ID: 0xe0ae Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x210 Process Name: C:\Windows\System32\winlogon.exe Network Information: Workstation Name: Source Network Address: - Source Port: - Detailed Authentication Information: Logon Process: Advapi Authentication Package: Negotiate Transited Services: - Package Name (NTLM only): - Key Length: 0 This event is generated when a logon session is created. It is generated on the computer that was accessed. The subject fields indicate the account on the

Security	Audit Success	12544	2015-04-28 19:37:42	Microsoft-Windows-Security-Auditing	local system which requested the logon. This is most commonly a service such as the Server service, or a local process such as Winlogon.exe or Services.exe. The logon type field indicates the kind of logon that occurred. The most common types are 2 (interactive) and 3 (network). The New Logon fields indicate the account for whom the new logon was created, i.e. the account that was logged on. The network fields indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impersonation level field indicates the extent to which a process in the logon session can impersonate. The authentication information fields provide detailed information about this specific logon request. - Logon GUID is a unique identifier that can be used to correlate this event with a KDC event. - Transited services indicate which intermediate services have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indicates the length of the generated session key. This will be 0 if no session key was requested.
Security	Audit Success	12544	2015-04-28 19:37:42	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: LTRANPHD$ Account Domain: WORKGROUP Logon ID: 0x3e7 Logon Type: 2 Impersonation Level: %%1833 New Logon: Security ID: S-1-5-90-1 Account Name: DWM-1 Account Domain: Window Manager Logon ID: 0xe0c5 Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x210 Process Name: C:\Windows\System32\winlogon.exe Network Information: Workstation Name: Source Network Address: - Source Port: - Detailed Authentication Information: Logon Process: Advapi Authentication Package: Negotiate Transited Services: - Package Name (NTLM only): - Key Length: 0 This event is generated when a logon session is created. It is generated on the computer that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service such as the Server service, or a local process such as Winlogon.exe or Services.exe. The logon type field indicates the kind of logon that occurred. The most common types are 2 (interactive) and 3 (network). The New Logon fields indicate the account for whom the new logon was created, i.e. the account that was logged on. The network fields indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impersonation level field indicates the extent to which a process in the logon session can impersonate. The authentication information fields provide detailed information about this specific logon request. - Logon GUID is a unique identifier that can be used to correlate this event with a KDC event. - Transited services indicate which intermediate services have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indicates the length of the generated session key. This will be 0 if no session key was requested.
Security	Audit Success	12544	2015-04-28 19:37:42	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: LTRANPHD$ Account Domain: WORKGROUP Logon ID: 0x3e7 Logon Type: 5 Impersonation Level: %%1833 New Logon: Security ID: S-1-5-19 Account Name: LOCAL SERVICE Account Domain: NT AUTHORITY Logon ID: 0x3e5 Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x238 Process Name: C:\Windows\System32\services.exe Network Information: Workstation Name: Source Network Address: - Source Port: - Detailed Authentication Information: Logon Process: Advapi Authentication Package: Negotiate Transited Services: - Package Name (NTLM only): - Key Length: 0 This event is generated when a logon session is created. It is generated on the computer that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service such as the Server service, or a local process such as Winlogon.exe or Services.exe. The logon type field indicates the kind of logon that occurred. The most common types are 2 (interactive) and 3 (network). The New Logon fields indicate the account for whom the new logon was created, i.e. the account that was logged on. The network fields indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impersonation level field indicates the extent to which a process in the logon session can impersonate. The authentication information fields provide detailed information about this specific logon request. - Logon GUID is a unique identifier that can be used to correlate this event with a KDC event. - Transited services indicate which intermediate services have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indicates the length of the generated session key. This will be 0 if no session key was requested.
Security	Audit Success	12544	2015-04-28 19:37:42	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: LTRANPHD$ Account Domain: WORKGROUP Logon ID: 0x3e7 Logon Type: 5 Impersonation Level: %%1833 New Logon: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Logon ID: 0x3e7 Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x238 Process Name: C:\Windows\System32\services.exe Network Information: Workstation Name: Source Network Address: - Source Port: - Detailed Authentication Information: Logon Process: Advapi Authentication Package: Negotiate Transited Services: - Package Name (NTLM only): - Key Length: 0 This event is generated when a logon session is created. It is generated on the computer that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service such as the Server service, or a local process such as Winlogon.exe or Services.exe. The logon type field indicates the kind of logon that occurred. The most common types are 2 (interactive) and 3 (network). The New Logon fields indicate the account for whom the new logon was created, i.e. the account that was logged on. The network fields indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impersonation level field indicates the extent to which a process in the logon session can impersonate. The authentication information fields provide detailed information about this specific logon request. - Logon GUID is a unique identifier that can be used to correlate this event with a KDC event. - Transited services indicate which intermediate services have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indicates the length of the generated

					session key. This will be 0 if no session key was requested.
Security	Audit Success	12544	2015-04-28 19:37:42	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: LTRANPHD$ Account Domain: WORKGROUP Logon ID: 0x3e7 Logon Type: 5 Impersonation Level: %%1833 New Logon: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Logon ID: 0x3e7 Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x238 Process Name: C:\Windows\System32\services.exe Network Information: Workstation Name: Source Network Address: - Source Port: - Detailed Authentication Information: Logon Process: Advapi Authentication Package: Negotiate Transited Services: - Package Name (NTLM only): - Key Length: 0 This event is generated when a logon session is created. It is generated on the computer that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service such as the Server service, or a local process such as Winlogon.exe or Services.exe. The logon type field indicates the kind of logon that occurred. The most common types are 2 (interactive) and 3 (network). The New Logon fields indicate the account for whom the new logon was created, i.e. the account that was logged on. The network fields indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impersonation level field indicates the extent to which a process in the logon session can impersonate. The authentication information fields provide detailed information about this specific logon request. - Logon GUID is a unique identifier that can be used to correlate this event with a KDC event. - Transited services indicate which intermediate services have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indicates the length of the generated session key. This will be 0 if no session key was requested.
Security	Audit Success	12548	2015-04-28 19:37:42	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Logon ID: 0x3e7 Privileges: SeAssignPrimaryTokenPrivilege SeTcbPrivilege SeSecurityPrivilege SeTakeOwnershipPrivilege SeLoadDriverPrivilege SeBackupPrivilege SeRestorePrivilege SeDebugPrivilege SeAuditPrivilege SeSystemEnvironmentPrivilege SeImpersonatePrivilege
Security	Audit Success	12548	2015-04-28 19:37:42	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-20 Account Name: NETWORK SERVICE Account Domain: NT AUTHORITY Logon ID: 0x3e4 Privileges: SeAssignPrimaryTokenPrivilege SeAuditPrivilege SeImpersonatePrivilege
Security	Audit Success	12548	2015-04-28 19:37:42	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-90-1 Account Name: DWM-1 Account Domain: Window Manager Logon ID: 0xe0ae Privileges: SeAssignPrimaryTokenPrivilege SeAuditPrivilege SeImpersonatePrivilege
Security	Audit Success	12548	2015-04-28 19:37:42	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-90-1 Account Name: DWM-1 Account Domain: Window Manager Logon ID: 0xe0c5 Privileges: SeAssignPrimaryTokenPrivilege SeAuditPrivilege
Security	Audit Success	12548	2015-04-28 19:37:42	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-19 Account Name: LOCAL SERVICE Account Domain: NT AUTHORITY Logon ID: 0x3e5 Privileges: SeAssignPrimaryTokenPrivilege SeAuditPrivilege SeImpersonatePrivilege
Security	Audit Success	12548	2015-04-28 19:37:42	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Logon ID: 0x3e7 Privileges: SeAssignPrimaryTokenPrivilege SeTcbPrivilege SeSecurityPrivilege SeTakeOwnershipPrivilege SeLoadDriverPrivilege SeBackupPrivilege SeRestorePrivilege SeDebugPrivilege SeAuditPrivilege SeSystemEnvironmentPrivilege SeImpersonatePrivilege
Security	Audit Success	12548	2015-04-28 19:37:42	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Logon ID: 0x3e7 Privileges: SeAssignPrimaryTokenPrivilege SeTcbPrivilege SeSecurityPrivilege SeTakeOwnershipPrivilege SeLoadDriverPrivilege SeBackupPrivilege SeRestorePrivilege SeDebugPrivilege SeAuditPrivilege SeSystemEnvironmentPrivilege SeImpersonatePrivilege
Security	Audit Success	13568	2015-04-28 19:37:42	Microsoft-Windows-Security-Auditing	4902: The Per-user audit policy table was created. Number of Elements: 0 Policy ID: 0x9033
Security	Audit Success	101	2015-04-28 19:37:43	Microsoft-Windows-Eventlog	1101: Audit events have been dropped by the transport. 0
Security	Audit Success	12292	2015-04-28 19:37:43	Microsoft-Windows-Security-Auditing	5033: The Windows Firewall Driver started successfully.
Security	Audit Success	12544	2015-04-28 19:37:43	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: LTRANPHD$ Account Domain: WORKGROUP Logon ID: 0x3e7 Logon Type: 5 Impersonation Level: %%1833 New Logon: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Logon ID: 0x3e7 Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x238 Process Name: C:\Windows\System32\services.exe Network Information: Workstation Name: Source Network Address: - Source Port: - Detailed Authentication Information: Logon Process: Advapi Authentication Package: Negotiate Transited Services: - Package Name (NTLM only): - Key Length: 0 This event is generated when a logon session is created. It is generated on the computer that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service such as the Server service, or a local process such as Winlogon.exe or Services.exe. The logon type field indicates the kind of logon that occurred. The most common types are 2 (interactive) and 3 (network). The New Logon fields indicate the account for whom the new logon was created, i.e. the account that was logged on. The network fields indicate where a

					remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impersonation level field indicates the extent to which a process in the logon session can impersonate. The authentication information fields provide detailed information about this specific logon request. - Logon GUID is a unique identifier that can be used to correlate this event with a KDC event. - Transited services indicate which intermediate services have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indicates the length of the generated session key. This will be 0 if no session key was requested.
Security	Audit Success	12548	2015-04-28 19:37:43	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Logon ID: 0x3e7 Privileges: SeAssignPrimaryTokenPrivilege SeTcbPrivilege SeSecurityPrivilege SeTakeOwnershipPrivilege SeLoadDriverPrivilege SeBackupPrivilege SeRestorePrivilege SeDebugPrivilege SeAuditPrivilege SeSystemEnvironmentPrivilege SeImpersonatePrivilege
Security	Audit Success	12292	2015-04-28 19:37:44	Microsoft-Windows-Security-Auditing	5024: The Windows Firewall service started successfully.
Security	Audit Success	12544	2015-04-28 19:37:44	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: LTRANPHD$ Account Domain: WORKGROUP Logon ID: 0x3e7 Logon Type: 5 Impersonation Level: %%1833 New Logon: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Logon ID: 0x3e7 Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x238 Process Name: C:\Windows\System32\services.exe Network Information: Workstation Name: Source Network Address: - Source Port: - Detailed Authentication Information: Logon Process: Advapi Authentication Package: Negotiate Transited Services: - Package Name (NTLM only): - Key Length: 0 This event is generated when a logon session is created. It is generated on the computer that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service such as the Server service, or a local process such as Winlogon.exe or Services.exe. The logon type field indicates the kind of logon that occurred. The most common types are 2 (interactive) and 3 (network). The New Logon fields indicate the account for whom the new logon was created, i.e. the account that was logged on. The network fields indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impersonation level field indicates the extent to which a process in the logon session can impersonate. The authentication information fields provide detailed information about this specific logon request. - Logon GUID is a unique identifier that can be used to correlate this event with a KDC event. - Transited services indicate which intermediate services have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indicates the length of the generated session key. This will be 0 if no session key was requested.
Security	Audit Success	12544	2015-04-28 19:37:44	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: LTRANPHD$ Account Domain: WORKGROUP Logon ID: 0x3e7 Logon Type: 5 Impersonation Level: %%1833 New Logon: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Logon ID: 0x3e7 Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x238 Process Name: C:\Windows\System32\services.exe Network Information: Workstation Name: Source Network Address: - Source Port: - Detailed Authentication Information: Logon Process: Advapi Authentication Package: Negotiate Transited Services: - Package Name (NTLM only): - Key Length: 0 This event is generated when a logon session is created. It is generated on the computer that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service such as the Server service, or a local process such as Winlogon.exe or Services.exe. The logon type field indicates the kind of logon that occurred. The most common types are 2 (interactive) and 3 (network). The New Logon fields indicate the account for whom the new logon was created, i.e. the account that was logged on. The network fields indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impersonation level field indicates the extent to which a process in the logon session can impersonate. The authentication information fields provide detailed information about this specific logon request. - Logon GUID is a unique identifier that can be used to correlate this event with a KDC event. - Transited services indicate which intermediate services have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indicates the length of the generated session key. This will be 0 if no session key was requested.
Security	Audit Success	12544	2015-04-28 19:37:44	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-0-0 Account Name: - Account Domain: - Logon ID: 0x0 Logon Type: 3 Impersonation Level: %%1833 New Logon: Security ID: S-1-5-7 Account Name: ANONYMOUS LOGON Account Domain: NT AUTHORITY Logon ID: 0x19ca7 Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x0 Process Name: - Network Information: Workstation Name: Source Network Address: - Source Port: - Detailed Authentication Information: Logon Process: NtLmSsp Authentication Package: NTLM Transited Services: - Package Name (NTLM only): NTLM V1 Key Length: 0 This event is generated when a logon session is created. It is generated on the computer that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service such as the Server service, or a local process such as Winlogon.exe or Services.exe. The logon type field indicates the kind of logon that occurred. The most common types are 2 (interactive) and 3 (network). The New Logon fields indicate the account for whom the new logon was created, i.e. the account that was logged on. The network fields indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impersonation level field indicates the extent to which a process in the logon session can impersonate. The authentication information fields provide detailed

					information about this specific logon request. - Logon GUID is a unique identifier that can be used to correlate this event with a KDC event. - Transited services indicate which intermediate services have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indicates the length of the generated session key. This will be 0 if no session key was requested.
Security	Audit Success	12548	2015-04-28 19:37:44	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Logon ID: 0x3e7 Privileges: SeAssignPrimaryTokenPrivilege SeTcbPrivilege SeSecurityPrivilege SeTakeOwnershipPrivilege SeLoadDriverPrivilege SeBackupPrivilege SeRestorePrivilege SeDebugPrivilege SeAuditPrivilege SeSystemEnvironmentPrivilege SeImpersonatePrivilege
Security	Audit Success	12548	2015-04-28 19:37:44	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Logon ID: 0x3e7 Privileges: SeAssignPrimaryTokenPrivilege SeTcbPrivilege SeSecurityPrivilege SeTakeOwnershipPrivilege SeLoadDriverPrivilege SeBackupPrivilege SeRestorePrivilege SeDebugPrivilege SeAuditPrivilege SeSystemEnvironmentPrivilege SeImpersonatePrivilege
Security	Audit Success	12544	2015-04-28 19:37:45	Microsoft-Windows-Security-Auditing	4648: A logon was attempted using explicit credentials. Subject: Security ID: S-1-5-18 Account Name: LTRANPHD$ Account Domain: WORKGROUP Logon ID: 0x3e7 Logon GUID: {00000000-0000-0000-0000-000000000000} Account Whose Credentials Were Used: Account Name: Liem Account Domain: LTRANPHD Logon GUID: {00000000-0000-0000-0000-000000000000} Target Server: Target Server Name: localhost Additional Information: localhost Process Information: Process ID: 0x210 Process Name: C:\Windows\System32\winlogon.exe Network Information: Network Address: 127.0.0.1 Port: 0 This event is generated when a process attempts to log on an account by explicitly specifying that account's credentials. This most commonly occurs in batch-type configurations such as scheduled tasks, or when using the RUNAS command.
Security	Audit Success	12544	2015-04-28 19:37:45	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: LTRANPHD$ Account Domain: WORKGROUP Logon ID: 0x3e7 Logon Type: 2 Impersonation Level: %%1833 New Logon: Security ID: S-1-5-21-1888849264-3803429180-4108621888-1001 Account Name: Liem Account Domain: LTRANPHD Logon ID: 0x1ba10 Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x210 Process Name: C:\Windows\System32\winlogon.exe Network Information: Workstation Name: LTRANPHD Source Network Address: 127.0.0.1 Source Port: 0 Detailed Authentication Information: Logon Process: User32 Authentication Package: Negotiate Transited Services: - Package Name (NTLM only): - Key Length: 0 This event is generated when a logon session is created. It is generated on the computer that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service such as the Server service, or a local process such as Winlogon.exe or Services.exe. The logon type field indicates the kind of logon that occurred. The most common types are 2 (interactive) and 3 (network). The New Logon fields indicate the account for whom the new logon was created, i.e. the account that was logged on. The network fields indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impersonation level field indicates the extent to which a process in the logon session can impersonate. The authentication information fields provide detailed information about this specific logon request. - Logon GUID is a unique identifier that can be used to correlate this event with a KDC event. - Transited services indicate which intermediate services have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indicates the length of the generated session key. This will be 0 if no session key was requested.
Security	Audit Success	12544	2015-04-28 19:37:45	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: LTRANPHD$ Account Domain: WORKGROUP Logon ID: 0x3e7 Logon Type: 2 Impersonation Level: %%1833 New Logon: Security ID: S-1-5-21-1888849264-3803429180-4108621888-1001 Account Name: Liem Account Domain: LTRANPHD Logon ID: 0x1ba43 Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x210 Process Name: C:\Windows\System32\winlogon.exe Network Information: Workstation Name: LTRANPHD Source Network Address: 127.0.0.1 Source Port: 0 Detailed Authentication Information: Logon Process: User32 Authentication Package: Negotiate Transited Services: - Package Name (NTLM only): - Key Length: 0 This event is generated when a logon session is created. It is generated on the computer that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service such as the Server service, or a local process such as Winlogon.exe or Services.exe. The logon type field indicates the kind of logon that occurred. The most common types are 2 (interactive) and 3 (network). The New Logon fields indicate the account for whom the new logon was created, i.e. the account that was logged on. The network fields indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impersonation level field indicates the extent to which a process in the logon session can impersonate. The authentication information fields provide detailed information about this specific logon request. - Logon GUID is a unique identifier that can be used to correlate this event with a KDC event. - Transited services indicate which intermediate services have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indicates the length of the generated session key. This will be 0 if no session key was requested.
Security	Audit Success	12548	2015-04-28 19:37:45	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-21-1888849264-3803429180-4108621888-1001 Account Name: Liem Account Domain: LTRANPHD Logon ID: 0x1ba10 Privileges: SeSecurityPrivilege SeTakeOwnershipPrivilege SeLoadDriverPrivilege SeBackupPrivilege SeRestorePrivilege SeDebugPrivilege SeSystemEnvironmentPrivilege SeImpersonatePrivilege
					4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: LTRANPHD$ Account Domain: WORKGROUP Logon ID: 0x3e7 Logon Type: 5 Impersonation Level: %%1833 New Logon: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Logon ID: 0x3e7 Logon GUID:

Security	Audit Success	12544	2015-04-28 19:37:46	Microsoft-Windows-Security-Auditing	{00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x238 Process Name: C:\Windows\System32\services.exe Network Information: Workstation Name: Source Network Address: - Source Port: - Detailed Authentication Information: Logon Process: Advapi Authentication Package: Negotiate Transited Services: - Package Name (NTLM only): - Key Length: 0 This event is generated when a logon session is created. It is generated on the computer that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service such as the Server service, or a local process such as Winlogon.exe or Services.exe. The logon type field indicates the kind of logon that occurred. The most common types are 2 (interactive) and 3 (network). The New Logon fields indicate the account for whom the new logon was created, i.e. the account that was logged on. The network fields indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impersonation level field indicates the extent to which a process in the logon session can impersonate. The authentication information fields provide detailed information about this specific logon request. - Logon GUID is a unique identifier that can be used to correlate this event with a KDC event. - Transited services indicate which intermediate services have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indicates the length of the generated session key. This will be 0 if no session key was requested.
Security	Audit Success	12548	2015-04-28 19:37:46	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Logon ID: 0x3e7 Privileges: SeAssignPrimaryTokenPrivilege SeTcbPrivilege SeSecurityPrivilege SeTakeOwnershipPrivilege SeLoadDriverPrivilege SeBackupPrivilege SeRestorePrivilege SeDebugPrivilege SeAuditPrivilege SeSystemEnvironmentPrivilege SeImpersonatePrivilege
Security	Audit Success	13824	2015-04-28 19:37:48	Microsoft-Windows-Security-Auditing	4797: An attempt was made to query the existence of a blank password for an account. Subject: Security ID: S-1-5-21-1888849264-3803429180-4108621888-1001 Account Name: Liem Account Domain: LTRANPHD Logon ID: 0x1ba43 Additional Information: Caller Workstation: LTRANPHD Target Account Name: Administrator Target Account Domain: LTRANPHD
Security	Audit Success	13824	2015-04-28 19:37:48	Microsoft-Windows-Security-Auditing	4797: An attempt was made to query the existence of a blank password for an account. Subject: Security ID: S-1-5-21-1888849264-3803429180-4108621888-1001 Account Name: Liem Account Domain: LTRANPHD Logon ID: 0x1ba43 Additional Information: Caller Workstation: LTRANPHD Target Account Name: Guest Target Account Domain: LTRANPHD
Security	Audit Success	13824	2015-04-28 19:37:48	Microsoft-Windows-Security-Auditing	4797: An attempt was made to query the existence of a blank password for an account. Subject: Security ID: S-1-5-21-1888849264-3803429180-4108621888-1001 Account Name: Liem Account Domain: LTRANPHD Logon ID: 0x1ba43 Additional Information: Caller Workstation: LTRANPHD Target Account Name: Administrator Target Account Domain: LTRANPHD
Security	Audit Success	13824	2015-04-28 19:37:48	Microsoft-Windows-Security-Auditing	4797: An attempt was made to query the existence of a blank password for an account. Subject: Security ID: S-1-5-21-1888849264-3803429180-4108621888-1001 Account Name: Liem Account Domain: LTRANPHD Logon ID: 0x1ba43 Additional Information: Caller Workstation: LTRANPHD Target Account Name: Guest Target Account Domain: LTRANPHD
Security	Audit Success	13824	2015-04-28 19:37:55	Microsoft-Windows-Security-Auditing	4797: An attempt was made to query the existence of a blank password for an account. Subject: Security ID: S-1-5-19 Account Name: LOCAL SERVICE Account Domain: NT AUTHORITY Logon ID: 0x3e5 Additional Information: Caller Workstation: LTRANPHD Target Account Name: Administrator Target Account Domain: LTRANPHD
Security	Audit Success	13824	2015-04-28 19:37:55	Microsoft-Windows-Security-Auditing	4797: An attempt was made to query the existence of a blank password for an account. Subject: Security ID: S-1-5-19 Account Name: LOCAL SERVICE Account Domain: NT AUTHORITY Logon ID: 0x3e5 Additional Information: Caller Workstation: LTRANPHD Target Account Name: Guest Target Account Domain: LTRANPHD
Security	Audit Success	13824	2015-04-28 19:37:55	Microsoft-Windows-Security-Auditing	4797: An attempt was made to query the existence of a blank password for an account. Subject: Security ID: S-1-5-19 Account Name: LOCAL SERVICE Account Domain: NT AUTHORITY Logon ID: 0x3e5 Additional Information: Caller Workstation: LTRANPHD Target Account Name: Liem Target Account Domain: LTRANPHD
Security	Audit Success	13824	2015-04-28 19:37:55	Microsoft-Windows-Security-Auditing	4797: An attempt was made to query the existence of a blank password for an account. Subject: Security ID: S-1-5-19 Account Name: LOCAL SERVICE Account Domain: NT AUTHORITY Logon ID: 0x3e5 Additional Information: Caller Workstation: LTRANPHD Target Account Name: Liem Target Account Domain: LTRANPHD
Security	Audit Success	12544	2015-04-28 19:38:10	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: LTRANPHD$ Account Domain: WORKGROUP Logon ID: 0x3e7 Logon Type: 5 Impersonation Level: %%1833 New Logon: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Logon ID: 0x3e7 Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x238 Process Name: C:\Windows\System32\services.exe Network Information: Workstation Name: Source Network Address: - Source Port: - Detailed Authentication Information: Logon Process: Advapi Authentication Package: Negotiate Transited Services: - Package Name (NTLM only): - Key Length: 0 This event is generated when a logon session is created. It is generated on the computer that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service such as the Server service, or a local process such as Winlogon.exe or Services.exe. The logon type field indicates the kind of logon that occurred. The most common types are 2 (interactive) and 3 (network). The New Logon fields indicate the account for whom the new logon was created, i.e. the account that was logged on. The network fields indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impersonation level field indicates the extent to which a process in the logon session can impersonate. The authentication information fields provide detailed information about this specific logon request. - Logon GUID is a unique identifier that can be used to correlate this event with a KDC event. - Transited

					services indicate which intermediate services have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indicates the length of the generated session key. This will be 0 if no session key was requested.
Security	Audit Success	12548	2015-04-28 19:38:10	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Logon ID: 0x3e7 Privileges: SeAssignPrimaryTokenPrivilege SeTcbPrivilege SeSecurityPrivilege SeTakeOwnershipPrivilege SeLoadDriverPrivilege SeBackupPrivilege SeRestorePrivilege SeDebugPrivilege SeAuditPrivilege SeSystemEnvironmentPrivilege SeImpersonatePrivilege
Security	Audit Success	12544	2015-04-28 19:38:12	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: LTRANPHD$ Account Domain: WORKGROUP Logon ID: 0x3e7 Logon Type: 5 Impersonation Level: %%1833 New Logon: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Logon ID: 0x3e7 Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x238 Process Name: C:\Windows\System32\services.exe Network Information: Workstation Name: Source Network Address: - Source Port: - Detailed Authentication Information: Logon Process: Advapi Authentication Package: Negotiate Transited Services: - Package Name (NTLM only): - Key Length: 0 This event is generated when a logon session is created. It is generated on the computer that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service such as the Server service, or a local process such as Winlogon.exe or Services.exe. The logon type field indicates the kind of logon that occurred. The most common types are 2 (interactive) and 3 (network). The New Logon fields indicate the account for whom the new logon was created, i.e. the account that was logged on. The network fields indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impersonation level field indicates the extent to which a process in the logon session can impersonate. The authentication information fields provide detailed information about this specific logon request. - Logon GUID is a unique identifier that can be used to correlate this event with a KDC event. - Transited services indicate which intermediate services have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indicates the length of the generated session key. This will be 0 if no session key was requested.
Security	Audit Success	12548	2015-04-28 19:38:12	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Logon ID: 0x3e7 Privileges: SeAssignPrimaryTokenPrivilege SeTcbPrivilege SeSecurityPrivilege SeTakeOwnershipPrivilege SeLoadDriverPrivilege SeBackupPrivilege SeRestorePrivilege SeDebugPrivilege SeAuditPrivilege SeSystemEnvironmentPrivilege SeImpersonatePrivilege
Security	Audit Success	12288	2015-04-28 20:15:22	Microsoft-Windows-Security-Auditing	4608: Windows is starting up. This event is logged when LSASS.EXE starts and the auditing subsystem is initialized.
Security	Audit Success	12544	2015-04-28 20:15:22	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-0-0 Account Name: - Account Domain: - Logon ID: 0x0 Logon Type: 0 Impersonation Level: - New Logon: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Logon ID: 0x3e7 Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x4 Process Name: Network Information: Workstation Name: - Source Network Address: - Source Port: - Detailed Authentication Information: Logon Process: - Authentication Package: - Transited Services: - Package Name (NTLM only): - Key Length: 0 This event is generated when a logon session is created. It is generated on the computer that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service such as the Server service, or a local process such as Winlogon.exe or Services.exe. The logon type field indicates the kind of logon that occurred. The most common types are 2 (interactive) and 3 (network). The New Logon fields indicate the account for whom the new logon was created, i.e. the account that was logged on. The network fields indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impersonation level field indicates the extent to which a process in the logon session can impersonate. The authentication information fields provide detailed information about this specific logon request. - Logon GUID is a unique identifier that can be used to correlate this event with a KDC event. - Transited services indicate which intermediate services have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indicates the length of the generated session key. This will be 0 if no session key was requested.
Security	Audit Success	12544	2015-04-28 20:15:22	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: LTRANPHD$ Account Domain: WORKGROUP Logon ID: 0x3e7 Logon Type: 5 Impersonation Level: %%1833 New Logon: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Logon ID: 0x3e7 Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x23c Process Name: C:\Windows\System32\services.exe Network Information: Workstation Name: Source Network Address: - Source Port: - Detailed Authentication Information: Logon Process: Advapi Authentication Package: Negotiate Transited Services: - Package Name (NTLM only): - Key Length: 0 This event is generated when a logon session is created. It is generated on the computer that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service such as the Server service, or a local process such as Winlogon.exe or Services.exe. The logon type field indicates the kind of logon that occurred. The most common types are 2 (interactive) and 3 (network). The New Logon fields indicate the account for whom the new logon was created, i.e. the account that was logged on. The network fields indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impersonation level field indicates the extent to which a process in the logon session can impersonate. The authentication information fields provide detailed information about this specific logon request.

					- Logon GUID is a unique identifier that can be used to correlate this event with a KDC event. - Transited services indicate which intermediate services have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indicates the length of the generated session key. This will be 0 if no session key was requested.
Security	Audit Success	12544	2015-04-28 20:15:22	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: LTRANPHD$ Account Domain: WORKGROUP Logon ID: 0x3e7 Logon Type: 5 Impersonation Level: %%1833 New Logon: Security ID: S-1-5-20 Account Name: NETWORK SERVICE Account Domain: NT AUTHORITY Logon ID: 0x3e4 Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x23c Process Name: C:\Windows\System32\services.exe Network Information: Workstation Name: Source Network Address: - Source Port: - Detailed Authentication Information: Logon Process: Advapi Authentication Package: Negotiate Transited Services: - Package Name (NTLM only): - Key Length: 0 This event is generated when a logon session is created. It is generated on the computer that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service such as the Server service, or a local process such as Winlogon.exe or Services.exe. The logon type field indicates the kind of logon that occurred. The most common types are 2 (interactive) and 3 (network). The New Logon fields indicate the account for whom the new logon was created, i.e. the account that was logged on. The network fields indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impersonation level field indicates the extent to which a process in the logon session can impersonate. The authentication information fields provide detailed information about this specific logon request. - Logon GUID is a unique identifier that can be used to correlate this event with a KDC event. - Transited services indicate which intermediate services have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indicates the length of the generated session key. This will be 0 if no session key was requested.
Security	Audit Success	12544	2015-04-28 20:15:22	Microsoft-Windows-Security-Auditing	4648: A logon was attempted using explicit credentials. Subject: Security ID: S-1-5-18 Account Name: LTRANPHD$ Account Domain: WORKGROUP Logon ID: 0x3e7 Logon GUID: {00000000-0000-0000-0000-000000000000} Account Whose Credentials Were Used: Account Name: DWM-1 Account Domain: Window Manager Logon GUID: {00000000-0000-0000-0000-000000000000} Target Server: Target Server Name: localhost Additional Information: localhost Process Information: Process ID: 0x20c Process Name: C:\Windows\System32\winlogon.exe Network Information: Network Address: - Port: - This event is generated when a process attempts to log on an account by explicitly specifying that account's credentials. This most commonly occurs in batch-type configurations such as scheduled tasks, or when using the RUNAS command.
Security	Audit Success	12544	2015-04-28 20:15:22	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: LTRANPHD$ Account Domain: WORKGROUP Logon ID: 0x3e7 Logon Type: 2 Impersonation Level: %%1833 New Logon: Security ID: S-1-5-90-1 Account Name: DWM-1 Account Domain: Window Manager Logon ID: 0xd4f9 Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x20c Process Name: C:\Windows\System32\winlogon.exe Network Information: Workstation Name: Source Network Address: - Source Port: - Detailed Authentication Information: Logon Process: Advapi Authentication Package: Negotiate Transited Services: - Package Name (NTLM only): - Key Length: 0 This event is generated when a logon session is created. It is generated on the computer that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service such as the Server service, or a local process such as Winlogon.exe or Services.exe. The logon type field indicates the kind of logon that occurred. The most common types are 2 (interactive) and 3 (network). The New Logon fields indicate the account for whom the new logon was created, i.e. the account that was logged on. The network fields indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impersonation level field indicates the extent to which a process in the logon session can impersonate. The authentication information fields provide detailed information about this specific logon request. - Logon GUID is a unique identifier that can be used to correlate this event with a KDC event. - Transited services indicate which intermediate services have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indicates the length of the generated session key. This will be 0 if no session key was requested.
Security	Audit Success	12544	2015-04-28 20:15:22	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: LTRANPHD$ Account Domain: WORKGROUP Logon ID: 0x3e7 Logon Type: 2 Impersonation Level: %%1833 New Logon: Security ID: S-1-5-90-1 Account Name: DWM-1 Account Domain: Window Manager Logon ID: 0xd522 Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x20c Process Name: C:\Windows\System32\winlogon.exe Network Information: Workstation Name: Source Network Address: - Source Port: - Detailed Authentication Information: Logon Process: Advapi Authentication Package: Negotiate Transited Services: - Package Name (NTLM only): - Key Length: 0 This event is generated when a logon session is created. It is generated on the computer that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service such as the Server service, or a local process such as Winlogon.exe or Services.exe. The logon type field indicates the kind of logon that occurred. The most common types are 2 (interactive) and 3 (network). The New Logon fields indicate the account for whom the new logon was created, i.e. the account that was logged on. The network fields indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impersonation level field indicates the extent to which a process in the logon session can impersonate. The authentication information fields provide detailed information about this specific logon request. - Logon GUID is a unique identifier that can be used to correlate this event with a KDC event. - Transited services indicate which intermediate services have participated in this logon request. - Package name indicates

					which sub-protocol was used among the NTLM protocols. - Key length indicates the length of the generated session key. This will be 0 if no session key was requested.
Security	Audit Success	12544	2015-04-28 20:15:22	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: LTRANPHD$ Account Domain: WORKGROUP Logon ID: 0x3e7 Logon Type: 5 Impersonation Level: %%1833 New Logon: Security ID: S-1-5-19 Account Name: LOCAL SERVICE Account Domain: NT AUTHORITY Logon ID: 0x3e5 Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x23c Process Name: C:\Windows\System32\services.exe Network Information: Workstation Name: Source Network Address: - Source Port: - Detailed Authentication Information: Logon Process: Advapi Authentication Package: Negotiate Transited Services: - Package Name (NTLM only): - Key Length: 0 This event is generated when a logon session is created. It is generated on the computer that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service such as the Server service, or a local process such as Winlogon.exe or Services.exe. The logon type field indicates the kind of logon that occurred. The most common types are 2 (interactive) and 3 (network). The New Logon fields indicate the account for whom the new logon was created, i.e. the account that was logged on. The network fields indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impersonation level field indicates the extent to which a process in the logon session can impersonate. The authentication information fields provide detailed information about this specific logon request. - Logon GUID is a unique identifier that can be used to correlate this event with a KDC event. - Transited services indicate which intermediate services have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indicates the length of the generated session key. This will be 0 if no session key was requested.
Security	Audit Success	12544	2015-04-28 20:15:22	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: LTRANPHD$ Account Domain: WORKGROUP Logon ID: 0x3e7 Logon Type: 5 Impersonation Level: %%1833 New Logon: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Logon ID: 0x3e7 Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x23c Process Name: C:\Windows\System32\services.exe Network Information: Workstation Name: Source Network Address: - Source Port: - Detailed Authentication Information: Logon Process: Advapi Authentication Package: Negotiate Transited Services: - Package Name (NTLM only): - Key Length: 0 This event is generated when a logon session is created. It is generated on the computer that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service such as the Server service, or a local process such as Winlogon.exe or Services.exe. The logon type field indicates the kind of logon that occurred. The most common types are 2 (interactive) and 3 (network). The New Logon fields indicate the account for whom the new logon was created, i.e. the account that was logged on. The network fields indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impersonation level field indicates the extent to which a process in the logon session can impersonate. The authentication information fields provide detailed information about this specific logon request. - Logon GUID is a unique identifier that can be used to correlate this event with a KDC event. - Transited services indicate which intermediate services have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indicates the length of the generated session key. This will be 0 if no session key was requested.
Security	Audit Success	12544	2015-04-28 20:15:22	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: LTRANPHD$ Account Domain: WORKGROUP Logon ID: 0x3e7 Logon Type: 5 Impersonation Level: %%1833 New Logon: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Logon ID: 0x3e7 Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x23c Process Name: C:\Windows\System32\services.exe Network Information: Workstation Name: Source Network Address: - Source Port: - Detailed Authentication Information: Logon Process: Advapi Authentication Package: Negotiate Transited Services: - Package Name (NTLM only): - Key Length: 0 This event is generated when a logon session is created. It is generated on the computer that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service such as the Server service, or a local process such as Winlogon.exe or Services.exe. The logon type field indicates the kind of logon that occurred. The most common types are 2 (interactive) and 3 (network). The New Logon fields indicate the account for whom the new logon was created, i.e. the account that was logged on. The network fields indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impersonation level field indicates the extent to which a process in the logon session can impersonate. The authentication information fields provide detailed information about this specific logon request. - Logon GUID is a unique identifier that can be used to correlate this event with a KDC event. - Transited services indicate which intermediate services have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indicates the length of the generated session key. This will be 0 if no session key was requested.
Security	Audit Success	12548	2015-04-28 20:15:22	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Logon ID: 0x3e7 Privileges: SeAssignPrimaryTokenPrivilege SeTcbPrivilege SeSecurityPrivilege SeTakeOwnershipPrivilege SeLoadDriverPrivilege SeBackupPrivilege SeRestorePrivilege SeDebugPrivilege SeAuditPrivilege SeSystemEnvironmentPrivilege SeImpersonatePrivilege
Security	Audit Success	12548	2015-04-28 20:15:22	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-20 Account Name: NETWORK SERVICE Account Domain: NT AUTHORITY Logon ID: 0x3e4 Privileges: SeAssignPrimaryTokenPrivilege SeAuditPrivilege SeImpersonatePrivilege

Security	Audit Success	12548	2015-04-28 20:15:22	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-90-1 Account Name: DWM-1 Account Domain: Window Manager Logon ID: 0xd4f9 Privileges: SeAssignPrimaryTokenPrivilege SeAuditPrivilege SeImpersonatePrivilege
Security	Audit Success	12548	2015-04-28 20:15:22	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-90-1 Account Name: DWM-1 Account Domain: Window Manager Logon ID: 0xd522 Privileges: SeAssignPrimaryTokenPrivilege SeAuditPrivilege
Security	Audit Success	12548	2015-04-28 20:15:22	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-19 Account Name: LOCAL SERVICE Account Domain: NT AUTHORITY Logon ID: 0x3e5 Privileges: SeAssignPrimaryTokenPrivilege SeAuditPrivilege SeImpersonatePrivilege
Security	Audit Success	12548	2015-04-28 20:15:22	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Logon ID: 0x3e7 Privileges: SeAssignPrimaryTokenPrivilege SeTcbPrivilege SeSecurityPrivilege SeTakeOwnershipPrivilege SeLoadDriverPrivilege SeBackupPrivilege SeRestorePrivilege SeDebugPrivilege SeAuditPrivilege SeSystemEnvironmentPrivilege SeImpersonatePrivilege
Security	Audit Success	12548	2015-04-28 20:15:22	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Logon ID: 0x3e7 Privileges: SeAssignPrimaryTokenPrivilege SeTcbPrivilege SeSecurityPrivilege SeTakeOwnershipPrivilege SeLoadDriverPrivilege SeBackupPrivilege SeRestorePrivilege SeDebugPrivilege SeAuditPrivilege SeSystemEnvironmentPrivilege SeImpersonatePrivilege
Security	Audit Success	13568	2015-04-28 20:15:22	Microsoft-Windows-Security-Auditing	4902: The Per-user audit policy table was created. Number of Elements: 0 Policy ID: 0x861a
Security	Audit Success	101	2015-04-28 20:15:23	Microsoft-Windows-Eventlog	1101: Audit events have been dropped by the transport. 0
Security	Audit Success	12292	2015-04-28 20:15:23	Microsoft-Windows-Security-Auditing	5033: The Windows Firewall Driver started successfully.
Security	Audit Success	12292	2015-04-28 20:15:23	Microsoft-Windows-Security-Auditing	5024: The Windows Firewall service started successfully.
Security	Audit Success	12544	2015-04-28 20:15:23	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: LTRANPHD$ Account Domain: WORKGROUP Logon ID: 0x3e7 Logon Type: 5 Impersonation Level: %%1833 New Logon: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Logon ID: 0x3e7 Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x23c Process Name: C:\Windows\System32\services.exe Network Information: Workstation Name: Source Network Address: - Source Port: - Detailed Authentication Information: Logon Process: Advapi Authentication Package: Negotiate Transited Services: - Package Name (NTLM only): - Key Length: 0 This event is generated when a logon session is created. It is generated on the computer that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service such as the Server service, or a local process such as Winlogon.exe or Services.exe. The logon type field indicates the kind of logon that occurred. The most common types are 2 (interactive) and 3 (network). The New Logon fields indicate the account for whom the new logon was created, i.e. the account that was logged on. The network fields indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impersonation level field indicates the extent to which a process in the logon session can impersonate. The authentication information fields provide detailed information about this specific logon request. - Logon GUID is a unique identifier that can be used to correlate this event with a KDC event. - Transited services indicate which intermediate services have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indicates the length of the generated session key. This will be 0 if no session key was requested.
Security	Audit Success	12544	2015-04-28 20:15:23	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: LTRANPHD$ Account Domain: WORKGROUP Logon ID: 0x3e7 Logon Type: 5 Impersonation Level: %%1833 New Logon: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Logon ID: 0x3e7 Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x23c Process Name: C:\Windows\System32\services.exe Network Information: Workstation Name: Source Network Address: - Source Port: - Detailed Authentication Information: Logon Process: Advapi Authentication Package: Negotiate Transited Services: - Package Name (NTLM only): - Key Length: 0 This event is generated when a logon session is created. It is generated on the computer that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service such as the Server service, or a local process such as Winlogon.exe or Services.exe. The logon type field indicates the kind of logon that occurred. The most common types are 2 (interactive) and 3 (network). The New Logon fields indicate the account for whom the new logon was created, i.e. the account that was logged on. The network fields indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impersonation level field indicates the extent to which a process in the logon session can impersonate. The authentication information fields provide detailed information about this specific logon request. - Logon GUID is a unique identifier that can be used to correlate this event with a KDC event. - Transited services indicate which intermediate services have participated in this logon request. - Package name indicates

					which sub-protocol was used among the NTLM protocols. - Key length indicates the length of the generated session key. This will be 0 if no session key was requested.
Security	Audit Success	12544	2015-04-28 20:15:23	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: LTRANPHD$ Account Domain: WORKGROUP Logon ID: 0x3e7 Logon Type: 5 Impersonation Level: %%1833 New Logon: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Logon ID: 0x3e7 Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x23c Process Name: C:\Windows\System32\services.exe Network Information: Workstation Name: Source Network Address: - Source Port: - Detailed Authentication Information: Logon Process: Advapi Authentication Package: Negotiate Transited Services: - Package Name (NTLM only): - Key Length: 0 This event is generated when a logon session is created. It is generated on the computer that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service such as the Server service, or a local process such as Winlogon.exe or Services.exe. The logon type field indicates the kind of logon that occurred. The most common types are 2 (interactive) and 3 (network). The New Logon fields indicate the account for whom the new logon was created, i.e. the account that was logged on. The network fields indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impersonation level field indicates the extent to which a process in the logon session can impersonate. The authentication information fields provide detailed information about this specific logon request. - Logon GUID is a unique identifier that can be used to correlate this event with a KDC event. - Transited services indicate which intermediate services have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indicates the length of the generated session key. This will be 0 if no session key was requested.
Security	Audit Success	12544	2015-04-28 20:15:23	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-0-0 Account Name: - Account Domain: - Logon ID: 0x0 Logon Type: 3 Impersonation Level: %%1833 New Logon: Security ID: S-1-5-7 Account Name: ANONYMOUS LOGON Account Domain: NT AUTHORITY Logon ID: 0x18d2d Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x0 Process Name: - Network Information: Workstation Name: Source Network Address: - Source Port: - Detailed Authentication Information: Logon Process: NtLmSsp Authentication Package: NTLM Transited Services: - Package Name (NTLM only): NTLM V1 Key Length: 0 This event is generated when a logon session is created. It is generated on the computer that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service such as the Server service, or a local process such as Winlogon.exe or Services.exe. The logon type field indicates the kind of logon that occurred. The most common types are 2 (interactive) and 3 (network). The New Logon fields indicate the account for whom the new logon was created, i.e. the account that was logged on. The network fields indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impersonation level field indicates the extent to which a process in the logon session can impersonate. The authentication information fields provide detailed information about this specific logon request. - Logon GUID is a unique identifier that can be used to correlate this event with a KDC event. - Transited services indicate which intermediate services have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indicates the length of the generated session key. This will be 0 if no session key was requested.
Security	Audit Success	12548	2015-04-28 20:15:23	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Logon ID: 0x3e7 Privileges: SeAssignPrimaryTokenPrivilege SeTcbPrivilege SeSecurityPrivilege SeTakeOwnershipPrivilege SeLoadDriverPrivilege SeBackupPrivilege SeRestorePrivilege SeDebugPrivilege SeAuditPrivilege SeSystemEnvironmentPrivilege SeImpersonatePrivilege
Security	Audit Success	12548	2015-04-28 20:15:23	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Logon ID: 0x3e7 Privileges: SeAssignPrimaryTokenPrivilege SeTcbPrivilege SeSecurityPrivilege SeTakeOwnershipPrivilege SeLoadDriverPrivilege SeBackupPrivilege SeRestorePrivilege SeDebugPrivilege SeAuditPrivilege SeSystemEnvironmentPrivilege SeImpersonatePrivilege
Security	Audit Success	12548	2015-04-28 20:15:23	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Logon ID: 0x3e7 Privileges: SeAssignPrimaryTokenPrivilege SeTcbPrivilege SeSecurityPrivilege SeTakeOwnershipPrivilege SeLoadDriverPrivilege SeBackupPrivilege SeRestorePrivilege SeDebugPrivilege SeAuditPrivilege SeSystemEnvironmentPrivilege SeImpersonatePrivilege
Security	Audit Success	12544	2015-04-28 20:15:29	Microsoft-Windows-Security-Auditing	4648: A logon was attempted using explicit credentials. Subject: Security ID: S-1-5-18 Account Name: LTRANPHD$ Account Domain: WORKGROUP Logon ID: 0x3e7 Logon GUID: {00000000-0000-0000-0000-000000000000} Account Whose Credentials Were Used: Account Name: Liem Account Domain: LTRANPHD Logon GUID: {00000000-0000-0000-0000-000000000000} Target Server: Target Server Name: localhost Additional Information: localhost Process Information: Process ID: 0x20c Process Name: C:\Windows\System32\winlogon.exe Network Information: Network Address: 127.0.0.1 Port: 0 This event is generated when a process attempts to log on an account by explicitly specifying that account's credentials. This most commonly occurs in batch-type configurations such as scheduled tasks, or when using the RUNAS command.
					4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: LTRANPHD$ Account Domain: WORKGROUP Logon ID: 0x3e7 Logon Type: 2 Impersonation Level: %%1833 New Logon: Security ID: S-1-5-21-1888849264-3803429180-4108621888-1001 Account Name: Liem Account Domain: LTRANPHD Logon ID: 0x1f487 Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x20c Process Name: C:\Windows\System32\winlogon.exe Network Information: Workstation Name: LTRANPHD Source Network Address: 127.0.0.1 Source Port: 0 Detailed Authentication Information:

	Security	Audit Success	12544	2015-04-28 20:15:29	Microsoft-Windows-Security-Auditing	Logon Process: User32 Authentication Package: Negotiate Transited Services: - Package Name (NTLM only): - Key Length: 0 This event is generated when a logon session is created. It is generated on the computer that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service such as the Server service, or a local process such as Winlogon.exe or Services.exe. The logon type field indicates the kind of logon that occurred. The most common types are 2 (interactive) and 3 (network). The New Logon fields indicate the account for whom the new logon was created, i.e. the account that was logged on. The network fields indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impersonation level field indicates the extent to which a process in the logon session can impersonate. The authentication information fields provide detailed information about this specific logon request. - Logon GUID is a unique identifier that can be used to correlate this event with a KDC event. - Transited services indicate which intermediate services have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indicates the length of the generated session key. This will be 0 if no session key was requested.
	Security	Audit Success	12544	2015-04-28 20:15:29	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: LTRANPHD$ Account Domain: WORKGROUP Logon ID: 0x3e7 Logon Type: 2 Impersonation Level: %%1833 New Logon: Security ID: S-1-5-21-1888849264-3803429180-4108621888-1001 Account Name: Liem Account Domain: LTRANPHD Logon ID: 0x1f4eb Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x20c Process Name: C:\Windows\System32\winlogon.exe Network Information: Workstation Name: LTRANPHD Source Network Address: 127.0.0.1 Source Port: 0 Detailed Authentication Information: Logon Process: User32 Authentication Package: Negotiate Transited Services: - Package Name (NTLM only): - Key Length: 0 This event is generated when a logon session is created. It is generated on the computer that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service such as the Server service, or a local process such as Winlogon.exe or Services.exe. The logon type field indicates the kind of logon that occurred. The most common types are 2 (interactive) and 3 (network). The New Logon fields indicate the account for whom the new logon was created, i.e. the account that was logged on. The network fields indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impersonation level field indicates the extent to which a process in the logon session can impersonate. The authentication information fields provide detailed information about this specific logon request. - Logon GUID is a unique identifier that can be used to correlate this event with a KDC event. - Transited services indicate which intermediate services have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indicates the length of the generated session key. This will be 0 if no session key was requested.
	Security	Audit Success	12548	2015-04-28 20:15:29	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-21-1888849264-3803429180-4108621888-1001 Account Name: Liem Account Domain: LTRANPHD Logon ID: 0x1f487 Privileges: SeSecurityPrivilege SeTakeOwnershipPrivilege SeLoadDriverPrivilege SeBackupPrivilege SeRestorePrivilege SeDebugPrivilege SeSystemEnvironmentPrivilege SeImpersonatePrivilege
	Security	Audit Success	12544	2015-04-28 20:15:30	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: LTRANPHD$ Account Domain: WORKGROUP Logon ID: 0x3e7 Logon Type: 5 Impersonation Level: %%1833 New Logon: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Logon ID: 0x3e7 Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x23c Process Name: C:\Windows\System32\services.exe Network Information: Workstation Name: Source Network Address: - Source Port: - Detailed Authentication Information: Logon Process: Advapi Authentication Package: Negotiate Transited Services: - Package Name (NTLM only): - Key Length: 0 This event is generated when a logon session is created. It is generated on the computer that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service such as the Server service, or a local process such as Winlogon.exe or Services.exe. The logon type field indicates the kind of logon that occurred. The most common types are 2 (interactive) and 3 (network). The New Logon fields indicate the account for whom the new logon was created, i.e. the account that was logged on. The network fields indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impersonation level field indicates the extent to which a process in the logon session can impersonate. The authentication information fields provide detailed information about this specific logon request. - Logon GUID is a unique identifier that can be used to correlate this event with a KDC event. - Transited services indicate which intermediate services have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indicates the length of the generated session key. This will be 0 if no session key was requested.
	Security	Audit Success	12548	2015-04-28 20:15:30	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Logon ID: 0x3e7 Privileges: SeAssignPrimaryTokenPrivilege SeTcbPrivilege SeSecurityPrivilege SeTakeOwnershipPrivilege SeLoadDriverPrivilege SeBackupPrivilege SeRestorePrivilege SeDebugPrivilege SeAuditPrivilege SeSystemEnvironmentPrivilege SeImpersonatePrivilege
	Security	Audit Success	13824	2015-04-28 20:15:31	Microsoft-Windows-Security-Auditing	4797: An attempt was made to query the existence of a blank password for an account. Subject: Security ID: S-1-5-19 Account Name: LOCAL SERVICE Account Domain: NT AUTHORITY Logon ID: 0x3e5 Additional Information: Caller Workstation: LTRANPHD Target Account Name: Administrator Target Account Domain: LTRANPHD
	Security	Audit Success	13824	2015-04-28 20:15:31	Microsoft-Windows-Security-Auditing	4797: An attempt was made to query the existence of a blank password for an account. Subject: Security ID: S-1-5-19 Account Name: LOCAL SERVICE Account Domain: NT AUTHORITY Logon ID: 0x3e5 Additional Information: Caller Workstation: LTRANPHD Target Account Name: Administrator Target Account Domain:

						LTRANPHD
Security	Audit Success	13824	2015-04-28 20:15:31		Microsoft-Windows-Security-Auditing	4797: An attempt was made to query the existence of a blank password for an account. Subject: Security ID: S-1-5-19 Account Name: LOCAL SERVICE Account Domain: NT AUTHORITY Logon ID: 0x3e5 Additional Information: Caller Workstation: LTRANPHD Target Account Name: Guest Target Account Domain: LTRANPHD
Security	Audit Success	13824	2015-04-28 20:15:31		Microsoft-Windows-Security-Auditing	4797: An attempt was made to query the existence of a blank password for an account. Subject: Security ID: S-1-5-19 Account Name: LOCAL SERVICE Account Domain: NT AUTHORITY Logon ID: 0x3e5 Additional Information: Caller Workstation: LTRANPHD Target Account Name: Guest Target Account Domain: LTRANPHD
Security	Audit Success	13824	2015-04-28 20:15:31		Microsoft-Windows-Security-Auditing	4797: An attempt was made to query the existence of a blank password for an account. Subject: Security ID: S-1-5-19 Account Name: LOCAL SERVICE Account Domain: NT AUTHORITY Logon ID: 0x3e5 Additional Information: Caller Workstation: LTRANPHD Target Account Name: Liem Target Account Domain: LTRANPHD
Security	Audit Success	13824	2015-04-28 20:15:31		Microsoft-Windows-Security-Auditing	4797: An attempt was made to query the existence of a blank password for an account. Subject: Security ID: S-1-5-19 Account Name: LOCAL SERVICE Account Domain: NT AUTHORITY Logon ID: 0x3e5 Additional Information: Caller Workstation: LTRANPHD Target Account Name: Liem Target Account Domain: LTRANPHD
Security	Audit Success	13824	2015-04-28 20:15:31		Microsoft-Windows-Security-Auditing	4797: An attempt was made to query the existence of a blank password for an account. Subject: Security ID: S-1-5-19 Account Name: LOCAL SERVICE Account Domain: NT AUTHORITY Logon ID: 0x3e5 Additional Information: Caller Workstation: LTRANPHD Target Account Name: Liem Target Account Domain: LTRANPHD
Security	Audit Success	13824	2015-04-28 20:15:31		Microsoft-Windows-Security-Auditing	4797: An attempt was made to query the existence of a blank password for an account. Subject: Security ID: S-1-5-19 Account Name: LOCAL SERVICE Account Domain: NT AUTHORITY Logon ID: 0x3e5 Additional Information: Caller Workstation: LTRANPHD Target Account Name: Liem Target Account Domain: LTRANPHD
Security	Audit Success	13824	2015-04-28 20:15:32		Microsoft-Windows-Security-Auditing	4797: An attempt was made to query the existence of a blank password for an account. Subject: Security ID: S-1-5-21-1888849264-3803429180-4108621888-1001 Account Name: Liem Account Domain: LTRANPHD Logon ID: 0x1f4eb Additional Information: Caller Workstation: LTRANPHD Target Account Name: Administrator Target Account Domain: LTRANPHD
Security	Audit Success	13824	2015-04-28 20:15:32		Microsoft-Windows-Security-Auditing	4797: An attempt was made to query the existence of a blank password for an account. Subject: Security ID: S-1-5-21-1888849264-3803429180-4108621888-1001 Account Name: Liem Account Domain: LTRANPHD Logon ID: 0x1f4eb Additional Information: Caller Workstation: LTRANPHD Target Account Name: Guest Target Account Domain: LTRANPHD
Security	Audit Success	13824	2015-04-28 20:15:32		Microsoft-Windows-Security-Auditing	4797: An attempt was made to query the existence of a blank password for an account. Subject: Security ID: S-1-5-21-1888849264-3803429180-4108621888-1001 Account Name: Liem Account Domain: LTRANPHD Logon ID: 0x1f4eb Additional Information: Caller Workstation: LTRANPHD Target Account Name: Administrator Target Account Domain: LTRANPHD
Security	Audit Success	13824	2015-04-28 20:15:32		Microsoft-Windows-Security-Auditing	4797: An attempt was made to query the existence of a blank password for an account. Subject: Security ID: S-1-5-21-1888849264-3803429180-4108621888-1001 Account Name: Liem Account Domain: LTRANPHD Logon ID: 0x1f4eb Additional Information: Caller Workstation: LTRANPHD Target Account Name: Guest Target Account Domain: LTRANPHD
Security	Audit Success	12545	2015-04-28 20:25:37		Microsoft-Windows-Security-Auditing	4647: User initiated logoff: Subject: Security ID: S-1-5-21-1888849264-3803429180-4108621888-1001 Account Name: Liem Account Domain: LTRANPHD Logon ID: 0x1f4eb This event is generated when a logoff is initiated. No further user-initiated activity can occur. This event can be interpreted as a logoff event.
Security	Audit Success	103	2015-04-28 20:25:41		Microsoft-Windows-Eventlog	1100: The event logging service has shut down.
Security	Audit Success	12288	2015-04-28 20:42:36		Microsoft-Windows-Security-Auditing	4608: Windows is starting up. This event is logged when LSASS.EXE starts and the auditing subsystem is initialized.
Security	Audit Success	12544	2015-04-28 20:42:36		Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-0-0 Account Name: - Account Domain: - Logon ID: 0x0 Logon Type: 0 Impersonation Level: - New Logon: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Logon ID: 0x3e7 Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x4 Process Name: Network Information: Workstation Name: - Source Network Address: - Source Port: - Detailed Authentication Information: Logon Process: - Authentication Package: - Transited Services: - Package Name (NTLM only): - Key Length: 0 This event is generated when a logon session is created. It is generated on the computer that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service such as the Server service, or a local process such as Winlogon.exe or Services.exe. The logon type field indicates the kind of logon that occurred. The most common types are 2 (interactive) and 3 (network). The New Logon fields indicate the account for whom the new logon was created, i.e. the account that was logged on. The network fields indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impersonation level field indicates the extent to which a process in the logon session can impersonate. The authentication information fields provide detailed information about this specific logon request. - Logon GUID is a unique identifier that can be used to correlate this event with a KDC event. - Transited services indicate which intermediate services have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indicates the length of the generated session key. This will be 0 if no session key was requested.
						4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: LTRANPHD$ Account Domain: WORKGROUP Logon ID: 0x3e7 Logon Type: 5 Impersonation Level: %%1833 New Logon:

Security	Audit Success	12544	2015-04-28 20:42:36	Microsoft-Windows-Security-Auditing	Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Logon ID: 0x3e7 Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x23c Process Name: C:\Windows\System32\services.exe Network Information: Workstation Name: Source Network Address: - Source Port: - Detailed Authentication Information: Logon Process: Advapi Authentication Package: Negotiate Transited Services: - Package Name (NTLM only): - Key Length: 0 This event is generated when a logon session is created. It is generated on the computer that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service such as the Server service, or a local process such as Winlogon.exe or Services.exe. The logon type field indicates the kind of logon that occurred. The most common types are 2 (interactive) and 3 (network). The New Logon fields indicate the account for whom the new logon was created, i.e. the account that was logged on. The network fields indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impersonation level field indicates the extent to which a process in the logon session can impersonate. The authentication information fields provide detailed information about this specific logon request. - Logon GUID is a unique identifier that can be used to correlate this event with a KDC event. - Transited services indicate which intermediate services have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indicates the length of the generated session key. This will be 0 if no session key was requested.
Security	Audit Success	12544	2015-04-28 20:42:36	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: LTRANPHD$ Account Domain: WORKGROUP Logon ID: 0x3e7 Logon Type: 5 Impersonation Level: %%1833 New Logon: Security ID: S-1-5-20 Account Name: NETWORK SERVICE Account Domain: NT AUTHORITY Logon ID: 0x3e4 Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x23c Process Name: C:\Windows\System32\services.exe Network Information: Workstation Name: Source Network Address: - Source Port: - Detailed Authentication Information: Logon Process: Advapi Authentication Package: Negotiate Transited Services: - Package Name (NTLM only): - Key Length: 0 This event is generated when a logon session is created. It is generated on the computer that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service such as the Server service, or a local process such as Winlogon.exe or Services.exe. The logon type field indicates the kind of logon that occurred. The most common types are 2 (interactive) and 3 (network). The New Logon fields indicate the account for whom the new logon was created, i.e. the account that was logged on. The network fields indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impersonation level field indicates the extent to which a process in the logon session can impersonate. The authentication information fields provide detailed information about this specific logon request. - Logon GUID is a unique identifier that can be used to correlate this event with a KDC event. - Transited services indicate which intermediate services have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indicates the length of the generated session key. This will be 0 if no session key was requested.
Security	Audit Success	12544	2015-04-28 20:42:36	Microsoft-Windows-Security-Auditing	4648: A logon was attempted using explicit credentials. Subject: Security ID: S-1-5-18 Account Name: LTRANPHD$ Account Domain: WORKGROUP Logon ID: 0x3e7 Logon GUID: {00000000-0000-0000-0000-000000000000} Account Whose Credentials Were Used: Account Name: DWM-1 Account Domain: Window Manager Logon GUID: {00000000-0000-0000-0000-000000000000} Target Server: Target Server Name: localhost Additional Information: localhost Process Information: Process ID: 0x20c Process Name: C:\Windows\System32\winlogon.exe Network Information: Network Address: - Port: - This event is generated when a process attempts to log on an account by explicitly specifying that account's credentials. This most commonly occurs in batch-type configurations such as scheduled tasks, or when using the RUNAS command.
Security	Audit Success	12544	2015-04-28 20:42:36	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: LTRANPHD$ Account Domain: WORKGROUP Logon ID: 0x3e7 Logon Type: 2 Impersonation Level: %%1833 New Logon: Security ID: S-1-5-90-1 Account Name: DWM-1 Account Domain: Window Manager Logon ID: 0xc4db Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x20c Process Name: C:\Windows\System32\winlogon.exe Network Information: Workstation Name: Source Network Address: - Source Port: - Detailed Authentication Information: Logon Process: Advapi Authentication Package: Negotiate Transited Services: - Package Name (NTLM only): - Key Length: 0 This event is generated when a logon session is created. It is generated on the computer that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service such as the Server service, or a local process such as Winlogon.exe or Services.exe. The logon type field indicates the kind of logon that occurred. The most common types are 2 (interactive) and 3 (network). The New Logon fields indicate the account for whom the new logon was created, i.e. the account that was logged on. The network fields indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impersonation level field indicates the extent to which a process in the logon session can impersonate. The authentication information fields provide detailed information about this specific logon request. - Logon GUID is a unique identifier that can be used to correlate this event with a KDC event. - Transited services indicate which intermediate services have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indicates the length of the generated session key. This will be 0 if no session key was requested.
					4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: LTRANPHD$ Account Domain: WORKGROUP Logon ID: 0x3e7 Logon Type: 2 Impersonation Level: %%1833 New Logon: Security ID: S-1-5-90-1 Account Name: DWM-1 Account Domain: Window Manager Logon ID: 0xc4f3 Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x20c Process Name:

Security	Audit Success	12544	2015-04-28 20:42:36	Microsoft-Windows-Security-Auditing	C:\Windows\System32\winlogon.exe Network Information: Workstation Name: Source Network Address: - Source Port: - Detailed Authentication Information: Logon Process: Advapi Authentication Package: Negotiate Transited Services: - Package Name (NTLM only): - Key Length: 0 This event is generated when a logon session is created. It is generated on the computer that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service such as the Server service, or a local process such as Winlogon.exe or Services.exe. The logon type field indicates the kind of logon that occurred. The most common types are 2 (interactive) and 3 (network). The New Logon fields indicate the account for whom the new logon was created, i.e. the account that was logged on. The network fields indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impersonation level field indicates the extent to which a process in the logon session can impersonate. The authentication information fields provide detailed information about this specific logon request. - Logon GUID is a unique identifier that can be used to correlate this event with a KDC event. - Transited services indicate which intermediate services have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indicates the length of the generated session key. This will be 0 if no session key was requested.
Security	Audit Success	12544	2015-04-28 20:42:36	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: LTRANPHD$ Account Domain: WORKGROUP Logon ID: 0x3e7 Logon Type: 5 Impersonation Level: %%1833 New Logon: Security ID: S-1-5-19 Account Name: LOCAL SERVICE Account Domain: NT AUTHORITY Logon ID: 0x3e5 Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x23c Process Name: C:\Windows\System32\services.exe Network Information: Workstation Name: Source Network Address: - Source Port: - Detailed Authentication Information: Logon Process: Advapi Authentication Package: Negotiate Transited Services: - Package Name (NTLM only): - Key Length: 0 This event is generated when a logon session is created. It is generated on the computer that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service such as the Server service, or a local process such as Winlogon.exe or Services.exe. The logon type field indicates the kind of logon that occurred. The most common types are 2 (interactive) and 3 (network). The New Logon fields indicate the account for whom the new logon was created, i.e. the account that was logged on. The network fields indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impersonation level field indicates the extent to which a process in the logon session can impersonate. The authentication information fields provide detailed information about this specific logon request. - Logon GUID is a unique identifier that can be used to correlate this event with a KDC event. - Transited services indicate which intermediate services have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indicates the length of the generated session key. This will be 0 if no session key was requested.
Security	Audit Success	12544	2015-04-28 20:42:36	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: LTRANPHD$ Account Domain: WORKGROUP Logon ID: 0x3e7 Logon Type: 5 Impersonation Level: %%1833 New Logon: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Logon ID: 0x3e7 Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x23c Process Name: C:\Windows\System32\services.exe Network Information: Workstation Name: Source Network Address: - Source Port: - Detailed Authentication Information: Logon Process: Advapi Authentication Package: Negotiate Transited Services: - Package Name (NTLM only): - Key Length: 0 This event is generated when a logon session is created. It is generated on the computer that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service such as the Server service, or a local process such as Winlogon.exe or Services.exe. The logon type field indicates the kind of logon that occurred. The most common types are 2 (interactive) and 3 (network). The New Logon fields indicate the account for whom the new logon was created, i.e. the account that was logged on. The network fields indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impersonation level field indicates the extent to which a process in the logon session can impersonate. The authentication information fields provide detailed information about this specific logon request. - Logon GUID is a unique identifier that can be used to correlate this event with a KDC event. - Transited services indicate which intermediate services have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indicates the length of the generated session key. This will be 0 if no session key was requested.
Security	Audit Success	12544	2015-04-28 20:42:36	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: LTRANPHD$ Account Domain: WORKGROUP Logon ID: 0x3e7 Logon Type: 5 Impersonation Level: %%1833 New Logon: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Logon ID: 0x3e7 Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x23c Process Name: C:\Windows\System32\services.exe Network Information: Workstation Name: Source Network Address: - Source Port: - Detailed Authentication Information: Logon Process: Advapi Authentication Package: Negotiate Transited Services: - Package Name (NTLM only): - Key Length: 0 This event is generated when a logon session is created. It is generated on the computer that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service such as the Server service, or a local process such as Winlogon.exe or Services.exe. The logon type field indicates the kind of logon that occurred. The most common types are 2 (interactive) and 3 (network). The New Logon fields indicate the account for whom the new logon was created, i.e. the account that was logged on. The network fields indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impersonation level field indicates the extent to which a process in the logon session can

					impersonate. The authentication information fields provide detailed information about this specific logon request. - Logon GUID is a unique identifier that can be used to correlate this event with a KDC event. - Transited services indicate which intermediate services have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indicates the length of the generated session key. This will be 0 if no session key was requested.
Security	Audit Success	12548	2015-04-28 20:42:36	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Logon ID: 0x3e7 Privileges: SeAssignPrimaryTokenPrivilege SeTcbPrivilege SeSecurityPrivilege SeTakeOwnershipPrivilege SeLoadDriverPrivilege SeBackupPrivilege SeRestorePrivilege SeDebugPrivilege SeAuditPrivilege SeSystemEnvironmentPrivilege SeImpersonatePrivilege
Security	Audit Success	12548	2015-04-28 20:42:36	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-20 Account Name: NETWORK SERVICE Account Domain: NT AUTHORITY Logon ID: 0x3e4 Privileges: SeAssignPrimaryTokenPrivilege SeAuditPrivilege SeImpersonatePrivilege
Security	Audit Success	12548	2015-04-28 20:42:36	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-90-1 Account Name: DWM-1 Account Domain: Window Manager Logon ID: 0xc4db Privileges: SeAssignPrimaryTokenPrivilege SeAuditPrivilege SeImpersonatePrivilege
Security	Audit Success	12548	2015-04-28 20:42:36	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-90-1 Account Name: DWM-1 Account Domain: Window Manager Logon ID: 0xc4f3 Privileges: SeAssignPrimaryTokenPrivilege SeAuditPrivilege
Security	Audit Success	12548	2015-04-28 20:42:36	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-19 Account Name: LOCAL SERVICE Account Domain: NT AUTHORITY Logon ID: 0x3e5 Privileges: SeAssignPrimaryTokenPrivilege SeAuditPrivilege SeImpersonatePrivilege
Security	Audit Success	12548	2015-04-28 20:42:36	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Logon ID: 0x3e7 Privileges: SeAssignPrimaryTokenPrivilege SeTcbPrivilege SeSecurityPrivilege SeTakeOwnershipPrivilege SeLoadDriverPrivilege SeBackupPrivilege SeRestorePrivilege SeDebugPrivilege SeAuditPrivilege SeSystemEnvironmentPrivilege SeImpersonatePrivilege
Security	Audit Success	12548	2015-04-28 20:42:36	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Logon ID: 0x3e7 Privileges: SeAssignPrimaryTokenPrivilege SeTcbPrivilege SeSecurityPrivilege SeTakeOwnershipPrivilege SeLoadDriverPrivilege SeBackupPrivilege SeRestorePrivilege SeDebugPrivilege SeAuditPrivilege SeSystemEnvironmentPrivilege SeImpersonatePrivilege
Security	Audit Success	13568	2015-04-28 20:42:36	Microsoft-Windows-Security-Auditing	4902: The Per-user audit policy table was created. Number of Elements: 0 Policy ID: 0x75e1
Security	Audit Success	12292	2015-04-28 20:42:37	Microsoft-Windows-Security-Auditing	5033: The Windows Firewall Driver started successfully.
Security	Audit Success	12544	2015-04-28 20:42:37	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: LTRANPHD$ Account Domain: WORKGROUP Logon ID: 0x3e7 Logon Type: 5 Impersonation Level: %%1833 New Logon: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Logon ID: 0x3e7 Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x23c Process Name: C:\Windows\System32\services.exe Network Information: Workstation Name: Source Network Address: - Source Port: - Detailed Authentication Information: Logon Process: Advapi Authentication Package: Negotiate Transited Services: - Package Name (NTLM only): - Key Length: 0 This event is generated when a logon session is created. It is generated on the computer that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service such as the Server service, or a local process such as Winlogon.exe or Services.exe. The logon type field indicates the kind of logon that occurred. The most common types are 2 (interactive) and 3 (network). The New Logon fields indicate the account for whom the new logon was created, i.e. the account that was logged on. The network fields indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impersonation level field indicates the extent to which a process in the logon session can impersonate. The authentication information fields provide detailed information about this specific logon request. - Logon GUID is a unique identifier that can be used to correlate this event with a KDC event. - Transited services indicate which intermediate services have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indicates the length of the generated session key. This will be 0 if no session key was requested.
Security	Audit Success	12544	2015-04-28 20:42:37	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: LTRANPHD$ Account Domain: WORKGROUP Logon ID: 0x3e7 Logon Type: 5 Impersonation Level: %%1833 New Logon: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Logon ID: 0x3e7 Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x23c Process Name: C:\Windows\System32\services.exe Network Information: Workstation Name: Source Network Address: - Source Port: - Detailed Authentication Information: Logon Process: Advapi Authentication Package: Negotiate Transited Services: - Package Name (NTLM only): - Key Length: 0 This event is generated when a logon session is created. It is generated on the computer that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service such as the Server service, or a local process such as Winlogon.exe or Services.exe. The logon type field indicates the kind of logon that occurred. The most common types are 2 (interactive) and 3 (network). The New Logon fields indicate the account for

					whom the new logon was created, i.e. the account that was logged on. The network fields indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impersonation level field indicates the extent to which a process in the logon session can impersonate. The authentication information fields provide detailed information about this specific logon request. - Logon GUID is a unique identifier that can be used to correlate this event with a KDC event. - Transited services indicate which intermediate services have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indicates the length of the generated session key. This will be 0 if no session key was requested.
Security	Audit Success	12548	2015-04-28 20:42:37	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Logon ID: 0x3e7 Privileges: SeAssignPrimaryTokenPrivilege SeTcbPrivilege SeSecurityPrivilege SeTakeOwnershipPrivilege SeLoadDriverPrivilege SeBackupPrivilege SeRestorePrivilege SeDebugPrivilege SeAuditPrivilege SeSystemEnvironmentPrivilege SeImpersonatePrivilege
Security	Audit Success	12548	2015-04-28 20:42:37	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Logon ID: 0x3e7 Privileges: SeAssignPrimaryTokenPrivilege SeTcbPrivilege SeSecurityPrivilege SeTakeOwnershipPrivilege SeLoadDriverPrivilege SeBackupPrivilege SeRestorePrivilege SeDebugPrivilege SeAuditPrivilege SeSystemEnvironmentPrivilege SeImpersonatePrivilege
Security	Audit Success	12292	2015-04-28 20:42:38	Microsoft-Windows-Security-Auditing	5024: The Windows Firewall service started successfully.
Security	Audit Success	12544	2015-04-28 20:42:38	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: LTRANPHD$ Account Domain: WORKGROUP Logon ID: 0x3e7 Logon Type: 5 Impersonation Level: %%1833 New Logon: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Logon ID: 0x3e7 Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x23c Process Name: C:\Windows\System32\services.exe Network Information: Workstation Name: Source Network Address: - Source Port: - Detailed Authentication Information: Logon Process: Advapi Authentication Package: Negotiate Transited Services: - Package Name (NTLM only): - Key Length: 0 This event is generated when a logon session is created. It is generated on the computer that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service such as the Server service, or a local process such as Winlogon.exe or Services.exe. The logon type field indicates the kind of logon that occurred. The most common types are 2 (interactive) and 3 (network). The New Logon fields indicate the account for whom the new logon was created, i.e. the account that was logged on. The network fields indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impersonation level field indicates the extent to which a process in the logon session can impersonate. The authentication information fields provide detailed information about this specific logon request. - Logon GUID is a unique identifier that can be used to correlate this event with a KDC event. - Transited services indicate which intermediate services have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indicates the length of the generated session key. This will be 0 if no session key was requested.
Security	Audit Success	12544	2015-04-28 20:42:38	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-0-0 Account Name: - Account Domain: - Logon ID: 0x0 Logon Type: 3 Impersonation Level: %%1833 New Logon: Security ID: S-1-5-7 Account Name: ANONYMOUS LOGON Account Domain: NT AUTHORITY Logon ID: 0x17fd4 Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x0 Process Name: - Network Information: Workstation Name: Source Network Address: - Source Port: - Detailed Authentication Information: Logon Process: NtLmSsp Authentication Package: NTLM Transited Services: - Package Name (NTLM only): NTLM V1 Key Length: 0 This event is generated when a logon session is created. It is generated on the computer that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service such as the Server service, or a local process such as Winlogon.exe or Services.exe. The logon type field indicates the kind of logon that occurred. The most common types are 2 (interactive) and 3 (network). The New Logon fields indicate the account for whom the new logon was created, i.e. the account that was logged on. The network fields indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impersonation level field indicates the extent to which a process in the logon session can impersonate. The authentication information fields provide detailed information about this specific logon request. - Logon GUID is a unique identifier that can be used to correlate this event with a KDC event. - Transited services indicate which intermediate services have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indicates the length of the generated session key. This will be 0 if no session key was requested.
Security	Audit Success	12548	2015-04-28 20:42:38	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Logon ID: 0x3e7 Privileges: SeAssignPrimaryTokenPrivilege SeTcbPrivilege SeSecurityPrivilege SeTakeOwnershipPrivilege SeLoadDriverPrivilege SeBackupPrivilege SeRestorePrivilege SeDebugPrivilege SeAuditPrivilege SeSystemEnvironmentPrivilege SeImpersonatePrivilege
Security	Audit Success	12544	2015-04-28 20:42:58	Microsoft-Windows-Security-Auditing	4648: A logon was attempted using explicit credentials. Subject: Security ID: S-1-5-18 Account Name: LTRANPHD$ Account Domain: WORKGROUP Logon ID: 0x3e7 Logon GUID: {00000000-0000-0000-0000-000000000000} Account Whose Credentials Were Used: Account Name: Liem Account Domain: LTRANPHD Logon GUID: {00000000-0000-0000-0000-000000000000} Target Server: Target Server Name: localhost Additional Information: localhost Process Information: Process ID: 0x20c Process Name: C:\Windows\System32\winlogon.exe Network Information: Network Address: 127.0.0.1 Port: 0 This event is

					generated when a process attempts to log on an account by explicitly specifying that account's credentials. This most commonly occurs in batch-type configurations such as scheduled tasks, or when using the RUNAS command.
Security	Audit Success	12544	2015-04-28 20:42:58	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: LTRANPHD$ Account Domain: WORKGROUP Logon ID: 0x3e7 Logon Type: 2 Impersonation Level: %%1833 New Logon: Security ID: S-1-5-21-1888849264-3803429180-4108621888-1001 Account Name: Liem Account Domain: LTRANPHD Logon ID: 0x2335f Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x20c Process Name: C:\Windows\System32\winlogon.exe Network Information: Workstation Name: LTRANPHD Source Network Address: 127.0.0.1 Source Port: 0 Detailed Authentication Information: Logon Process: User32 Authentication Package: Negotiate Transited Services: - Package Name (NTLM only): - Key Length: 0 This event is generated when a logon session is created. It is generated on the computer that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service such as the Server service, or a local process such as Winlogon.exe or Services.exe. The logon type field indicates the kind of logon that occurred. The most common types are 2 (interactive) and 3 (network). The New Logon fields indicate the account for whom the new logon was created, i.e. the account that was logged on. The network fields indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impersonation level field indicates the extent to which a process in the logon session can impersonate. The authentication information fields provide detailed information about this specific logon request. - Logon GUID is a unique identifier that can be used to correlate this event with a KDC event. - Transited services indicate which intermediate services have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indicates the length of the generated session key. This will be 0 if no session key was requested.
Security	Audit Success	12544	2015-04-28 20:42:58	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: LTRANPHD$ Account Domain: WORKGROUP Logon ID: 0x3e7 Logon Type: 2 Impersonation Level: %%1833 New Logon: Security ID: S-1-5-21-1888849264-3803429180-4108621888-1001 Account Name: Liem Account Domain: LTRANPHD Logon ID: 0x233bd Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x20c Process Name: C:\Windows\System32\winlogon.exe Network Information: Workstation Name: LTRANPHD Source Network Address: 127.0.0.1 Source Port: 0 Detailed Authentication Information: Logon Process: User32 Authentication Package: Negotiate Transited Services: - Package Name (NTLM only): - Key Length: 0 This event is generated when a logon session is created. It is generated on the computer that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service such as the Server service, or a local process such as Winlogon.exe or Services.exe. The logon type field indicates the kind of logon that occurred. The most common types are 2 (interactive) and 3 (network). The New Logon fields indicate the account for whom the new logon was created, i.e. the account that was logged on. The network fields indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impersonation level field indicates the extent to which a process in the logon session can impersonate. The authentication information fields provide detailed information about this specific logon request. - Logon GUID is a unique identifier that can be used to correlate this event with a KDC event. - Transited services indicate which intermediate services have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indicates the length of the generated session key. This will be 0 if no session key was requested.
Security	Audit Success	12544	2015-04-28 20:42:58	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: LTRANPHD$ Account Domain: WORKGROUP Logon ID: 0x3e7 Logon Type: 5 Impersonation Level: %%1833 New Logon: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Logon ID: 0x3e7 Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x23c Process Name: C:\Windows\System32\services.exe Network Information: Workstation Name: Source Network Address: - Source Port: - Detailed Authentication Information: Logon Process: Advapi Authentication Package: Negotiate Transited Services: - Package Name (NTLM only): - Key Length: 0 This event is generated when a logon session is created. It is generated on the computer that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service such as the Server service, or a local process such as Winlogon.exe or Services.exe. The logon type field indicates the kind of logon that occurred. The most common types are 2 (interactive) and 3 (network). The New Logon fields indicate the account for whom the new logon was created, i.e. the account that was logged on. The network fields indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impersonation level field indicates the extent to which a process in the logon session can impersonate. The authentication information fields provide detailed information about this specific logon request. - Logon GUID is a unique identifier that can be used to correlate this event with a KDC event. - Transited services indicate which intermediate services have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indicates the length of the generated session key. This will be 0 if no session key was requested.
Security	Audit Success	12548	2015-04-28 20:42:58	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-21-1888849264-3803429180-4108621888-1001 Account Name: Liem Account Domain: LTRANPHD Logon ID: 0x2335f Privileges: SeSecurityPrivilege SeTakeOwnershipPrivilege SeLoadDriverPrivilege SeBackupPrivilege SeRestorePrivilege SeDebugPrivilege SeSystemEnvironmentPrivilege SeImpersonatePrivilege
Security	Audit	12548	2015-04-28	Microsoft-Windows-Security-	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Logon ID: 0x3e7 Privileges: SeAssignPrimaryTokenPrivilege SeTcbPrivilege

	Success		20:42:58	Auditing	SeSecurityPrivilege SeTakeOwnershipPrivilege SeLoadDriverPrivilege SeBackupPrivilege SeRestorePrivilege SeDebugPrivilege SeAuditPrivilege SeSystemEnvironmentPrivilege SeImpersonatePrivilege
Security	Audit Success	13824	2015-04-28 20:42:59	Microsoft-Windows-Security-Auditing	4797: An attempt was made to query the existence of a blank password for an account. Subject: Security ID: S-1-5-19 Account Name: LOCAL SERVICE Account Domain: NT AUTHORITY Logon ID: 0x3e5 Additional Information: Caller Workstation: LTRANPHD Target Account Name: Administrator Target Account Domain: LTRANPHD
Security	Audit Success	13824	2015-04-28 20:42:59	Microsoft-Windows-Security-Auditing	4797: An attempt was made to query the existence of a blank password for an account. Subject: Security ID: S-1-5-19 Account Name: LOCAL SERVICE Account Domain: NT AUTHORITY Logon ID: 0x3e5 Additional Information: Caller Workstation: LTRANPHD Target Account Name: Guest Target Account Domain: LTRANPHD
Security	Audit Success	13824	2015-04-28 20:42:59	Microsoft-Windows-Security-Auditing	4797: An attempt was made to query the existence of a blank password for an account. Subject: Security ID: S-1-5-19 Account Name: LOCAL SERVICE Account Domain: NT AUTHORITY Logon ID: 0x3e5 Additional Information: Caller Workstation: LTRANPHD Target Account Name: Liem Target Account Domain: LTRANPHD
Security	Audit Success	13824	2015-04-28 20:42:59	Microsoft-Windows-Security-Auditing	4797: An attempt was made to query the existence of a blank password for an account. Subject: Security ID: S-1-5-19 Account Name: LOCAL SERVICE Account Domain: NT AUTHORITY Logon ID: 0x3e5 Additional Information: Caller Workstation: LTRANPHD Target Account Name: Liem Target Account Domain: LTRANPHD
Security	Audit Success	13824	2015-04-28 20:42:59	Microsoft-Windows-Security-Auditing	4797: An attempt was made to query the existence of a blank password for an account. Subject: Security ID: S-1-5-19 Account Name: LOCAL SERVICE Account Domain: NT AUTHORITY Logon ID: 0x3e5 Additional Information: Caller Workstation: LTRANPHD Target Account Name: Administrator Target Account Domain: LTRANPHD
Security	Audit Success	13824	2015-04-28 20:42:59	Microsoft-Windows-Security-Auditing	4797: An attempt was made to query the existence of a blank password for an account. Subject: Security ID: S-1-5-19 Account Name: LOCAL SERVICE Account Domain: NT AUTHORITY Logon ID: 0x3e5 Additional Information: Caller Workstation: LTRANPHD Target Account Name: Guest Target Account Domain: LTRANPHD
Security	Audit Success	13824	2015-04-28 20:42:59	Microsoft-Windows-Security-Auditing	4797: An attempt was made to query the existence of a blank password for an account. Subject: Security ID: S-1-5-19 Account Name: LOCAL SERVICE Account Domain: NT AUTHORITY Logon ID: 0x3e5 Additional Information: Caller Workstation: LTRANPHD Target Account Name: Liem Target Account Domain: LTRANPHD
Security	Audit Success	13824	2015-04-28 20:42:59	Microsoft-Windows-Security-Auditing	4797: An attempt was made to query the existence of a blank password for an account. Subject: Security ID: S-1-5-19 Account Name: LOCAL SERVICE Account Domain: NT AUTHORITY Logon ID: 0x3e5 Additional Information: Caller Workstation: LTRANPHD Target Account Name: Administrator Target Account Domain: LTRANPHD
Security	Audit Success	13824	2015-04-28 20:42:59	Microsoft-Windows-Security-Auditing	4797: An attempt was made to query the existence of a blank password for an account. Subject: Security ID: S-1-5-19 Account Name: LOCAL SERVICE Account Domain: NT AUTHORITY Logon ID: 0x3e5 Additional Information: Caller Workstation: LTRANPHD Target Account Name: Liem Target Account Domain: LTRANPHD
Security	Audit Success	13824	2015-04-28 20:42:59	Microsoft-Windows-Security-Auditing	4797: An attempt was made to query the existence of a blank password for an account. Subject: Security ID: S-1-5-19 Account Name: LOCAL SERVICE Account Domain: NT AUTHORITY Logon ID: 0x3e5 Additional Information: Caller Workstation: LTRANPHD Target Account Name: Administrator Target Account Domain: LTRANPHD
Security	Audit Success	13824	2015-04-28 20:42:59	Microsoft-Windows-Security-Auditing	4797: An attempt was made to query the existence of a blank password for an account. Subject: Security ID: S-1-5-19 Account Name: LOCAL SERVICE Account Domain: NT AUTHORITY Logon ID: 0x3e5 Additional Information: Caller Workstation: LTRANPHD Target Account Name: Guest Target Account Domain: LTRANPHD
Security	Audit Success	13824	2015-04-28 20:42:59	Microsoft-Windows-Security-Auditing	4797: An attempt was made to query the existence of a blank password for an account. Subject: Security ID: S-1-5-19 Account Name: LOCAL SERVICE Account Domain: NT AUTHORITY Logon ID: 0x3e5 Additional Information: Caller Workstation: LTRANPHD Target Account Name: Liem Target Account Domain: LTRANPHD
Security	Audit Success	13824	2015-04-28 20:42:59	Microsoft-Windows-Security-Auditing	4797: An attempt was made to query the existence of a blank password for an account. Subject: Security ID: S-1-5-19 Account Name: LOCAL SERVICE Account Domain: NT AUTHORITY Logon ID: 0x3e5 Additional Information: Caller Workstation: LTRANPHD Target Account Name: Administrator Target Account Domain: LTRANPHD
Security	Audit Success	13824	2015-04-28 20:42:59	Microsoft-Windows-Security-Auditing	4797: An attempt was made to query the existence of a blank password for an account. Subject: Security ID: S-1-5-19 Account Name: LOCAL SERVICE Account Domain: NT AUTHORITY Logon ID: 0x3e5 Additional Information: Caller Workstation: LTRANPHD Target Account Name: Guest Target Account Domain: LTRANPHD
Security	Audit Success	13824	2015-04-28 20:42:59	Microsoft-Windows-Security-Auditing	4797: An attempt was made to query the existence of a blank password for an account. Subject: Security ID: S-1-5-19 Account Name: LOCAL SERVICE Account Domain: NT AUTHORITY Logon ID: 0x3e5 Additional Information: Caller Workstation: LTRANPHD Target Account Name: Liem Target Account Domain: LTRANPHD
Security	Audit Success	13824	2015-04-28 20:42:59	Microsoft-Windows-Security-Auditing	4797: An attempt was made to query the existence of a blank password for an account. Subject: Security ID: S-1-5-19 Account Name: LOCAL SERVICE Account Domain: NT AUTHORITY Logon ID: 0x3e5 Additional Information: Caller Workstation: LTRANPHD Target Account Name: Liem Target Account Domain: LTRANPHD
Security	Audit Success	13824	2015-04-28 20:43:01	Microsoft-Windows-Security-Auditing	4797: An attempt was made to query the existence of a blank password for an account. Subject: Security ID: S-1-5-21-1888849264-3803429180-4108621888-1001 Account Name: Liem Account Domain: LTRANPHD Logon ID: 0x233bd Additional Information: Caller Workstation: LTRANPHD Target Account Name: Administrator Target Account Domain: LTRANPHD
					4797: An attempt was made to query the existence of a blank password for an account. Subject: Security ID:

Security	Audit Success	13824	2015-04-28 20:43:01	Microsoft-Windows-Security-Auditing	S-1-5-21-1888849264-3803429180-4108621888-1001 Account Name: Liem Account Domain: LTRANPHD Logon ID: 0x233bd Additional Information: Caller Workstation: LTRANPHD Target Account Name: Guest Target Account Domain: LTRANPHD
Security	Audit Success	13824	2015-04-28 20:43:01	Microsoft-Windows-Security-Auditing	4797: An attempt was made to query the existence of a blank password for an account. Subject: Security ID: S-1-5-21-1888849264-3803429180-4108621888-1001 Account Name: Liem Account Domain: LTRANPHD Logon ID: 0x233bd Additional Information: Caller Workstation: LTRANPHD Target Account Name: Administrator Target Account Domain: LTRANPHD
Security	Audit Success	13824	2015-04-28 20:43:01	Microsoft-Windows-Security-Auditing	4797: An attempt was made to query the existence of a blank password for an account. Subject: Security ID: S-1-5-21-1888849264-3803429180-4108621888-1001 Account Name: Liem Account Domain: LTRANPHD Logon ID: 0x233bd Additional Information: Caller Workstation: LTRANPHD Target Account Name: Guest Target Account Domain: LTRANPHD
Security	Audit Success	12544	2015-04-28 20:53:16	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: LTRANPHD$ Account Domain: WORKGROUP Logon ID: 0x3e7 Logon Type: 5 Impersonation Level: %%1833 New Logon: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Logon ID: 0x3e7 Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x23c Process Name: C:\Windows\System32\services.exe Network Information: Workstation Name: Source Network Address: - Source Port: - Detailed Authentication Information: Logon Process: Advapi Authentication Package: Negotiate Transited Services: - Package Name (NTLM only): - Key Length: 0 This event is generated when a logon session is created. It is generated on the computer that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service such as the Server service, or a local process such as Winlogon.exe or Services.exe. The logon type field indicates the kind of logon that occurred. The most common types are 2 (interactive) and 3 (network). The New Logon fields indicate the account for whom the new logon was created, i.e. the account that was logged on. The network fields indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impersonation level field indicates the extent to which a process in the logon session can impersonate. The authentication information fields provide detailed information about this specific logon request. - Logon GUID is a unique identifier that can be used to correlate this event with a KDC event. - Transited services indicate which intermediate services have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indicates the length of the generated session key. This will be 0 if no session key was requested.
Security	Audit Success	12548	2015-04-28 20:53:16	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Logon ID: 0x3e7 Privileges: SeAssignPrimaryTokenPrivilege SeTcbPrivilege SeSecurityPrivilege SeTakeOwnershipPrivilege SeLoadDriverPrivilege SeBackupPrivilege SeRestorePrivilege SeDebugPrivilege SeAuditPrivilege SeSystemEnvironmentPrivilege SeImpersonatePrivilege
Security	Audit Success	12544	2015-04-28 20:53:18	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: LTRANPHD$ Account Domain: WORKGROUP Logon ID: 0x3e7 Logon Type: 5 Impersonation Level: %%1833 New Logon: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Logon ID: 0x3e7 Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x23c Process Name: C:\Windows\System32\services.exe Network Information: Workstation Name: Source Network Address: - Source Port: - Detailed Authentication Information: Logon Process: Advapi Authentication Package: Negotiate Transited Services: - Package Name (NTLM only): - Key Length: 0 This event is generated when a logon session is created. It is generated on the computer that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service such as the Server service, or a local process such as Winlogon.exe or Services.exe. The logon type field indicates the kind of logon that occurred. The most common types are 2 (interactive) and 3 (network). The New Logon fields indicate the account for whom the new logon was created, i.e. the account that was logged on. The network fields indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impersonation level field indicates the extent to which a process in the logon session can impersonate. The authentication information fields provide detailed information about this specific logon request. - Logon GUID is a unique identifier that can be used to correlate this event with a KDC event. - Transited services indicate which intermediate services have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indicates the length of the generated session key. This will be 0 if no session key was requested.
Security	Audit Success	12548	2015-04-28 20:53:18	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Logon ID: 0x3e7 Privileges: SeAssignPrimaryTokenPrivilege SeTcbPrivilege SeSecurityPrivilege SeTakeOwnershipPrivilege SeLoadDriverPrivilege SeBackupPrivilege SeRestorePrivilege SeDebugPrivilege SeAuditPrivilege SeSystemEnvironmentPrivilege SeImpersonatePrivilege
					4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: LTRANPHD$ Account Domain: WORKGROUP Logon ID: 0x3e7 Logon Type: 5 Impersonation Level: %%1833 New Logon: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Logon ID: 0x3e7 Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x23c Process Name: C:\Windows\System32\services.exe Network Information: Workstation Name: Source Network Address: - Source Port: - Detailed Authentication Information: Logon Process: Advapi Authentication Package: Negotiate Transited Services: - Package Name (NTLM only): - Key Length: 0 This event is generated when a logon session is created. It is generated on the computer that was accessed. The subject fields indicate the account on the local

Security	Audit Success	12544	2015-04-28 21:00:29	Microsoft-Windows-Security-Auditing	system which requested the logon. This is most commonly a service such as the Server service, or a local process such as Winlogon.exe or Services.exe. The logon type field indicates the kind of logon that occurred. The most common types are 2 (interactive) and 3 (network). The New Logon fields indicate the account for whom the new logon was created, i.e. the account that was logged on. The network fields indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impersonation level field indicates the extent to which a process in the logon session can impersonate. The authentication information fields provide detailed information about this specific logon request. - Logon GUID is a unique identifier that can be used to correlate this event with a KDC event. - Transited services indicate which intermediate services have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indicates the length of the generated session key. This will be 0 if no session key was requested.
Security	Audit Success	12544	2015-04-28 21:00:29	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: LTRANPHD$ Account Domain: WORKGROUP Logon ID: 0x3e7 Logon Type: 5 Impersonation Level: %%1833 New Logon: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Logon ID: 0x3e7 Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x23c Process Name: C:\Windows\System32\services.exe Network Information: Workstation Name: Source Network Address: - Source Port: - Detailed Authentication Information: Logon Process: Advapi Authentication Package: Negotiate Transited Services: - Package Name (NTLM only): - Key Length: 0 This event is generated when a logon session is created. It is generated on the computer that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service such as the Server service, or a local process such as Winlogon.exe or Services.exe. The logon type field indicates the kind of logon that occurred. The most common types are 2 (interactive) and 3 (network). The New Logon fields indicate the account for whom the new logon was created, i.e. the account that was logged on. The network fields indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impersonation level field indicates the extent to which a process in the logon session can impersonate. The authentication information fields provide detailed information about this specific logon request. - Logon GUID is a unique identifier that can be used to correlate this event with a KDC event. - Transited services indicate which intermediate services have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indicates the length of the generated session key. This will be 0 if no session key was requested.
Security	Audit Success	12548	2015-04-28 21:00:29	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Logon ID: 0x3e7 Privileges: SeAssignPrimaryTokenPrivilege SeTcbPrivilege SeSecurityPrivilege SeTakeOwnershipPrivilege SeLoadDriverPrivilege SeBackupPrivilege SeRestorePrivilege SeDebugPrivilege SeAuditPrivilege SeSystemEnvironmentPrivilege SeImpersonatePrivilege
Security	Audit Success	12548	2015-04-28 21:00:29	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Logon ID: 0x3e7 Privileges: SeAssignPrimaryTokenPrivilege SeTcbPrivilege SeSecurityPrivilege SeTakeOwnershipPrivilege SeLoadDriverPrivilege SeBackupPrivilege SeRestorePrivilege SeDebugPrivilege SeAuditPrivilege SeSystemEnvironmentPrivilege SeImpersonatePrivilege
Security	Audit Success	12288	2015-04-29 11:34:20	Microsoft-Windows-Security-Auditing	4608: Windows is starting up. This event is logged when LSASS.EXE starts and the auditing subsystem is initialized.
Security	Audit Success	12544	2015-04-29 11:34:20	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-0-0 Account Name: - Account Domain: - Logon ID: 0x0 Logon Type: 0 Impersonation Level: - New Logon: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Logon ID: 0x3e7 Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x4 Process Name: Network Information: Workstation Name: - Source Network Address: - Source Port: - Detailed Authentication Information: Logon Process: - Authentication Package: - Transited Services: - Package Name (NTLM only): - Key Length: 0 This event is generated when a logon session is created. It is generated on the computer that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service such as the Server service, or a local process such as Winlogon.exe or Services.exe. The logon type field indicates the kind of logon that occurred. The most common types are 2 (interactive) and 3 (network). The New Logon fields indicate the account for whom the new logon was created, i.e. the account that was logged on. The network fields indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impersonation level field indicates the extent to which a process in the logon session can impersonate. The authentication information fields provide detailed information about this specific logon request. - Logon GUID is a unique identifier that can be used to correlate this event with a KDC event. - Transited services indicate which intermediate services have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indicates the length of the generated session key. This will be 0 if no session key was requested.
					4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: LTRANPHD$ Account Domain: WORKGROUP Logon ID: 0x3e7 Logon Type: 5 Impersonation Level: %%1833 New Logon: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Logon ID: 0x3e7 Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x238 Process Name: C:\Windows\System32\services.exe Network Information: Workstation Name: Source Network Address: - Source Port: - Detailed Authentication Information: Logon Process: Advapi Authentication Package: Negotiate Transited Services: - Package Name (NTLM only): - Key Length: 0 This event is generated when a logon session is

Security	Audit Success	12544	2015-04-29 11:34:20	Microsoft-Windows-Security-Auditing	created. It is generated on the computer that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service such as the Server service, or a local process such as Winlogon.exe or Services.exe. The logon type field indicates the kind of logon that occurred. The most common types are 2 (interactive) and 3 (network). The New Logon fields indicate the account for whom the new logon was created, i.e. the account that was logged on. The network fields indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impersonation level field indicates the extent to which a process in the logon session can impersonate. The authentication information fields provide detailed information about this specific logon request. - Logon GUID is a unique identifier that can be used to correlate this event with a KDC event. - Transited services indicate which intermediate services have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indicates the length of the generated session key. This will be 0 if no session key was requested.
Security	Audit Success	12544	2015-04-29 11:34:20	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: LTRANPHD$ Account Domain: WORKGROUP Logon ID: 0x3e7 Logon Type: 5 Impersonation Level: %%1833 New Logon: Security ID: S-1-5-20 Account Name: NETWORK SERVICE Account Domain: NT AUTHORITY Logon ID: 0x3e4 Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x238 Process Name: C:\Windows\System32\services.exe Network Information: Workstation Name: Source Network Address: - Source Port: - Detailed Authentication Information: Logon Process: Advapi Authentication Package: Negotiate Transited Services: - Package Name (NTLM only): - Key Length: 0 This event is generated when a logon session is created. It is generated on the computer that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service such as the Server service, or a local process such as Winlogon.exe or Services.exe. The logon type field indicates the kind of logon that occurred. The most common types are 2 (interactive) and 3 (network). The New Logon fields indicate the account for whom the new logon was created, i.e. the account that was logged on. The network fields indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impersonation level field indicates the extent to which a process in the logon session can impersonate. The authentication information fields provide detailed information about this specific logon request. - Logon GUID is a unique identifier that can be used to correlate this event with a KDC event. - Transited services indicate which intermediate services have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indicates the length of the generated session key. This will be 0 if no session key was requested.
Security	Audit Success	12544	2015-04-29 11:34:20	Microsoft-Windows-Security-Auditing	4648: A logon was attempted using explicit credentials. Subject: Security ID: S-1-5-18 Account Name: LTRANPHD$ Account Domain: WORKGROUP Logon ID: 0x3e7 Logon GUID: {00000000-0000-0000-0000-000000000000} Account Whose Credentials Were Used: Account Name: DWM-1 Account Domain: Window Manager Logon GUID: {00000000-0000-0000-0000-000000000000} Target Server: Target Server Name: localhost Additional Information: localhost Process Information: Process ID: 0x208 Process Name: C:\Windows\System32\winlogon.exe Network Information: Network Address: - Port: - This event is generated when a process attempts to log on an account by explicitly specifying that account's credentials. This most commonly occurs in batch-type configurations such as scheduled tasks, or when using the RUNAS command.
Security	Audit Success	12544	2015-04-29 11:34:20	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: LTRANPHD$ Account Domain: WORKGROUP Logon ID: 0x3e7 Logon Type: 2 Impersonation Level: %%1833 New Logon: Security ID: S-1-5-90-1 Account Name: DWM-1 Account Domain: Window Manager Logon ID: 0xc50b Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x208 Process Name: C:\Windows\System32\winlogon.exe Network Information: Workstation Name: Source Network Address: - Source Port: - Detailed Authentication Information: Logon Process: Advapi Authentication Package: Negotiate Transited Services: - Package Name (NTLM only): - Key Length: 0 This event is generated when a logon session is created. It is generated on the computer that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service such as the Server service, or a local process such as Winlogon.exe or Services.exe. The logon type field indicates the kind of logon that occurred. The most common types are 2 (interactive) and 3 (network). The New Logon fields indicate the account for whom the new logon was created, i.e. the account that was logged on. The network fields indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impersonation level field indicates the extent to which a process in the logon session can impersonate. The authentication information fields provide detailed information about this specific logon request. - Logon GUID is a unique identifier that can be used to correlate this event with a KDC event. - Transited services indicate which intermediate services have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indicates the length of the generated session key. This will be 0 if no session key was requested.
			2015-04-		4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: LTRANPHD$ Account Domain: WORKGROUP Logon ID: 0x3e7 Logon Type: 2 Impersonation Level: %%1833 New Logon: Security ID: S-1-5-90-1 Account Name: DWM-1 Account Domain: Window Manager Logon ID: 0xc52b Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x208 Process Name: C:\Windows\System32\winlogon.exe Network Information: Workstation Name: Source Network Address: - Source Port: - Detailed Authentication Information: Logon Process: Advapi Authentication Package: Negotiate Transited Services: - Package Name (NTLM only): - Key Length: 0 This event is generated when a logon session is created. It is generated on the computer that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service such as the Server service, or a local

Security	Audit Success	12544	29 11:34:20	Microsoft-Windows-Security-Auditing	process such as Winlogon.exe or Services.exe. The logon type field indicates the kind of logon that occurred. The most common types are 2 (interactive) and 3 (network). The New Logon fields indicate the account for whom the new logon was created, i.e. the account that was logged on. The network fields indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impersonation level field indicates the extent to which a process in the logon session can impersonate. The authentication information fields provide detailed information about this specific logon request. - Logon GUID is a unique identifier that can be used to correlate this event with a KDC event. - Transited services indicate which intermediate services have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indicates the length of the generated session key. This will be 0 if no session key was requested.
Security	Audit Success	12544	2015-04-29 11:34:20	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: LTRANPHD$ Account Domain: WORKGROUP Logon ID: 0x3e7 Logon Type: 5 Impersonation Level: %%1833 New Logon: Security ID: S-1-5-19 Account Name: LOCAL SERVICE Account Domain: NT AUTHORITY Logon ID: 0x3e5 Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x238 Process Name: C:\Windows\System32\services.exe Network Information: Workstation Name: Source Network Address: - Source Port: - Detailed Authentication Information: Logon Process: Advapi Authentication Package: Negotiate Transited Services: - Package Name (NTLM only): - Key Length: 0 This event is generated when a logon session is created. It is generated on the computer that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service such as the Server service, or a local process such as Winlogon.exe or Services.exe. The logon type field indicates the kind of logon that occurred. The most common types are 2 (interactive) and 3 (network). The New Logon fields indicate the account for whom the new logon was created, i.e. the account that was logged on. The network fields indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impersonation level field indicates the extent to which a process in the logon session can impersonate. The authentication information fields provide detailed information about this specific logon request. - Logon GUID is a unique identifier that can be used to correlate this event with a KDC event. - Transited services indicate which intermediate services have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indicates the length of the generated session key. This will be 0 if no session key was requested.
Security	Audit Success	12544	2015-04-29 11:34:20	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: LTRANPHD$ Account Domain: WORKGROUP Logon ID: 0x3e7 Logon Type: 5 Impersonation Level: %%1833 New Logon: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Logon ID: 0x3e7 Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x238 Process Name: C:\Windows\System32\services.exe Network Information: Workstation Name: Source Network Address: - Source Port: - Detailed Authentication Information: Logon Process: Advapi Authentication Package: Negotiate Transited Services: - Package Name (NTLM only): - Key Length: 0 This event is generated when a logon session is created. It is generated on the computer that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service such as the Server service, or a local process such as Winlogon.exe or Services.exe. The logon type field indicates the kind of logon that occurred. The most common types are 2 (interactive) and 3 (network). The New Logon fields indicate the account for whom the new logon was created, i.e. the account that was logged on. The network fields indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impersonation level field indicates the extent to which a process in the logon session can impersonate. The authentication information fields provide detailed information about this specific logon request. - Logon GUID is a unique identifier that can be used to correlate this event with a KDC event. - Transited services indicate which intermediate services have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indicates the length of the generated session key. This will be 0 if no session key was requested.
Security	Audit Success	12544	2015-04-29 11:34:20	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: LTRANPHD$ Account Domain: WORKGROUP Logon ID: 0x3e7 Logon Type: 5 Impersonation Level: %%1833 New Logon: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Logon ID: 0x3e7 Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x238 Process Name: C:\Windows\System32\services.exe Network Information: Workstation Name: Source Network Address: - Source Port: - Detailed Authentication Information: Logon Process: Advapi Authentication Package: Negotiate Transited Services: - Package Name (NTLM only): - Key Length: 0 This event is generated when a logon session is created. It is generated on the computer that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service such as the Server service, or a local process such as Winlogon.exe or Services.exe. The logon type field indicates the kind of logon that occurred. The most common types are 2 (interactive) and 3 (network). The New Logon fields indicate the account for whom the new logon was created, i.e. the account that was logged on. The network fields indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impersonation level field indicates the extent to which a process in the logon session can impersonate. The authentication information fields provide detailed information about this specific logon request. - Logon GUID is a unique identifier that can be used to correlate this event with a KDC event. - Transited services indicate which intermediate services have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indicates the length of the generated

					session key. This will be 0 if no session key was requested.
Security	Audit Success	12548	2015-04-29 11:34:20	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Logon ID: 0x3e7 Privileges: SeAssignPrimaryTokenPrivilege SeTcbPrivilege SeSecurityPrivilege SeTakeOwnershipPrivilege SeLoadDriverPrivilege SeBackupPrivilege SeRestorePrivilege SeDebugPrivilege SeAuditPrivilege SeSystemEnvironmentPrivilege SeImpersonatePrivilege
Security	Audit Success	12548	2015-04-29 11:34:20	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-20 Account Name: NETWORK SERVICE Account Domain: NT AUTHORITY Logon ID: 0x3e4 Privileges: SeAssignPrimaryTokenPrivilege SeAuditPrivilege SeImpersonatePrivilege
Security	Audit Success	12548	2015-04-29 11:34:20	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-90-1 Account Name: DWM-1 Account Domain: Window Manager Logon ID: 0xc50b Privileges: SeAssignPrimaryTokenPrivilege SeAuditPrivilege SeImpersonatePrivilege
Security	Audit Success	12548	2015-04-29 11:34:20	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-90-1 Account Name: DWM-1 Account Domain: Window Manager Logon ID: 0xc52b Privileges: SeAssignPrimaryTokenPrivilege SeAuditPrivilege
Security	Audit Success	12548	2015-04-29 11:34:20	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-19 Account Name: LOCAL SERVICE Account Domain: NT AUTHORITY Logon ID: 0x3e5 Privileges: SeAssignPrimaryTokenPrivilege SeAuditPrivilege SeImpersonatePrivilege
Security	Audit Success	12548	2015-04-29 11:34:20	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Logon ID: 0x3e7 Privileges: SeAssignPrimaryTokenPrivilege SeTcbPrivilege SeSecurityPrivilege SeTakeOwnershipPrivilege SeLoadDriverPrivilege SeBackupPrivilege SeRestorePrivilege SeDebugPrivilege SeAuditPrivilege SeSystemEnvironmentPrivilege SeImpersonatePrivilege
Security	Audit Success	12548	2015-04-29 11:34:20	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Logon ID: 0x3e7 Privileges: SeAssignPrimaryTokenPrivilege SeTcbPrivilege SeSecurityPrivilege SeTakeOwnershipPrivilege SeLoadDriverPrivilege SeBackupPrivilege SeRestorePrivilege SeDebugPrivilege SeAuditPrivilege SeSystemEnvironmentPrivilege SeImpersonatePrivilege
Security	Audit Success	13568	2015-04-29 11:34:20	Microsoft-Windows-Security-Auditing	4902: The Per-user audit policy table was created. Number of Elements: 0 Policy ID: 0x75c0
Security	Audit Success	12292	2015-04-29 11:34:21	Microsoft-Windows-Security-Auditing	5033: The Windows Firewall Driver started successfully.
Security	Audit Success	12292	2015-04-29 11:34:21	Microsoft-Windows-Security-Auditing	5024: The Windows Firewall service started successfully.
Security	Audit Success	12544	2015-04-29 11:34:21	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: LTRANPHD$ Account Domain: WORKGROUP Logon ID: 0x3e7 Logon Type: 5 Impersonation Level: %%1833 New Logon: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Logon ID: 0x3e7 Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x238 Process Name: C:\Windows\System32\services.exe Network Information: Workstation Name: Source Network Address: - Source Port: - Detailed Authentication Information: Logon Process: Advapi Authentication Package: Negotiate Transited Services: - Package Name (NTLM only): - Key Length: 0 This event is generated when a logon session is created. It is generated on the computer that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service such as the Server service, or a local process such as Winlogon.exe or Services.exe. The logon type field indicates the kind of logon that occurred. The most common types are 2 (interactive) and 3 (network). The New Logon fields indicate the account for whom the new logon was created, i.e. the account that was logged on. The network fields indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impersonation level field indicates the extent to which a process in the logon session can impersonate. The authentication information fields provide detailed information about this specific logon request. - Logon GUID is a unique identifier that can be used to correlate this event with a KDC event. - Transited services indicate which intermediate services have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indicates the length of the generated session key. This will be 0 if no session key was requested.
Security	Audit Success	12544	2015-04-29 11:34:21	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: LTRANPHD$ Account Domain: WORKGROUP Logon ID: 0x3e7 Logon Type: 5 Impersonation Level: %%1833 New Logon: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Logon ID: 0x3e7 Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x238 Process Name: C:\Windows\System32\services.exe Network Information: Workstation Name: Source Network Address: - Source Port: - Detailed Authentication Information: Logon Process: Advapi Authentication Package: Negotiate Transited Services: - Package Name (NTLM only): - Key Length: 0 This event is generated when a logon session is created. It is generated on the computer that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service such as the Server service, or a local process such as Winlogon.exe or Services.exe. The logon type field indicates the kind of logon that occurred. The most common types are 2 (interactive) and 3 (network). The New Logon fields indicate the account for whom the new logon was created, i.e. the account that was logged on. The network fields indicate where a

					remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impersonation level field indicates the extent to which a process in the logon session can impersonate. The authentication information fields provide detailed information about this specific logon request. - Logon GUID is a unique identifier that can be used to correlate this event with a KDC event. - Transited services indicate which intermediate services have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indicates the length of the generated session key. This will be 0 if no session key was requested.
Security	Audit Success	12548	2015-04-29 11:34:21	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Logon ID: 0x3e7 Privileges: SeAssignPrimaryTokenPrivilege SeTcbPrivilege SeSecurityPrivilege SeTakeOwnershipPrivilege SeLoadDriverPrivilege SeBackupPrivilege SeRestorePrivilege SeDebugPrivilege SeAuditPrivilege SeSystemEnvironmentPrivilege SeImpersonatePrivilege
Security	Audit Success	12548	2015-04-29 11:34:21	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Logon ID: 0x3e7 Privileges: SeAssignPrimaryTokenPrivilege SeTcbPrivilege SeSecurityPrivilege SeTakeOwnershipPrivilege SeLoadDriverPrivilege SeBackupPrivilege SeRestorePrivilege SeDebugPrivilege SeAuditPrivilege SeSystemEnvironmentPrivilege SeImpersonatePrivilege
Security	Audit Success	12544	2015-04-29 11:34:22	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: LTRANPHD$ Account Domain: WORKGROUP Logon ID: 0x3e7 Logon Type: 5 Impersonation Level: %%1833 New Logon: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Logon ID: 0x3e7 Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x238 Process Name: C:\Windows\System32\services.exe Network Information: Workstation Name: Source Network Address: - Source Port: - Detailed Authentication Information: Logon Process: Advapi Authentication Package: Negotiate Transited Services: - Package Name (NTLM only): - Key Length: 0 This event is generated when a logon session is created. It is generated on the computer that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service such as the Server service, or a local process such as Winlogon.exe or Services.exe. The logon type field indicates the kind of logon that occurred. The most common types are 2 (interactive) and 3 (network). The New Logon fields indicate the account for whom the new logon was created, i.e. the account that was logged on. The network fields indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impersonation level field indicates the extent to which a process in the logon session can impersonate. The authentication information fields provide detailed information about this specific logon request. - Logon GUID is a unique identifier that can be used to correlate this event with a KDC event. - Transited services indicate which intermediate services have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indicates the length of the generated session key. This will be 0 if no session key was requested.
Security	Audit Success	12544	2015-04-29 11:34:22	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-0-0 Account Name: - Account Domain: - Logon ID: 0x0 Logon Type: 3 Impersonation Level: %%1833 New Logon: Security ID: S-1-5-7 Account Name: ANONYMOUS LOGON Account Domain: NT AUTHORITY Logon ID: 0x182b1 Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x0 Process Name: - Network Information: Workstation Name: Source Network Address: - Source Port: - Detailed Authentication Information: Logon Process: NtLmSsp Authentication Package: NTLM Transited Services: - Package Name (NTLM only): NTLM V1 Key Length: 0 This event is generated when a logon session is created. It is generated on the computer that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service such as the Server service, or a local process such as Winlogon.exe or Services.exe. The logon type field indicates the kind of logon that occurred. The most common types are 2 (interactive) and 3 (network). The New Logon fields indicate the account for whom the new logon was created, i.e. the account that was logged on. The network fields indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impersonation level field indicates the extent to which a process in the logon session can impersonate. The authentication information fields provide detailed information about this specific logon request. - Logon GUID is a unique identifier that can be used to correlate this event with a KDC event. - Transited services indicate which intermediate services have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indicates the length of the generated session key. This will be 0 if no session key was requested.
Security	Audit Success	12548	2015-04-29 11:34:22	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Logon ID: 0x3e7 Privileges: SeAssignPrimaryTokenPrivilege SeTcbPrivilege SeSecurityPrivilege SeTakeOwnershipPrivilege SeLoadDriverPrivilege SeBackupPrivilege SeRestorePrivilege SeDebugPrivilege SeAuditPrivilege SeSystemEnvironmentPrivilege SeImpersonatePrivilege
Security	Audit Success	12544	2015-04-29 11:34:23	Microsoft-Windows-Security-Auditing	4648: A logon was attempted using explicit credentials. Subject: Security ID: S-1-5-18 Account Name: LTRANPHD$ Account Domain: WORKGROUP Logon ID: 0x3e7 Logon GUID: {00000000-0000-0000-0000-000000000000} Account Whose Credentials Were Used: Account Name: Liem Account Domain: LTRANPHD Logon GUID: {00000000-0000-0000-0000-000000000000} Target Server: Target Server Name: localhost Additional Information: localhost Process Information: Process ID: 0x208 Process Name: C:\Windows\System32\winlogon.exe Network Information: Network Address: 127.0.0.1 Port: 0 This event is generated when a process attempts to log on an account by explicitly specifying that account's credentials. This most commonly occurs in batch-type configurations such as scheduled tasks, or when using the RUNAS command.
					4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: LTRANPHD$

Security	Audit Success	12544	2015-04-29 11:34:23	Microsoft-Windows-Security-Auditing	Account Domain: WORKGROUP Logon ID: 0x3e7 Logon Type: 2 Impersonation Level: %%1833 New Logon: Security ID: S-1-5-21-1888849264-3803429180-4108621888-1001 Account Name: Liem Account Domain: LTRANPHD Logon ID: 0x1ab21 Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x208 Process Name: C:\Windows\System32\winlogon.exe Network Information: Workstation Name: LTRANPHD Source Network Address: 127.0.0.1 Source Port: 0 Detailed Authentication Information: Logon Process: User32 Authentication Package: Negotiate Transited Services: - Package Name (NTLM only): - Key Length: 0 This event is generated when a logon session is created. It is generated on the computer that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service such as the Server service, or a local process such as Winlogon.exe or Services.exe. The logon type field indicates the kind of logon that occurred. The most common types are 2 (interactive) and 3 (network). The New Logon fields indicate the account for whom the new logon was created, i.e. the account that was logged on. The network fields indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impersonation level field indicates the extent to which a process in the logon session can impersonate. The authentication information fields provide detailed information about this specific logon request. - Logon GUID is a unique identifier that can be used to correlate this event with a KDC event. - Transited services indicate which intermediate services have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indicates the length of the generated session key. This will be 0 if no session key was requested.
Security	Audit Success	12544	2015-04-29 11:34:23	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: LTRANPHD$ Account Domain: WORKGROUP Logon ID: 0x3e7 Logon Type: 2 Impersonation Level: %%1833 New Logon: Security ID: S-1-5-21-1888849264-3803429180-4108621888-1001 Account Name: Liem Account Domain: LTRANPHD Logon ID: 0x1abf6 Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x208 Process Name: C:\Windows\System32\winlogon.exe Network Information: Workstation Name: LTRANPHD Source Network Address: 127.0.0.1 Source Port: 0 Detailed Authentication Information: Logon Process: User32 Authentication Package: Negotiate Transited Services: - Package Name (NTLM only): - Key Length: 0 This event is generated when a logon session is created. It is generated on the computer that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service such as the Server service, or a local process such as Winlogon.exe or Services.exe. The logon type field indicates the kind of logon that occurred. The most common types are 2 (interactive) and 3 (network). The New Logon fields indicate the account for whom the new logon was created, i.e. the account that was logged on. The network fields indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impersonation level field indicates the extent to which a process in the logon session can impersonate. The authentication information fields provide detailed information about this specific logon request. - Logon GUID is a unique identifier that can be used to correlate this event with a KDC event. - Transited services indicate which intermediate services have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indicates the length of the generated session key. This will be 0 if no session key was requested.
Security	Audit Success	12548	2015-04-29 11:34:23	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-21-1888849264-3803429180-4108621888-1001 Account Name: Liem Account Domain: LTRANPHD Logon ID: 0x1ab21 Privileges: SeSecurityPrivilege SeTakeOwnershipPrivilege SeLoadDriverPrivilege SeBackupPrivilege SeRestorePrivilege SeDebugPrivilege SeSystemEnvironmentPrivilege SeImpersonatePrivilege
Security	Audit Success	12544	2015-04-29 11:34:25	Microsoft-Windows-Security-Auditing	4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: LTRANPHD$ Account Domain: WORKGROUP Logon ID: 0x3e7 Logon Type: 5 Impersonation Level: %%1833 New Logon: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Logon ID: 0x3e7 Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x238 Process Name: C:\Windows\System32\services.exe Network Information: Workstation Name: Source Network Address: - Source Port: - Detailed Authentication Information: Logon Process: Advapi Authentication Package: Negotiate Transited Services: - Package Name (NTLM only): - Key Length: 0 This event is generated when a logon session is created. It is generated on the computer that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service such as the Server service, or a local process such as Winlogon.exe or Services.exe. The logon type field indicates the kind of logon that occurred. The most common types are 2 (interactive) and 3 (network). The New Logon fields indicate the account for whom the new logon was created, i.e. the account that was logged on. The network fields indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impersonation level field indicates the extent to which a process in the logon session can impersonate. The authentication information fields provide detailed information about this specific logon request. - Logon GUID is a unique identifier that can be used to correlate this event with a KDC event. - Transited services indicate which intermediate services have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indicates the length of the generated session key. This will be 0 if no session key was requested.
Security	Audit Success	12548	2015-04-29 11:34:25	Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Logon ID: 0x3e7 Privileges: SeAssignPrimaryTokenPrivilege SeTcbPrivilege SeSecurityPrivilege SeTakeOwnershipPrivilege SeLoadDriverPrivilege SeBackupPrivilege SeRestorePrivilege SeDebugPrivilege SeAuditPrivilege SeSystemEnvironmentPrivilege SeImpersonatePrivilege
Security	Audit	13824	2015-04-29	Microsoft-Windows-Security-	4797: An attempt was made to query the existence of a blank password for an account. Subject: Security ID: S-1-5-21-1888849264-3803429180-4108621888-1001 Account Name: Liem Account Domain: LTRANPHD Logon

	Success		11:34:27	Auditing	ID: 0x1abf6 Additional Information: Caller Workstation: LTRANPHD Target Account Name: Administrator Target Account Domain: LTRANPHD
Security	Audit Success	13824	2015-04-29 11:34:27	Microsoft-Windows-Security-Auditing	4797: An attempt was made to query the existence of a blank password for an account. Subject: Security ID: S-1-5-21-1888849264-3803429180-4108621888-1001 Account Name: Liem Account Domain: LTRANPHD Logon ID: 0x1abf6 Additional Information: Caller Workstation: LTRANPHD Target Account Name: Guest Target Account Domain: LTRANPHD
Security	Audit Success	13824	2015-04-29 11:34:27	Microsoft-Windows-Security-Auditing	4797: An attempt was made to query the existence of a blank password for an account. Subject: Security ID: S-1-5-21-1888849264-3803429180-4108621888-1001 Account Name: Liem Account Domain: LTRANPHD Logon ID: 0x1abf6 Additional Information: Caller Workstation: LTRANPHD Target Account Name: Administrator Target Account Domain: LTRANPHD
Security	Audit Success	13824	2015-04-29 11:34:27	Microsoft-Windows-Security-Auditing	4797: An attempt was made to query the existence of a blank password for an account. Subject: Security ID: S-1-5-21-1888849264-3803429180-4108621888-1001 Account Name: Liem Account Domain: LTRANPHD Logon ID: 0x1abf6 Additional Information: Caller Workstation: LTRANPHD Target Account Name: Guest Target Account Domain: LTRANPHD
Security	Audit Success	13824	2015-04-29 11:34:29	Microsoft-Windows-Security-Auditing	4797: An attempt was made to query the existence of a blank password for an account. Subject: Security ID: S-1-5-19 Account Name: LOCAL SERVICE Account Domain: NT AUTHORITY Logon ID: 0x3e5 Additional Information: Caller Workstation: LTRANPHD Target Account Name: Administrator Target Account Domain: LTRANPHD
Security	Audit Success	13824	2015-04-29 11:34:29	Microsoft-Windows-Security-Auditing	4797: An attempt was made to query the existence of a blank password for an account. Subject: Security ID: S-1-5-19 Account Name: LOCAL SERVICE Account Domain: NT AUTHORITY Logon ID: 0x3e5 Additional Information: Caller Workstation: LTRANPHD Target Account Name: Guest Target Account Domain: LTRANPHD
Security	Audit Success	13824	2015-04-29 11:34:29	Microsoft-Windows-Security-Auditing	4797: An attempt was made to query the existence of a blank password for an account. Subject: Security ID: S-1-5-19 Account Name: LOCAL SERVICE Account Domain: NT AUTHORITY Logon ID: 0x3e5 Additional Information: Caller Workstation: LTRANPHD Target Account Name: Liem Target Account Domain: LTRANPHD
Security	Audit Success	13824	2015-04-29 11:34:29	Microsoft-Windows-Security-Auditing	4797: An attempt was made to query the existence of a blank password for an account. Subject: Security ID: S-1-5-19 Account Name: LOCAL SERVICE Account Domain: NT AUTHORITY Logon ID: 0x3e5 Additional Information: Caller Workstation: LTRANPHD Target Account Name: Administrator Target Account Domain: LTRANPHD
Security	Audit Success	13824	2015-04-29 11:34:29	Microsoft-Windows-Security-Auditing	4797: An attempt was made to query the existence of a blank password for an account. Subject: Security ID: S-1-5-19 Account Name: LOCAL SERVICE Account Domain: NT AUTHORITY Logon ID: 0x3e5 Additional Information: Caller Workstation: LTRANPHD Target Account Name: Liem Target Account Domain: LTRANPHD
Security	Audit Success	13824	2015-04-29 11:34:29	Microsoft-Windows-Security-Auditing	4797: An attempt was made to query the existence of a blank password for an account. Subject: Security ID: S-1-5-19 Account Name: LOCAL SERVICE Account Domain: NT AUTHORITY Logon ID: 0x3e5 Additional Information: Caller Workstation: LTRANPHD Target Account Name: Guest Target Account Domain: LTRANPHD
Security	Audit Success	13824	2015-04-29 11:34:29	Microsoft-Windows-Security-Auditing	4797: An attempt was made to query the existence of a blank password for an account. Subject: Security ID: S-1-5-19 Account Name: LOCAL SERVICE Account Domain: NT AUTHORITY Logon ID: 0x3e5 Additional Information: Caller Workstation: LTRANPHD Target Account Name: Liem Target Account Domain: LTRANPHD
Security	Audit Success	13824	2015-04-29 11:34:29	Microsoft-Windows-Security-Auditing	4797: An attempt was made to query the existence of a blank password for an account. Subject: Security ID: S-1-5-19 Account Name: LOCAL SERVICE Account Domain: NT AUTHORITY Logon ID: 0x3e5 Additional Information: Caller Workstation: LTRANPHD Target Account Name: Liem Target Account Domain: LTRANPHD
Security	Audit Success	13824	2015-04-29 11:37:30	Microsoft-Windows-Security-Auditing	4797: An attempt was made to query the existence of a blank password for an account. Subject: Security ID: S-1-5-21-1888849264-3803429180-4108621888-1001 Account Name: Liem Account Domain: LTRANPHD Logon ID: 0x1abf6 Additional Information: Caller Workstation: LTRANPHD Target Account Name: Administrator Target Account Domain: LTRANPHD
Security	Audit Success	13824	2015-04-29 11:37:30	Microsoft-Windows-Security-Auditing	4797: An attempt was made to query the existence of a blank password for an account. Subject: Security ID: S-1-5-21-1888849264-3803429180-4108621888-1001 Account Name: Liem Account Domain: LTRANPHD Logon ID: 0x1abf6 Additional Information: Caller Workstation: LTRANPHD Target Account Name: Guest Target Account Domain: LTRANPHD
Security	Audit Success	13824	2015-04-29 11:37:30	Microsoft-Windows-Security-Auditing	4797: An attempt was made to query the existence of a blank password for an account. Subject: Security ID: S-1-5-21-1888849264-3803429180-4108621888-1001 Account Name: Liem Account Domain: LTRANPHD Logon ID: 0x1abf6 Additional Information: Caller Workstation: LTRANPHD Target Account Name: Administrator Target Account Domain: LTRANPHD
Security	Audit Success	13824	2015-04-29 11:37:30	Microsoft-Windows-Security-Auditing	4797: An attempt was made to query the existence of a blank password for an account. Subject: Security ID: S-1-5-21-1888849264-3803429180-4108621888-1001 Account Name: Liem Account Domain: LTRANPHD Logon ID: 0x1abf6 Additional Information: Caller Workstation: LTRANPHD Target Account Name: Guest Target Account Domain: LTRANPHD
					4624: An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: LTRANPHD$ Account Domain: WORKGROUP Logon ID: 0x3e7 Logon Type: 5 Impersonation Level: %%1833 New Logon: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Logon ID: 0x3e7 Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x238 Process Name: C:\Windows\System32\services.exe Network Information: Workstation Name: Source Network Address: - Source Port: - Detailed Authentication Information: Logon Process: Advapi Authentication Package: Negotiate Transited Services: - Package Name (NTLM only): - Key Length: 0 This event is generated when a logon session is created. It is generated on the computer that was accessed. The subject fields indicate the account on the local

	Security	Audit Success	12544	2015-04-29 11:39:02		Microsoft-Windows-Security-Auditing	system which requested the logon. This is most commonly a service such as the Server service, or a local process such as Winlogon.exe or Services.exe. The logon type field indicates the kind of logon that occurred. The most common types are 2 (interactive) and 3 (network). The New Logon fields indicate the account for whom the new logon was created, i.e. the account that was logged on. The network fields indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impersonation level field indicates the extent to which a process in the logon session can impersonate. The authentication information fields provide detailed information about this specific logon request. - Logon GUID is a unique identifier that can be used to correlate this event with a KDC event. - Transited services indicate which intermediate services have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indicates the length of the generated session key. This will be 0 if no session key was requested.
	Security	Audit Success	12548	2015-04-29 11:39:02		Microsoft-Windows-Security-Auditing	4672: Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Logon ID: 0x3e7 Privileges: SeAssignPrimaryTokenPrivilege SeTcbPrivilege SeSecurityPrivilege SeTakeOwnershipPrivilege SeLoadDriverPrivilege SeBackupPrivilege SeRestorePrivilege SeDebugPrivilege SeAuditPrivilege SeSystemEnvironmentPrivilege SeImpersonatePrivilege
	System	Warning	None	2015-04-22 16:22:19		BTHUSB	28: The local adapter does not support Bluetooth Low Energy.
	System	Warning	None	2015-04-22 16:22:20		k57nd60a	4: Broadcom NetLink (TM) Gigabit Ethernet: The network link is down. Check to make sure the network cable is properly connected.
	System	Warning	None	2015-04-22 18:07:15		k57nd60a	4: Broadcom NetLink (TM) Gigabit Ethernet: The network link is down. Check to make sure the network cable is properly connected.
	System	Warning	None	2015-04-22 18:52:57		k57nd60a	4: Broadcom NetLink (TM) Gigabit Ethernet: The network link is down. Check to make sure the network cable is properly connected.
	System	Error	None	2015-04-22 19:03:57	Liem	DCOM	10016: The application-specific permission settings do not grant Local Launch permission for the COM Server application with CLSID {7022A3B3-D004-4F52-AF11-E9E987FEE25F} and APPID {ADA41B3C-C6FD-4A08-8CC1-D6EFDE67BE7D} to the user LTRANPHD\Liem SID (S-1-5-21-1888849264-3803429180-4108621888-1001) from address LocalHost (Using LRPC) running in the application container Unavailable SID (Unavailable). This security permission can be modified using the Component Services administrative tool.
	System	Error	None	2015-04-22 19:04:19	Liem	DCOM	10016: The application-specific permission settings do not grant Local Launch permission for the COM Server application with CLSID {7022A3B3-D004-4F52-AF11-E9E987FEE25F} and APPID {ADA41B3C-C6FD-4A08-8CC1-D6EFDE67BE7D} to the user LTRANPHD\Liem SID (S-1-5-21-1888849264-3803429180-4108621888-1001) from address LocalHost (Using LRPC) running in the application container Unavailable SID (Unavailable). This security permission can be modified using the Component Services administrative tool.
	System	Warning	None	2015-04-22 19:05:13		k57nd60a	4: Broadcom NetLink (TM) Gigabit Ethernet: The network link is down. Check to make sure the network cable is properly connected.
	System	Error	None	2015-04-22 19:05:21		Service Control Manager	7023: The Intel(R) Content Protection HECI Service service terminated with the following error: %%2147942659
	System	Warning	None	2015-04-22 19:19:19		BTHUSB	28: The local adapter does not support Bluetooth Low Energy.
	System	Warning	None	2015-04-22 19:47:37		k57nd60a	4: Broadcom NetLink (TM) Gigabit Ethernet: The network link is down. Check to make sure the network cable is properly connected.
	System	Warning	None	2015-04-22 19:49:33		k57nd60a	4: Broadcom NetLink (TM) Gigabit Ethernet: The network link is down. Check to make sure the network cable is properly connected.
	System	Warning	None	2015-04-22 19:52:58		k57nd60a	4: Broadcom NetLink (TM) Gigabit Ethernet: The network link is down. Check to make sure the network cable is properly connected.
	System	Warning	None	2015-04-22 19:54:19		k57nd60a	4: Broadcom NetLink (TM) Gigabit Ethernet: The network link is down. Check to make sure the network cable is properly connected.
	System	Warning	None	2015-04-22 19:55:09		BTHUSB	28: The local adapter does not support Bluetooth Low Energy.
	System	Warning	None	2015-04-22 19:57:56		BTHUSB	28: The local adapter does not support Bluetooth Low Energy.

System	Warning	None	2015-04-22 20:18:21	BTHUSB	28: The local adapter does not support Bluetooth Low Energy.
System	Warning	None	2015-04-22 20:24:36	BTHUSB	28: The local adapter does not support Bluetooth Low Energy.
System	Error	None	2015-04-22 20:24:38	EventLog	6008: The previous system shutdown at 7:54:23 PM on ?4/?22/?2015 was unexpected.
System	Warning	None	2015-04-22 20:24:38	k57nd60a	4: Broadcom NetLink (TM) Gigabit Ethernet: The network link is down. Check to make sure the network cable is properly connected.
System	Warning	None	2015-04-22 20:56:12	BTHUSB	28: The local adapter does not support Bluetooth Low Energy.
System	Error	None	2015-04-22 20:56:14	EventLog	6008: The previous system shutdown at 8:41:45 PM on ?4/?22/?2015 was unexpected.
System	Warning	None	2015-04-22 20:56:14	k57nd60a	4: Broadcom NetLink (TM) Gigabit Ethernet: The network link is down. Check to make sure the network cable is properly connected.
System	Warning	None	2015-04-22 21:18:09	BTHUSB	28: The local adapter does not support Bluetooth Low Energy.
System	Warning	None	2015-04-22 21:18:10	k57nd60a	4: Broadcom NetLink (TM) Gigabit Ethernet: The network link is down. Check to make sure the network cable is properly connected.
System	Error	None	2015-04-22 21:33:48	bScsiSDa	15: The device, \Device\Scsi\bScsiSDa1, is not ready for access yet.
System	Error	None	2015-04-22 21:34:08	bScsiSDa	15: The device, \Device\Scsi\bScsiSDa1, is not ready for access yet.
System	Error	None	2015-04-22 21:34:28	bScsiSDa	15: The device, \Device\Scsi\bScsiSDa1, is not ready for access yet.
System	Warning	None	2015-04-23 07:23:44	BTHUSB	28: The local adapter does not support Bluetooth Low Energy.
System	Warning	None	2015-04-23 07:23:46	k57nd60a	4: Broadcom NetLink (TM) Gigabit Ethernet: The network link is down. Check to make sure the network cable is properly connected.
System	Error	None	2015-04-23 08:20:39	bScsiSDa	15: The device, \Device\Scsi\bScsiSDa1, is not ready for access yet.
System	Error	None	2015-04-23 08:20:59	bScsiSDa	15: The device, \Device\Scsi\bScsiSDa1, is not ready for access yet.
System	Error	None	2015-04-23 08:21:19	bScsiSDa	15: The device, \Device\Scsi\bScsiSDa1, is not ready for access yet.
System	Warning	None	2015-04-23 08:53:05	k57nd60a	4: Broadcom NetLink (TM) Gigabit Ethernet: The network link is down. Check to make sure the network cable is properly connected.
System	Warning	None	2015-04-23 08:53:05	BTHUSB	28: The local adapter does not support Bluetooth Low Energy.
System	Error	None	2015-04-23 08:53:11	EventLog	6008: The previous system shutdown at 8:27:49 AM on ?4/?23/?2015 was unexpected.
System	Error	None	2015-04-23 08:53:24	Service Control Manager	7024: The Windows Search service terminated with the following service-specific error: %%2147749126

	System	Error	None	2015-04-23 08:53:24		Service Control Manager	7031: The Windows Search service terminated unexpectedly. It has done this 1 time(s). The following corrective action will be taken in 30000 milliseconds: Restart the service.
	System	Error	None	2015-04-23 08:53:54		Service Control Manager	7032: The Service Control Manager tried to take a corrective action (Restart the service) after the unexpected termination of the Windows Search service, but this action failed with the following error: %%1056
	System	Error	None	2015-04-23 12:32:58		EventLog	6008: The previous system shutdown at 9:18:11 AM on ?4/?23/?2015 was unexpected.
	System	Warning	None	2015-04-23 12:32:58		BTHUSB	28: The local adapter does not support Bluetooth Low Energy.
	System	Warning	None	2015-04-23 12:33:00		k57nd60a	4: Broadcom NetLink (TM) Gigabit Ethernet: The network link is down. Check to make sure the network cable is properly connected.
	System	Warning	None	2015-04-24 17:31:51	LOCAL SERVICE	Microsoft-Windows-Time-Service	52: The time service has set the time with offset 2858395 seconds.
	System	Warning	None	2015-04-24 17:34:59		BTHUSB	28: The local adapter does not support Bluetooth Low Energy.
	System	Warning	None	2015-04-24 17:58:27		BTHUSB	28: The local adapter does not support Bluetooth Low Energy.
	System	Warning	None	2015-04-24 17:58:28		k57nd60a	4: Broadcom NetLink (TM) Gigabit Ethernet: The network link is down. Check to make sure the network cable is properly connected.
	System	Error	None	2015-04-24 17:58:33		EventLog	6008: The previous system shutdown at 5:57:36 PM on ?4/?24/?2015 was unexpected.
	System	Warning	None	2015-04-24 18:00:42		BTHUSB	28: The local adapter does not support Bluetooth Low Energy.
	System	Warning	None	2015-04-24 18:00:43		k57nd60a	4: Broadcom NetLink (TM) Gigabit Ethernet: The network link is down. Check to make sure the network cable is properly connected.
	System	Warning	None	2015-04-24 18:10:35		BTHUSB	28: The local adapter does not support Bluetooth Low Energy.
	System	Warning	None	2015-04-24 18:10:36		k57nd60a	4: Broadcom NetLink (TM) Gigabit Ethernet: The network link is down. Check to make sure the network cable is properly connected.
	System	Error	None	2015-04-24 18:21:22	Liem	DCOM	10010: The server {1B1F472E-3221-4826-97DB-2C2324D389AE} did not register with DCOM within the required timeout.
	System	Error	None	2015-04-24 18:21:52	Liem	DCOM	10010: The server {BF6C1E47-86EC-4194-9CE5-13C15DCB2001} did not register with DCOM within the required timeout.
	System	Error	None	2015-04-24 19:01:19		EventLog	6008: The previous system shutdown at 6:39:35 PM on ?4/?24/?2015 was unexpected.
	System	Warning	None	2015-04-24 19:01:20		BTHUSB	28: The local adapter does not support Bluetooth Low Energy.
	System	Warning	None	2015-04-24 19:01:21		k57nd60a	4: Broadcom NetLink (TM) Gigabit Ethernet: The network link is down. Check to make sure the network cable is properly connected.
	System	Warning	None	2015-04-24 19:37:34		BTHUSB	28: The local adapter does not support Bluetooth Low Energy.
	System	Warning	None	2015-04-24		k57nd60a	4: Broadcom NetLink (TM) Gigabit Ethernet: The network link is down. Check to make sure the network cable is properly connected.

			19:37:36			
	System	Error	None	2015-04-24 19:37:46	volmgr	46: Crash dump initialization failed!
	System	Error	None	2015-04-24 19:37:49	EventLog	6008: The previous system shutdown at 7:30:19 PM on ?4/?24/?2015 was unexpected.
	System	Warning	None	2015-04-24 19:37:49	BTHUSB	28: The local adapter does not support Bluetooth Low Energy.
	System	Warning	None	2015-04-24 19:37:51	k57nd60a	4: Broadcom NetLink (TM) Gigabit Ethernet: The network link is down. Check to make sure the network cable is properly connected.
	System	Warning	None	2015-04-24 19:41:54	BTHUSB	28: The local adapter does not support Bluetooth Low Energy.
	System	Warning	None	2015-04-24 19:41:55	k57nd60a	4: Broadcom NetLink (TM) Gigabit Ethernet: The network link is down. Check to make sure the network cable is properly connected.
	System	Error	None	2015-04-24 20:35:19	EventLog	6008: The previous system shutdown at 8:10:54 PM on ?4/?24/?2015 was unexpected.
	System	Warning	None	2015-04-24 20:35:19	BTHUSB	28: The local adapter does not support Bluetooth Low Energy.
	System	Warning	None	2015-04-24 20:35:20	k57nd60a	4: Broadcom NetLink (TM) Gigabit Ethernet: The network link is down. Check to make sure the network cable is properly connected.
	System	Error	None	2015-04-24 20:35:24	Service Control Manager	7024: The Windows Search service terminated with the following service-specific error: %%2147749126
	System	Error	None	2015-04-24 20:35:24	Service Control Manager	7031: The Windows Search service terminated unexpectedly. It has done this 1 time(s). The following corrective action will be taken in 30000 milliseconds: Restart the service.
	System	Error	None	2015-04-24 20:35:54	Service Control Manager	7032: The Service Control Manager tried to take a corrective action (Restart the service) after the unexpected termination of the Windows Search service, but this action failed with the following error: %%1056
	System	Warning	None	2015-04-24 20:47:07	k57nd60a	4: Broadcom NetLink (TM) Gigabit Ethernet: The network link is down. Check to make sure the network cable is properly connected.
	System	Error	None	2015-04-24 20:47:14	Liem DCOM	10005: DCOM got error "1084" attempting to start the service ShellHWDetection with arguments "Unavailable" in order to run the server: {DD522ACC-F821-461A-A407-50B198B896DC}
	System	Error	None	2015-04-24 20:47:14	Liem DCOM	10005: DCOM got error "1084" attempting to start the service ShellHWDetection with arguments "Unavailable" in order to run the server: {DD522ACC-F821-461A-A407-50B198B896DC}
	System	Error	None	2015-04-24 20:47:14	Liem DCOM	10005: DCOM got error "1084" attempting to start the service EventSystem with arguments "Unavailable" in order to run the server: {1BE1F766-5536-11D1-B726-00C04FB926AF}
	System	Error	None	2015-04-24 20:47:15	Liem DCOM	10005: DCOM got error "1084" attempting to start the service WSearch with arguments "Unavailable" in order to run the server: {9E175B68-F52A-11D8-B9A5-505054503030}
	System	Error	None	2015-04-24 20:47:15	Liem DCOM	10005: DCOM got error "1084" attempting to start the service WSearch with arguments "Unavailable" in order to run the server: {9E175B68-F52A-11D8-B9A5-505054503030}
	System	Error	None	2015-04-24 20:47:15	Liem DCOM	10005: DCOM got error "1084" attempting to start the service WSearch with arguments "Unavailable" in order to run the server: {7D096C5F-AC08-4F1F-BEB7-5C22C517CE39}
	System	Error	None	2015-04-24 20:47:21	Liem DCOM	10005: DCOM got error "1084" attempting to start the service ShellHWDetection with arguments "Unavailable" in order to run the server: {DD522ACC-F821-461A-A407-50B198B896DC}
				2015-04-		10005: DCOM got error "1084" attempting to start the service WSearch with arguments "Unavailable" in order

System	Error	None	24 20:47:21	Liem	DCOM	to run the server: {B52D54BB-4818-4EB9-AA80-F9EACD371DF8}
System	Error	None	2015-04-24 20:47:21	Liem	DCOM	10005: DCOM got error "1084" attempting to start the service WSearch with arguments "Unavailable" in order to run the server: {B52D54BB-4818-4EB9-AA80-F9EACD371DF8}
System	Error	None	2015-04-24 20:47:21	Liem	DCOM	10005: DCOM got error "1084" attempting to start the service WSearch with arguments "Unavailable" in order to run the server: {B52D54BB-4818-4EB9-AA80-F9EACD371DF8}
System	Error	None	2015-04-24 20:47:21	Liem	DCOM	10005: DCOM got error "1084" attempting to start the service WSearch with arguments "Unavailable" in order to run the server: {B52D54BB-4818-4EB9-AA80-F9EACD371DF8}
System	Error	None	2015-04-24 20:47:21	Liem	DCOM	10005: DCOM got error "1084" attempting to start the service WSearch with arguments "Unavailable" in order to run the server: {B52D54BB-4818-4EB9-AA80-F9EACD371DF8}
System	Error	None	2015-04-24 20:47:21	Liem	DCOM	10005: DCOM got error "1084" attempting to start the service WSearch with arguments "Unavailable" in order to run the server: {B52D54BB-4818-4EB9-AA80-F9EACD371DF8}
System	Error	None	2015-04-24 20:47:21	Liem	DCOM	10005: DCOM got error "1084" attempting to start the service WSearch with arguments "Unavailable" in order to run the server: {B52D54BB-4818-4EB9-AA80-F9EACD371DF8}
System	Error	None	2015-04-24 20:47:21	Liem	DCOM	10005: DCOM got error "1084" attempting to start the service WSearch with arguments "Unavailable" in order to run the server: {B52D54BB-4818-4EB9-AA80-F9EACD371DF8}
System	Error	None	2015-04-24 20:47:21	Liem	DCOM	10005: DCOM got error "1084" attempting to start the service WSearch with arguments "Unavailable" in order to run the server: {B52D54BB-4818-4EB9-AA80-F9EACD371DF8}
System	Error	None	2015-04-24 20:47:21	Liem	DCOM	10005: DCOM got error "1084" attempting to start the service WSearch with arguments "Unavailable" in order to run the server: {B52D54BB-4818-4EB9-AA80-F9EACD371DF8}
System	Error	None	2015-04-24 20:47:21	Liem	DCOM	10005: DCOM got error "1084" attempting to start the service WSearch with arguments "Unavailable" in order to run the server: {B52D54BB-4818-4EB9-AA80-F9EACD371DF8}
System	Error	None	2015-04-24 20:47:21	Liem	DCOM	10005: DCOM got error "1084" attempting to start the service WSearch with arguments "Unavailable" in order to run the server: {B52D54BB-4818-4EB9-AA80-F9EACD371DF8}
System	Error	None	2015-04-24 20:47:22	Liem	DCOM	10005: DCOM got error "1084" attempting to start the service WSearch with arguments "Unavailable" in order to run the server: {B52D54BB-4818-4EB9-AA80-F9EACD371DF8}
System	Error	None	2015-04-24 20:47:22	Liem	DCOM	10005: DCOM got error "1084" attempting to start the service WSearch with arguments "Unavailable" in order to run the server: {B52D54BB-4818-4EB9-AA80-F9EACD371DF8}
System	Error	None	2015-04-24 20:47:22	Liem	DCOM	10005: DCOM got error "1084" attempting to start the service WSearch with arguments "Unavailable" in order to run the server: {B52D54BB-4818-4EB9-AA80-F9EACD371DF8}
System	Error	None	2015-04-24 20:47:22	Liem	DCOM	10005: DCOM got error "1084" attempting to start the service WSearch with arguments "Unavailable" in order to run the server: {B52D54BB-4818-4EB9-AA80-F9EACD371DF8}
System	Error	None	2015-04-24 20:47:22	Liem	DCOM	10005: DCOM got error "1084" attempting to start the service WSearch with arguments "Unavailable" in order to run the server: {B52D54BB-4818-4EB9-AA80-F9EACD371DF8}
System	Error	None	2015-04-24 20:47:22	Liem	DCOM	10005: DCOM got error "1084" attempting to start the service WSearch with arguments "Unavailable" in order to run the server: {B52D54BB-4818-4EB9-AA80-F9EACD371DF8}
System	Error	None	2015-04-24 20:47:22	Liem	DCOM	10005: DCOM got error "1084" attempting to start the service WSearch with arguments "Unavailable" in order to run the server: {B52D54BB-4818-4EB9-AA80-F9EACD371DF8}
System	Error	None	2015-04-24 20:47:22	Liem	DCOM	10005: DCOM got error "1084" attempting to start the service WSearch with arguments "Unavailable" in order to run the server: {B52D54BB-4818-4EB9-AA80-F9EACD371DF8}
System	Error	None	2015-04-24 20:47:22	Liem	DCOM	10005: DCOM got error "1084" attempting to start the service WSearch with arguments "Unavailable" in order to run the server: {B52D54BB-4818-4EB9-AA80-F9EACD371DF8}

System	Error	None	2015-04-24 20:47:22	Liem	DCOM	10005: DCOM got error "1084" attempting to start the service WSearch with arguments "Unavailable" in order to run the server: {B52D54BB-4818-4EB9-AA80-F9EACD371DF8}
System	Error	None	2015-04-24 20:47:22	Liem	DCOM	10005: DCOM got error "1084" attempting to start the service WSearch with arguments "Unavailable" in order to run the server: {B52D54BB-4818-4EB9-AA80-F9EACD371DF8}
System	Error	None	2015-04-24 20:47:22	Liem	DCOM	10005: DCOM got error "1084" attempting to start the service WSearch with arguments "Unavailable" in order to run the server: {B52D54BB-4818-4EB9-AA80-F9EACD371DF8}
System	Error	None	2015-04-24 20:47:22	Liem	DCOM	10005: DCOM got error "1084" attempting to start the service WSearch with arguments "Unavailable" in order to run the server: {B52D54BB-4818-4EB9-AA80-F9EACD371DF8}
System	Error	None	2015-04-24 20:47:22	Liem	DCOM	10005: DCOM got error "1084" attempting to start the service WSearch with arguments "Unavailable" in order to run the server: {B52D54BB-4818-4EB9-AA80-F9EACD371DF8}
System	Error	None	2015-04-24 20:47:22	Liem	DCOM	10005: DCOM got error "1084" attempting to start the service WSearch with arguments "Unavailable" in order to run the server: {B52D54BB-4818-4EB9-AA80-F9EACD371DF8}
System	Error	None	2015-04-24 20:47:22	Liem	DCOM	10005: DCOM got error "1084" attempting to start the service WSearch with arguments "Unavailable" in order to run the server: {B52D54BB-4818-4EB9-AA80-F9EACD371DF8}
System	Error	None	2015-04-24 20:47:22	Liem	DCOM	10005: DCOM got error "1084" attempting to start the service WSearch with arguments "Unavailable" in order to run the server: {B52D54BB-4818-4EB9-AA80-F9EACD371DF8}
System	Error	None	2015-04-24 20:47:22	Liem	DCOM	10005: DCOM got error "1084" attempting to start the service WSearch with arguments "Unavailable" in order to run the server: {B52D54BB-4818-4EB9-AA80-F9EACD371DF8}
System	Error	None	2015-04-24 20:47:22	Liem	DCOM	10005: DCOM got error "1084" attempting to start the service WSearch with arguments "Unavailable" in order to run the server: {B52D54BB-4818-4EB9-AA80-F9EACD371DF8}
System	Error	None	2015-04-24 20:47:22	Liem	DCOM	10005: DCOM got error "1084" attempting to start the service WSearch with arguments "Unavailable" in order to run the server: {B52D54BB-4818-4EB9-AA80-F9EACD371DF8}
System	Error	None	2015-04-24 20:47:22	Liem	DCOM	10005: DCOM got error "1084" attempting to start the service WSearch with arguments "Unavailable" in order to run the server: {B52D54BB-4818-4EB9-AA80-F9EACD371DF8}
System	Error	None	2015-04-24 20:47:22	Liem	DCOM	10005: DCOM got error "1084" attempting to start the service WSearch with arguments "Unavailable" in order to run the server: {B52D54BB-4818-4EB9-AA80-F9EACD371DF8}
System	Error	None	2015-04-24 20:47:22	Liem	DCOM	10005: DCOM got error "1084" attempting to start the service WSearch with arguments "Unavailable" in order to run the server: {B52D54BB-4818-4EB9-AA80-F9EACD371DF8}
System	Error	None	2015-04-24 20:47:22	Liem	DCOM	10005: DCOM got error "1084" attempting to start the service WSearch with arguments "Unavailable" in order to run the server: {B52D54BB-4818-4EB9-AA80-F9EACD371DF8}
System	Error	None	2015-04-24 20:47:22	Liem	DCOM	10005: DCOM got error "1084" attempting to start the service WSearch with arguments "Unavailable" in order to run the server: {B52D54BB-4818-4EB9-AA80-F9EACD371DF8}
System	Error	None	2015-04-24 20:47:22	Liem	DCOM	10005: DCOM got error "1084" attempting to start the service WSearch with arguments "Unavailable" in order to run the server: {B52D54BB-4818-4EB9-AA80-F9EACD371DF8}
System	Error	None	2015-04-24 20:47:22	Liem	DCOM	10005: DCOM got error "1084" attempting to start the service WSearch with arguments "Unavailable" in order to run the server: {B52D54BB-4818-4EB9-AA80-F9EACD371DF8}
System	Error	None	2015-04-24 20:47:22	Liem	DCOM	10005: DCOM got error "1084" attempting to start the service WSearch with arguments "Unavailable" in order to run the server: {B52D54BB-4818-4EB9-AA80-F9EACD371DF8}
System	Error	None	2015-04-24 20:47:22	Liem	DCOM	10005: DCOM got error "1084" attempting to start the service WSearch with arguments "Unavailable" in order to run the server: {B52D54BB-4818-4EB9-AA80-F9EACD371DF8}
System	Error	None	2015-04-24 20:47:22	Liem	DCOM	10005: DCOM got error "1084" attempting to start the service WSearch with arguments "Unavailable" in order to run the server: {B52D54BB-4818-4EB9-AA80-F9EACD371DF8}
System	Error	None	2015-04-24 20:47:22	Liem	DCOM	10005: DCOM got error "1084" attempting to start the service WSearch with arguments "Unavailable" in order to run the server: {B52D54BB-4818-4EB9-AA80-F9EACD371DF8}
System	Error	None	2015-04-24 20:47:22	Liem	DCOM	10005: DCOM got error "1084" attempting to start the service WSearch with arguments "Unavailable" in order to run the server: {B52D54BB-4818-4EB9-AA80-F9EACD371DF8}
System	Error	None	2015-04-24 20:47:22	Liem	DCOM	10005: DCOM got error "1084" attempting to start the service WSearch with arguments "Unavailable" in order to run the server: {B52D54BB-4818-4EB9-AA80-F9EACD371DF8}
System	Error	None	2015-04-24 20:47:22	Liem	DCOM	10005: DCOM got error "1084" attempting to start the service WSearch with arguments "Unavailable" in order to run the server: {B52D54BB-4818-4EB9-AA80-F9EACD371DF8}

System	Error	None	2015-04-24 20:47:22	Liem	DCOM	10005: DCOM got error "1084" attempting to start the service WSearch with arguments "Unavailable" in order to run the server: {B52D54BB-4818-4EB9-AA80-F9EACD371DF8}
System	Error	None	2015-04-24 20:47:22	Liem	DCOM	10005: DCOM got error "1084" attempting to start the service WSearch with arguments "Unavailable" in order to run the server: {B52D54BB-4818-4EB9-AA80-F9EACD371DF8}
System	Error	None	2015-04-24 20:47:22	Liem	DCOM	10005: DCOM got error "1084" attempting to start the service WSearch with arguments "Unavailable" in order to run the server: {B52D54BB-4818-4EB9-AA80-F9EACD371DF8}
System	Error	None	2015-04-24 20:47:22	Liem	DCOM	10005: DCOM got error "1084" attempting to start the service WSearch with arguments "Unavailable" in order to run the server: {B52D54BB-4818-4EB9-AA80-F9EACD371DF8}
System	Error	None	2015-04-24 20:47:22	Liem	DCOM	10005: DCOM got error "1084" attempting to start the service WSearch with arguments "Unavailable" in order to run the server: {B52D54BB-4818-4EB9-AA80-F9EACD371DF8}
System	Error	None	2015-04-24 20:47:22	Liem	DCOM	10005: DCOM got error "1084" attempting to start the service WSearch with arguments "Unavailable" in order to run the server: {B52D54BB-4818-4EB9-AA80-F9EACD371DF8}
System	Error	None	2015-04-24 20:47:22	Liem	DCOM	10005: DCOM got error "1084" attempting to start the service WSearch with arguments "Unavailable" in order to run the server: {B52D54BB-4818-4EB9-AA80-F9EACD371DF8}
System	Error	None	2015-04-24 20:47:22	Liem	DCOM	10005: DCOM got error "1084" attempting to start the service WSearch with arguments "Unavailable" in order to run the server: {B52D54BB-4818-4EB9-AA80-F9EACD371DF8}
System	Error	None	2015-04-24 20:47:22	Liem	DCOM	10005: DCOM got error "1084" attempting to start the service WSearch with arguments "Unavailable" in order to run the server: {B52D54BB-4818-4EB9-AA80-F9EACD371DF8}
System	Error	None	2015-04-24 20:47:22	Liem	DCOM	10005: DCOM got error "1084" attempting to start the service WSearch with arguments "Unavailable" in order to run the server: {B52D54BB-4818-4EB9-AA80-F9EACD371DF8}
System	Error	None	2015-04-24 20:47:22	Liem	DCOM	10005: DCOM got error "1084" attempting to start the service WSearch with arguments "Unavailable" in order to run the server: {B52D54BB-4818-4EB9-AA80-F9EACD371DF8}
System	Error	None	2015-04-24 20:47:22	Liem	DCOM	10005: DCOM got error "1084" attempting to start the service WSearch with arguments "Unavailable" in order to run the server: {B52D54BB-4818-4EB9-AA80-F9EACD371DF8}
System	Error	None	2015-04-24 20:47:29	Liem	DCOM	10005: DCOM got error "1084" attempting to start the service ShellHWDetection with arguments "Unavailable" in order to run the server: {DD522ACC-F821-461A-A407-50B198B896DC}
System	Error	None	2015-04-24 20:47:29	Liem	DCOM	10005: DCOM got error "1084" attempting to start the service WSearch with arguments "Unavailable" in order to run the server: {B52D54BB-4818-4EB9-AA80-F9EACD371DF8}
System	Error	None	2015-04-24 20:47:29	Liem	DCOM	10005: DCOM got error "1084" attempting to start the service WSearch with arguments "Unavailable" in order to run the server: {B52D54BB-4818-4EB9-AA80-F9EACD371DF8}
System	Error	None	2015-04-24 20:47:30	Liem	DCOM	10005: DCOM got error "1084" attempting to start the service WSearch with arguments "Unavailable" in order to run the server: {B52D54BB-4818-4EB9-AA80-F9EACD371DF8}
System	Error	None	2015-04-24 20:47:30	Liem	DCOM	10005: DCOM got error "1084" attempting to start the service WSearch with arguments "Unavailable" in order to run the server: {B52D54BB-4818-4EB9-AA80-F9EACD371DF8}
System	Error	None	2015-04-24 20:47:30	Liem	DCOM	10005: DCOM got error "1084" attempting to start the service WSearch with arguments "Unavailable" in order to run the server: {B52D54BB-4818-4EB9-AA80-F9EACD371DF8}
System	Error	None	2015-04-24 20:47:30	Liem	DCOM	10005: DCOM got error "1084" attempting to start the service WSearch with arguments "Unavailable" in order to run the server: {B52D54BB-4818-4EB9-AA80-F9EACD371DF8}
System	Error	None	2015-04-24 20:47:42	Liem	DCOM	10005: DCOM got error "1084" attempting to start the service ShellHWDetection with arguments "Unavailable" in order to run the server: {DD522ACC-F821-461A-A407-50B198B896DC}
System	Error	None	2015-04-24 20:47:42	Liem	DCOM	10005: DCOM got error "1084" attempting to start the service WSearch with arguments "Unavailable" in order to run the server: {B52D54BB-4818-4EB9-AA80-F9EACD371DF8}

System	Error	None	2015-04-24 20:47:42	Liem	DCOM	10005: DCOM got error "1084" attempting to start the service WSearch with arguments "Unavailable" in order to run the server: {B52D54BB-4818-4EB9-AA80-F9EACD371DF8}
System	Error	None	2015-04-24 20:47:43	Liem	DCOM	10005: DCOM got error "1084" attempting to start the service WSearch with arguments "Unavailable" in order to run the server: {B52D54BB-4818-4EB9-AA80-F9EACD371DF8}
System	Error	None	2015-04-24 20:47:43	Liem	DCOM	10005: DCOM got error "1084" attempting to start the service WSearch with arguments "Unavailable" in order to run the server: {B52D54BB-4818-4EB9-AA80-F9EACD371DF8}
System	Error	None	2015-04-24 20:47:43	Liem	DCOM	10005: DCOM got error "1084" attempting to start the service WSearch with arguments "Unavailable" in order to run the server: {B52D54BB-4818-4EB9-AA80-F9EACD371DF8}
System	Error	None	2015-04-24 20:47:43	Liem	DCOM	10005: DCOM got error "1084" attempting to start the service WSearch with arguments "Unavailable" in order to run the server: {B52D54BB-4818-4EB9-AA80-F9EACD371DF8}
System	Error	None	2015-04-24 20:47:43	Liem	DCOM	10005: DCOM got error "1084" attempting to start the service WSearch with arguments "Unavailable" in order to run the server: {B52D54BB-4818-4EB9-AA80-F9EACD371DF8}
System	Error	None	2015-04-24 20:47:43	Liem	DCOM	10005: DCOM got error "1084" attempting to start the service WSearch with arguments "Unavailable" in order to run the server: {B52D54BB-4818-4EB9-AA80-F9EACD371DF8}
System	Error	None	2015-04-24 20:47:43	Liem	DCOM	10005: DCOM got error "1084" attempting to start the service WSearch with arguments "Unavailable" in order to run the server: {B52D54BB-4818-4EB9-AA80-F9EACD371DF8}
System	Error	None	2015-04-24 20:47:43	Liem	DCOM	10005: DCOM got error "1084" attempting to start the service WSearch with arguments "Unavailable" in order to run the server: {B52D54BB-4818-4EB9-AA80-F9EACD371DF8}
System	Error	None	2015-04-24 20:47:43	Liem	DCOM	10005: DCOM got error "1084" attempting to start the service WSearch with arguments "Unavailable" in order to run the server: {B52D54BB-4818-4EB9-AA80-F9EACD371DF8}
System	Error	None	2015-04-24 20:47:43	Liem	DCOM	10005: DCOM got error "1084" attempting to start the service WSearch with arguments "Unavailable" in order to run the server: {B52D54BB-4818-4EB9-AA80-F9EACD371DF8}
System	Error	None	2015-04-24 20:47:43	Liem	DCOM	10005: DCOM got error "1084" attempting to start the service WSearch with arguments "Unavailable" in order to run the server: {B52D54BB-4818-4EB9-AA80-F9EACD371DF8}
System	Error	None	2015-04-24 20:47:43	Liem	DCOM	10005: DCOM got error "1084" attempting to start the service WSearch with arguments "Unavailable" in order to run the server: {B52D54BB-4818-4EB9-AA80-F9EACD371DF8}
System	Error	None	2015-04-24 20:47:43	Liem	DCOM	10005: DCOM got error "1084" attempting to start the service WSearch with arguments "Unavailable" in order to run the server: {B52D54BB-4818-4EB9-AA80-F9EACD371DF8}
System	Error	None	2015-04-24 20:47:43	Liem	DCOM	10005: DCOM got error "1084" attempting to start the service WSearch with arguments "Unavailable" in order to run the server: {B52D54BB-4818-4EB9-AA80-F9EACD371DF8}
System	Error	None	2015-04-24 20:47:43	Liem	DCOM	10005: DCOM got error "1084" attempting to start the service WSearch with arguments "Unavailable" in order to run the server: {B52D54BB-4818-4EB9-AA80-F9EACD371DF8}
System	Error	None	2015-04-24 20:47:43	Liem	DCOM	10005: DCOM got error "1084" attempting to start the service WSearch with arguments "Unavailable" in order to run the server: {B52D54BB-4818-4EB9-AA80-F9EACD371DF8}
System	Error	None	2015-04-24 20:47:43	Liem	DCOM	10005: DCOM got error "1084" attempting to start the service WSearch with arguments "Unavailable" in order to run the server: {B52D54BB-4818-4EB9-AA80-F9EACD371DF8}
System	Error	None	2015-04-24 20:47:43	Liem	DCOM	10005: DCOM got error "1084" attempting to start the service WSearch with arguments "Unavailable" in order to run the server: {B52D54BB-4818-4EB9-AA80-F9EACD371DF8}
System	Error	None	2015-04-24 20:47:43	Liem	DCOM	10005: DCOM got error "1084" attempting to start the service WSearch with arguments "Unavailable" in order to run the server: {B52D54BB-4818-4EB9-AA80-F9EACD371DF8}
System	Error	None	2015-04-24	Liem	DCOM	10005: DCOM got error "1084" attempting to start the service WSearch with arguments "Unavailable" in order to run the server: {B52D54BB-4818-4EB9-AA80-F9EACD371DF8}

			20:47:43			
System	Error	None	2015-04-24 20:47:43	Liem	DCOM	10005: DCOM got error "1084" attempting to start the service WSearch with arguments "Unavailable" in order to run the server: {B52D54BB-4818-4EB9-AA80-F9EACD371DF8}
System	Error	None	2015-04-24 20:47:43	Liem	DCOM	10005: DCOM got error "1084" attempting to start the service WSearch with arguments "Unavailable" in order to run the server: {B52D54BB-4818-4EB9-AA80-F9EACD371DF8}
System	Error	None	2015-04-24 20:47:43	Liem	DCOM	10005: DCOM got error "1084" attempting to start the service WSearch with arguments "Unavailable" in order to run the server: {B52D54BB-4818-4EB9-AA80-F9EACD371DF8}
System	Error	None	2015-04-24 20:47:43	Liem	DCOM	10005: DCOM got error "1084" attempting to start the service WSearch with arguments "Unavailable" in order to run the server: {B52D54BB-4818-4EB9-AA80-F9EACD371DF8}
System	Error	None	2015-04-24 20:47:43	Liem	DCOM	10005: DCOM got error "1084" attempting to start the service WSearch with arguments "Unavailable" in order to run the server: {B52D54BB-4818-4EB9-AA80-F9EACD371DF8}
System	Error	None	2015-04-24 20:47:43	Liem	DCOM	10005: DCOM got error "1084" attempting to start the service WSearch with arguments "Unavailable" in order to run the server: {B52D54BB-4818-4EB9-AA80-F9EACD371DF8}
System	Error	None	2015-04-24 20:47:43	Liem	DCOM	10005: DCOM got error "1084" attempting to start the service WSearch with arguments "Unavailable" in order to run the server: {B52D54BB-4818-4EB9-AA80-F9EACD371DF8}
System	Error	None	2015-04-24 20:47:43	Liem	DCOM	10005: DCOM got error "1084" attempting to start the service WSearch with arguments "Unavailable" in order to run the server: {B52D54BB-4818-4EB9-AA80-F9EACD371DF8}
System	Error	None	2015-04-24 20:47:43	Liem	DCOM	10005: DCOM got error "1084" attempting to start the service WSearch with arguments "Unavailable" in order to run the server: {B52D54BB-4818-4EB9-AA80-F9EACD371DF8}
System	Error	None	2015-04-24 20:47:43	Liem	DCOM	10005: DCOM got error "1084" attempting to start the service WSearch with arguments "Unavailable" in order to run the server: {B52D54BB-4818-4EB9-AA80-F9EACD371DF8}
System	Error	None	2015-04-24 20:47:43	Liem	DCOM	10005: DCOM got error "1084" attempting to start the service WSearch with arguments "Unavailable" in order to run the server: {B52D54BB-4818-4EB9-AA80-F9EACD371DF8}
System	Error	None	2015-04-24 20:47:43	Liem	DCOM	10005: DCOM got error "1084" attempting to start the service WSearch with arguments "Unavailable" in order to run the server: {B52D54BB-4818-4EB9-AA80-F9EACD371DF8}
System	Error	None	2015-04-24 20:47:43	Liem	DCOM	10005: DCOM got error "1084" attempting to start the service WSearch with arguments "Unavailable" in order to run the server: {B52D54BB-4818-4EB9-AA80-F9EACD371DF8}
System	Error	None	2015-04-24 20:47:43	Liem	DCOM	10005: DCOM got error "1084" attempting to start the service WSearch with arguments "Unavailable" in order to run the server: {B52D54BB-4818-4EB9-AA80-F9EACD371DF8}
System	Error	None	2015-04-24 20:47:43	Liem	DCOM	10005: DCOM got error "1084" attempting to start the service WSearch with arguments "Unavailable" in order to run the server: {B52D54BB-4818-4EB9-AA80-F9EACD371DF8}
System	Error	None	2015-04-24 20:47:43	Liem	DCOM	10005: DCOM got error "1084" attempting to start the service WSearch with arguments "Unavailable" in order to run the server: {B52D54BB-4818-4EB9-AA80-F9EACD371DF8}
System	Error	None	2015-04-24 20:47:43	Liem	DCOM	10005: DCOM got error "1084" attempting to start the service WSearch with arguments "Unavailable" in order to run the server: {B52D54BB-4818-4EB9-AA80-F9EACD371DF8}
System	Error	None	2015-04-24 20:47:43	Liem	DCOM	10005: DCOM got error "1084" attempting to start the service WSearch with arguments "Unavailable" in order to run the server: {B52D54BB-4818-4EB9-AA80-F9EACD371DF8}
System	Error	None	2015-04-24 20:47:43	Liem	DCOM	10005: DCOM got error "1084" attempting to start the service WSearch with arguments "Unavailable" in order to run the server: {B52D54BB-4818-4EB9-AA80-F9EACD371DF8}
System	Error	None	2015-04-24 20:47:43	Liem	DCOM	10005: DCOM got error "1084" attempting to start the service WSearch with arguments "Unavailable" in order to run the server: {B52D54BB-4818-4EB9-AA80-F9EACD371DF8}
			2015-04-			10005: DCOM got error "1084" attempting to start the service WSearch with arguments "Unavailable" in order

System	Error	None	24 20:47:43	Liem	DCOM	to run the server: {B52D54BB-4818-4EB9-AA80-F9EACD371DF8}
System	Error	None	2015-04-24 20:47:43	Liem	DCOM	10005: DCOM got error "1084" attempting to start the service WSearch with arguments "Unavailable" in order to run the server: {B52D54BB-4818-4EB9-AA80-F9EACD371DF8}
System	Error	None	2015-04-24 20:47:52	Liem	DCOM	10005: DCOM got error "1084" attempting to start the service ShellHWDetection with arguments "Unavailable" in order to run the server: {DD522ACC-F821-461A-A407-50B198B896DC}
System	Error	None	2015-04-24 20:47:59	Liem	DCOM	10005: DCOM got error "1084" attempting to start the service ShellHWDetection with arguments "Unavailable" in order to run the server: {DD522ACC-F821-461A-A407-50B198B896DC}
System	Error	None	2015-04-24 20:48:01	Liem	DCOM	10005: DCOM got error "1084" attempting to start the service WSearch with arguments "Unavailable" in order to run the server: {B52D54BB-4818-4EB9-AA80-F9EACD371DF8}
System	Error	None	2015-04-24 20:48:01	Liem	DCOM	10005: DCOM got error "1084" attempting to start the service WSearch with arguments "Unavailable" in order to run the server: {B52D54BB-4818-4EB9-AA80-F9EACD371DF8}
System	Error	None	2015-04-24 20:48:01	Liem	DCOM	10005: DCOM got error "1084" attempting to start the service WSearch with arguments "Unavailable" in order to run the server: {B52D54BB-4818-4EB9-AA80-F9EACD371DF8}
System	Error	None	2015-04-24 20:48:01	Liem	DCOM	10005: DCOM got error "1084" attempting to start the service WSearch with arguments "Unavailable" in order to run the server: {B52D54BB-4818-4EB9-AA80-F9EACD371DF8}
System	Error	None	2015-04-24 20:48:04	Liem	DCOM	10005: DCOM got error "1084" attempting to start the service ShellHWDetection with arguments "Unavailable" in order to run the server: {DD522ACC-F821-461A-A407-50B198B896DC}
System	Error	None	2015-04-24 20:48:10	Liem	DCOM	10005: DCOM got error "1084" attempting to start the service ShellHWDetection with arguments "Unavailable" in order to run the server: {DD522ACC-F821-461A-A407-50B198B896DC}
System	Error	None	2015-04-24 20:48:11	Liem	DCOM	10005: DCOM got error "1084" attempting to start the service WSearch with arguments "Unavailable" in order to run the server: {B52D54BB-4818-4EB9-AA80-F9EACD371DF8}
System	Error	None	2015-04-24 20:48:11	Liem	DCOM	10005: DCOM got error "1084" attempting to start the service WSearch with arguments "Unavailable" in order to run the server: {B52D54BB-4818-4EB9-AA80-F9EACD371DF8}
System	Error	None	2015-04-24 20:48:11	Liem	DCOM	10005: DCOM got error "1084" attempting to start the service WSearch with arguments "Unavailable" in order to run the server: {B52D54BB-4818-4EB9-AA80-F9EACD371DF8}
System	Error	None	2015-04-24 20:48:11	Liem	DCOM	10005: DCOM got error "1084" attempting to start the service WSearch with arguments "Unavailable" in order to run the server: {B52D54BB-4818-4EB9-AA80-F9EACD371DF8}
System	Error	None	2015-04-24 20:48:11	Liem	DCOM	10005: DCOM got error "1084" attempting to start the service WSearch with arguments "Unavailable" in order to run the server: {B52D54BB-4818-4EB9-AA80-F9EACD371DF8}
System	Error	None	2015-04-24 20:48:11	Liem	DCOM	10005: DCOM got error "1084" attempting to start the service WSearch with arguments "Unavailable" in order to run the server: {B52D54BB-4818-4EB9-AA80-F9EACD371DF8}
System	Error	None	2015-04-24 20:48:11	Liem	DCOM	10005: DCOM got error "1084" attempting to start the service WSearch with arguments "Unavailable" in order to run the server: {B52D54BB-4818-4EB9-AA80-F9EACD371DF8}
System	Error	None	2015-04-24 20:48:11	Liem	DCOM	10005: DCOM got error "1084" attempting to start the service WSearch with arguments "Unavailable" in order to run the server: {B52D54BB-4818-4EB9-AA80-F9EACD371DF8}
System	Error	None	2015-04-24 20:48:12	Liem	DCOM	10005: DCOM got error "1084" attempting to start the service WSearch with arguments "Unavailable" in order to run the server: {B52D54BB-4818-4EB9-AA80-F9EACD371DF8}
System	Error	None	2015-04-24 20:48:12	Liem	DCOM	10005: DCOM got error "1084" attempting to start the service WSearch with arguments "Unavailable" in order to run the server: {B52D54BB-4818-4EB9-AA80-F9EACD371DF8}
System	Error	None	2015-04-24 20:48:12	Liem	DCOM	10005: DCOM got error "1084" attempting to start the service WSearch with arguments "Unavailable" in order to run the server: {B52D54BB-4818-4EB9-AA80-F9EACD371DF8}

System	Error	None	2015-04-24 20:48:12	Liem	DCOM	10005: DCOM got error "1084" attempting to start the service WSearch with arguments "Unavailable" in order to run the server: {B52D54BB-4818-4EB9-AA80-F9EACD371DF8}
System	Error	None	2015-04-24 20:48:13	Liem	DCOM	10005: DCOM got error "1084" attempting to start the service WSearch with arguments "Unavailable" in order to run the server: {B52D54BB-4818-4EB9-AA80-F9EACD371DF8}
System	Error	None	2015-04-24 20:48:13	Liem	DCOM	10005: DCOM got error "1084" attempting to start the service WSearch with arguments "Unavailable" in order to run the server: {B52D54BB-4818-4EB9-AA80-F9EACD371DF8}
System	Error	None	2015-04-24 20:48:13	Liem	DCOM	10005: DCOM got error "1084" attempting to start the service WSearch with arguments "Unavailable" in order to run the server: {B52D54BB-4818-4EB9-AA80-F9EACD371DF8}
System	Error	None	2015-04-24 20:48:13	Liem	DCOM	10005: DCOM got error "1084" attempting to start the service WSearch with arguments "Unavailable" in order to run the server: {B52D54BB-4818-4EB9-AA80-F9EACD371DF8}
System	Error	None	2015-04-24 20:48:17	Liem	DCOM	10005: DCOM got error "1084" attempting to start the service ShellHWDetection with arguments "Unavailable" in order to run the server: {DD522ACC-F821-461A-A407-50B198B896DC}
System	Error	None	2015-04-24 20:48:29	Liem	DCOM	10005: DCOM got error "1084" attempting to start the service ShellHWDetection with arguments "Unavailable" in order to run the server: {DD522ACC-F821-461A-A407-50B198B896DC}
System	Error	None	2015-04-24 20:48:35	Liem	DCOM	10005: DCOM got error "1084" attempting to start the service WSearch with arguments "Unavailable" in order to run the server: {7D096C5F-AC08-4F1F-BEB7-5C22C517CE39}
System	Error	None	2015-04-24 20:48:35	Liem	DCOM	10005: DCOM got error "1084" attempting to start the service WSearch with arguments "Unavailable" in order to run the server: {7D096C5F-AC08-4F1F-BEB7-5C22C517CE39}
System	Error	None	2015-04-24 20:48:38	Liem	DCOM	10005: DCOM got error "1084" attempting to start the service WSearch with arguments "Unavailable" in order to run the server: {7D096C5F-AC08-4F1F-BEB7-5C22C517CE39}
System	Error	None	2015-04-24 20:48:38	Liem	DCOM	10005: DCOM got error "1084" attempting to start the service WSearch with arguments "Unavailable" in order to run the server: {7D096C5F-AC08-4F1F-BEB7-5C22C517CE39}
System	Error	None	2015-04-24 20:48:58	Liem	DCOM	10005: DCOM got error "1084" attempting to start the service ShellHWDetection with arguments "Unavailable" in order to run the server: {DD522ACC-F821-461A-A407-50B198B896DC}
System	Error	None	2015-04-24 20:48:58	Liem	DCOM	10005: DCOM got error "1084" attempting to start the service WSearch with arguments "Unavailable" in order to run the server: {9E175B68-F52A-11D8-B9A5-505054503030}
System	Warning	None	2015-04-24 20:49:12		BTHUSB	28: The local adapter does not support Bluetooth Low Energy.
System	Warning	None	2015-04-24 20:49:13		k57nd60a	4: Broadcom NetLink (TM) Gigabit Ethernet: The network link is down. Check to make sure the network cable is properly connected.
System	Error	None	2015-04-24 20:49:18	Liem	DCOM	10016: The application-specific permission settings do not grant Local Launch permission for the COM Server application with CLSID {7022A3B3-D004-4F52-AF11-E9E987FEE25F} and APPID {ADA41B3C-C6FD-4A08-8CC1-D6EFDE67BE7D} to the user LTRANPHD\Liem SID (S-1-5-21-1888849264-3803429180-4108621888-1001) from address LocalHost (Using LRPC) running in the application container Unavailable SID (Unavailable). This security permission can be modified using the Component Services administrative tool.
System	Error	None	2015-04-24 21:04:18	Liem	DCOM	10010: The server {9BA05972-F6A8-11CF-A442-00A0C90A8F39} did not register with DCOM within the required timeout.
System	Warning	None	2015-04-24 21:04:47		BTHUSB	28: The local adapter does not support Bluetooth Low Energy.
System	Warning	None	2015-04-24 21:04:48		k57nd60a	4: Broadcom NetLink (TM) Gigabit Ethernet: The network link is down. Check to make sure the network cable is properly connected.
System	Warning	None	2015-04-24 21:05:13		BTHUSB	28: The local adapter does not support Bluetooth Low Energy.
			2015-04-			

System	Warning	None	24 21:05:14	k57nd60a	4: Broadcom NetLink (TM) Gigabit Ethernet: The network link is down. Check to make sure the network cable is properly connected.
System	Warning	None	2015-04-24 21:05:34	BTHUSB	28: The local adapter does not support Bluetooth Low Energy.
System	Warning	None	2015-04-24 21:05:35	k57nd60a	4: Broadcom NetLink (TM) Gigabit Ethernet: The network link is down. Check to make sure the network cable is properly connected.
System	Warning	None	2015-04-24 21:06:23	BTHUSB	28: The local adapter does not support Bluetooth Low Energy.
System	Warning	None	2015-04-24 21:06:25	k57nd60a	4: Broadcom NetLink (TM) Gigabit Ethernet: The network link is down. Check to make sure the network cable is properly connected.
System	Error	None	2015-04-24 21:36:34	EventLog	6008: The previous system shutdown at 9:35:23 PM on ?4/?24/?2015 was unexpected.
System	Warning	None	2015-04-24 21:36:34	BTHUSB	28: The local adapter does not support Bluetooth Low Energy.
System	Warning	None	2015-04-24 21:36:35	k57nd60a	4: Broadcom NetLink (TM) Gigabit Ethernet: The network link is down. Check to make sure the network cable is properly connected.
System	Error	None	2015-04-24 22:06:41	EventLog	6008: The previous system shutdown at 10:05:34 PM on ?4/?24/?2015 was unexpected.
System	Warning	None	2015-04-24 22:06:41	BTHUSB	28: The local adapter does not support Bluetooth Low Energy.
System	Warning	None	2015-04-24 22:06:42	k57nd60a	4: Broadcom NetLink (TM) Gigabit Ethernet: The network link is down. Check to make sure the network cable is properly connected.
System	Warning	None	2015-04-24 22:16:54	BTHUSB	28: The local adapter does not support Bluetooth Low Energy.
System	Warning	None	2015-04-24 22:16:56	k57nd60a	4: Broadcom NetLink (TM) Gigabit Ethernet: The network link is down. Check to make sure the network cable is properly connected.
System	Error	None	2015-04-24 22:33:50	bScsiSDa	15: The device, \Device\Scsi\bScsiSDa1, is not ready for access yet.
System	Error	None	2015-04-24 22:34:10	bScsiSDa	15: The device, \Device\Scsi\bScsiSDa1, is not ready for access yet.
System	Error	None	2015-04-24 22:34:30	bScsiSDa	15: The device, \Device\Scsi\bScsiSDa1, is not ready for access yet.
System	Warning	None	2015-04-25 07:22:38	BTHUSB	28: The local adapter does not support Bluetooth Low Energy.
System	Warning	None	2015-04-25 07:22:39	k57nd60a	4: Broadcom NetLink (TM) Gigabit Ethernet: The network link is down. Check to make sure the network cable is properly connected.
System	Warning	None	2015-04-25 07:52:47	BTHUSB	28: The local adapter does not support Bluetooth Low Energy.
System	Warning	None	2015-04-25 07:52:48	k57nd60a	4: Broadcom NetLink (TM) Gigabit Ethernet: The network link is down. Check to make sure the network cable is properly connected.
System	Error	None	2015-04-25 07:52:52	EventLog	6008: The previous system shutdown at 7:51:37 AM on ?4/?25/?2015 was unexpected.

System	Error	None	2015-04-25 08:04:55	Liem	DCOM	10010: The server {BF6C1E47-86EC-4194-9CE5-13C15DCB2001} did not register with DCOM within the required timeout.
System	Error	None	2015-04-25 08:05:25	Liem	DCOM	10010: The server {1B1F472E-3221-4826-97DB-2C2324D389AE} did not register with DCOM within the required timeout.
System	Error	None	2015-04-25 08:14:55		bScsiSDa	15: The device, \Device\Scsi\bScsiSDa1, is not ready for access yet.
System	Error	None	2015-04-25 08:15:15		bScsiSDa	15: The device, \Device\Scsi\bScsiSDa1, is not ready for access yet.
System	Error	None	2015-04-25 08:15:35		bScsiSDa	15: The device, \Device\Scsi\bScsiSDa1, is not ready for access yet.
System	Error	None	2015-04-25 08:44:55		EventLog	6008: The previous system shutdown at 8:43:30 AM on ?4/?25/?2015 was unexpected.
System	Warning	None	2015-04-25 08:44:55		BTHUSB	28: The local adapter does not support Bluetooth Low Energy.
System	Warning	None	2015-04-25 08:44:56		k57nd60a	4: Broadcom NetLink (TM) Gigabit Ethernet: The network link is down. Check to make sure the network cable is properly connected.
System	Warning	None	2015-04-25 08:45:50		BTHUSB	28: The local adapter does not support Bluetooth Low Energy.
System	Warning	None	2015-04-25 08:45:51		k57nd60a	4: Broadcom NetLink (TM) Gigabit Ethernet: The network link is down. Check to make sure the network cable is properly connected.
System	Error	None	2015-04-25 09:01:42		bScsiSDa	15: The device, \Device\Scsi\bScsiSDa1, is not ready for access yet.
System	Error	None	2015-04-25 09:02:02		bScsiSDa	15: The device, \Device\Scsi\bScsiSDa1, is not ready for access yet.
System	Error	None	2015-04-25 09:02:22		bScsiSDa	15: The device, \Device\Scsi\bScsiSDa1, is not ready for access yet.
System	Error	None	2015-04-25 10:14:22		EventLog	6008: The previous system shutdown at 9:32:13 AM on ?4/?25/?2015 was unexpected.
System	Warning	None	2015-04-25 10:14:22		BTHUSB	28: The local adapter does not support Bluetooth Low Energy.
System	Warning	None	2015-04-25 10:14:24		k57nd60a	4: Broadcom NetLink (TM) Gigabit Ethernet: The network link is down. Check to make sure the network cable is properly connected.
System	Warning	None	2015-04-25 10:38:00		BTHUSB	28: The local adapter does not support Bluetooth Low Energy.
System	Warning	None	2015-04-25 10:38:01		k57nd60a	4: Broadcom NetLink (TM) Gigabit Ethernet: The network link is down. Check to make sure the network cable is properly connected.
System	Warning	None	2015-04-25 10:42:28		BTHUSB	28: The local adapter does not support Bluetooth Low Energy.
System	Warning	None	2015-04-25 10:42:30		k57nd60a	4: Broadcom NetLink (TM) Gigabit Ethernet: The network link is down. Check to make sure the network cable is properly connected.
System	Warning	None	2015-04-25 10:46:57		BTHUSB	28: The local adapter does not support Bluetooth Low Energy.

System	Warning	None	2015-04-25 10:46:59	k57nd60a	4: Broadcom NetLink (TM) Gigabit Ethernet: The network link is down. Check to make sure the network cable is properly connected.
System	Warning	None	2015-04-25 10:48:25	BTHUSB	28: The local adapter does not support Bluetooth Low Energy.
System	Warning	None	2015-04-25 10:48:27	k57nd60a	4: Broadcom NetLink (TM) Gigabit Ethernet: The network link is down. Check to make sure the network cable is properly connected.
System	Warning	None	2015-04-25 11:11:56	BTHUSB	28: The local adapter does not support Bluetooth Low Energy.
System	Warning	None	2015-04-25 11:11:58	k57nd60a	4: Broadcom NetLink (TM) Gigabit Ethernet: The network link is down. Check to make sure the network cable is properly connected.
System	Warning	None	2015-04-25 11:12:23	BTHUSB	28: The local adapter does not support Bluetooth Low Energy.
System	Warning	None	2015-04-25 11:12:24	k57nd60a	4: Broadcom NetLink (TM) Gigabit Ethernet: The network link is down. Check to make sure the network cable is properly connected.
System	Error	None	2015-04-25 15:32:49	EventLog	6008: The previous system shutdown at 11:41:22 AM on ?4/?25/?2015 was unexpected.
System	Warning	None	2015-04-25 15:32:51	BTHUSB	28: The local adapter does not support Bluetooth Low Energy.
System	Warning	None	2015-04-25 15:32:51	k57nd60a	4: Broadcom NetLink (TM) Gigabit Ethernet: The network link is down. Check to make sure the network cable is properly connected.
System	Warning	None	2015-04-25 15:52:51	BTHUSB	28: The local adapter does not support Bluetooth Low Energy.
System	Warning	None	2015-04-25 16:02:56	k57nd60a	4: Broadcom NetLink (TM) Gigabit Ethernet: The network link is down. Check to make sure the network cable is properly connected.
System	Warning	None	2015-04-25 16:02:56	BTHUSB	28: The local adapter does not support Bluetooth Low Energy.
System	Error	None	2015-04-25 16:03:00	EventLog	6008: The previous system shutdown at 4:01:49 PM on ?4/?25/?2015 was unexpected.
System	Error	None	2015-04-25 17:13:20	EventLog	6008: The previous system shutdown at 4:32:00 PM on ?4/?25/?2015 was unexpected.
System	Warning	None	2015-04-25 17:13:22	k57nd60a	4: Broadcom NetLink (TM) Gigabit Ethernet: The network link is down. Check to make sure the network cable is properly connected.
System	Warning	None	2015-04-25 17:13:22	BTHUSB	28: The local adapter does not support Bluetooth Low Energy.
System	Error	None	2015-04-25 17:49:43	EventLog	6008: The previous system shutdown at 5:42:20 PM on ?4/?25/?2015 was unexpected.
System	Warning	None	2015-04-25 17:49:44	BTHUSB	28: The local adapter does not support Bluetooth Low Energy.
System	Warning	None	2015-04-25 17:49:45	k57nd60a	4: Broadcom NetLink (TM) Gigabit Ethernet: The network link is down. Check to make sure the network cable is properly connected.
System	Error	None	2015-04-26 08:56:24	EventLog	6008: The previous system shutdown at 6:18:43 PM on ?4/?25/?2015 was unexpected.

System	Warning	None	2015-04-26 08:56:25		k57nd60a	4: Broadcom NetLink (TM) Gigabit Ethernet: The network link is down. Check to make sure the network cable is properly connected.
System	Warning	None	2015-04-26 08:56:25		BTHUSB	28: The local adapter does not support Bluetooth Low Energy.
System	Error	None	2015-04-26 09:07:06	Liem	DCOM	10010: The server {BF6C1E47-86EC-4194-9CE5-13C15DCB2001} did not register with DCOM within the required timeout.
System	Error	None	2015-04-26 09:07:36	Liem	DCOM	10010: The server {1B1F472E-3221-4826-97DB-2C2324D389AE} did not register with DCOM within the required timeout.
System	Warning	None	2015-04-26 09:29:57		BTHUSB	28: The local adapter does not support Bluetooth Low Energy.
System	Warning	None	2015-04-26 09:29:59		k57nd60a	4: Broadcom NetLink (TM) Gigabit Ethernet: The network link is down. Check to make sure the network cable is properly connected.
System	Error	None	2015-04-26 09:30:03		EventLog	6008: The previous system shutdown at 9:25:24 AM on ?4/?26/?2015 was unexpected.
System	Warning	None	2015-04-26 10:00:02		BTHUSB	28: The local adapter does not support Bluetooth Low Energy.
System	Error	None	2015-04-26 10:00:03		EventLog	6008: The previous system shutdown at 9:59:04 AM on ?4/?26/?2015 was unexpected.
System	Warning	None	2015-04-26 10:00:04		k57nd60a	4: Broadcom NetLink (TM) Gigabit Ethernet: The network link is down. Check to make sure the network cable is properly connected.
System	Error	None	2015-04-26 12:26:10		bScsiSDa	15: The device, \Device\Scsi\bScsiSDa1, is not ready for access yet.
System	Error	None	2015-04-26 12:26:30		bScsiSDa	15: The device, \Device\Scsi\bScsiSDa1, is not ready for access yet.
System	Error	None	2015-04-26 12:26:50		bScsiSDa	15: The device, \Device\Scsi\bScsiSDa1, is not ready for access yet.
System	Error	None	2015-04-26 12:56:08		EventLog	6008: The previous system shutdown at 12:54:55 PM on ?4/?26/?2015 was unexpected.
System	Warning	None	2015-04-26 12:56:08		BTHUSB	28: The local adapter does not support Bluetooth Low Energy.
System	Warning	None	2015-04-26 12:56:10		k57nd60a	4: Broadcom NetLink (TM) Gigabit Ethernet: The network link is down. Check to make sure the network cable is properly connected.
System	Error	None	2015-04-26 13:26:14		EventLog	6008: The previous system shutdown at 1:25:08 PM on ?4/?26/?2015 was unexpected.
System	Warning	None	2015-04-26 13:26:14		BTHUSB	28: The local adapter does not support Bluetooth Low Energy.
System	Warning	None	2015-04-26 13:26:15		k57nd60a	4: Broadcom NetLink (TM) Gigabit Ethernet: The network link is down. Check to make sure the network cable is properly connected.
System	Error	None	2015-04-27 17:04:49		EventLog	6008: The previous system shutdown at 1:55:14 PM on ?4/?26/?2015 was unexpected.
System	Warning	None	2015-04-27		BTHUSB	28: The local adapter does not support Bluetooth Low Energy.

			17:04:49			
System	Warning	None	2015-04-27 17:04:51		k57nd60a	4: Broadcom NetLink (TM) Gigabit Ethernet: The network link is down. Check to make sure the network cable is properly connected.
System	Warning	None	2015-04-27 17:34:57		k57nd60a	4: Broadcom NetLink (TM) Gigabit Ethernet: The network link is down. Check to make sure the network cable is properly connected.
System	Warning	None	2015-04-27 17:34:59		BTHUSB	28: The local adapter does not support Bluetooth Low Energy.
System	Error	None	2015-04-27 17:35:01		EventLog	6008: The previous system shutdown at 5:33:49 PM on ?4/?27/?2015 was unexpected.
System	Error	None	2015-04-27 18:02:31	Liem	DCOM	10010: The server {BF6C1E47-86EC-4194-9CE5-13C15DCB2001} did not register with DCOM within the required timeout.
System	Error	None	2015-04-27 18:03:01	Liem	DCOM	10010: The server {1B1F472E-3221-4826-97DB-2C2324D389AE} did not register with DCOM within the required timeout.
System	Error	None	2015-04-27 18:32:23		EventLog	6008: The previous system shutdown at 6:04:01 PM on ?4/?27/?2015 was unexpected.
System	Warning	None	2015-04-27 18:32:23		BTHUSB	28: The local adapter does not support Bluetooth Low Energy.
System	Warning	None	2015-04-27 18:32:25		k57nd60a	4: Broadcom NetLink (TM) Gigabit Ethernet: The network link is down. Check to make sure the network cable is properly connected.
System	Error	None	2015-04-28 18:36:22		EventLog	6008: The previous system shutdown at 7:01:23 PM on ?4/?27/?2015 was unexpected.
System	Warning	None	2015-04-28 18:36:22		BTHUSB	28: The local adapter does not support Bluetooth Low Energy.
System	Warning	None	2015-04-28 18:36:24		k57nd60a	4: Broadcom NetLink (TM) Gigabit Ethernet: The network link is down. Check to make sure the network cable is properly connected.
System	Warning	None	2015-04-28 19:06:30		BTHUSB	28: The local adapter does not support Bluetooth Low Energy.
System	Warning	None	2015-04-28 19:06:31		k57nd60a	4: Broadcom NetLink (TM) Gigabit Ethernet: The network link is down. Check to make sure the network cable is properly connected.
System	Error	None	2015-04-28 19:06:35		EventLog	6008: The previous system shutdown at 7:05:22 PM on ?4/?28/?2015 was unexpected.
System	Error	None	2015-04-28 19:37:42		EventLog	6008: The previous system shutdown at 7:35:35 PM on ?4/?28/?2015 was unexpected.
System	Warning	None	2015-04-28 19:37:43		BTHUSB	28: The local adapter does not support Bluetooth Low Energy.
System	Warning	None	2015-04-28 19:37:44		k57nd60a	4: Broadcom NetLink (TM) Gigabit Ethernet: The network link is down. Check to make sure the network cable is properly connected.
System	Error	None	2015-04-28 20:15:22		EventLog	6008: The previous system shutdown at 8:06:42 PM on ?4/?28/?2015 was unexpected.
System	Warning	None	2015-04-28 20:15:23		BTHUSB	28: The local adapter does not support Bluetooth Low Energy.
			2015-04-			4: Broadcom NetLink (TM) Gigabit Ethernet: The network link is down. Check to make sure the network cable is

System	Warning	None	28 20:15:24		k57nd60a	properly connected.
System	Warning	None	2015-04-28 20:42:37		BTHUSB	28: The local adapter does not support Bluetooth Low Energy.
System	Warning	None	2015-04-28 20:42:38		k57nd60a	4: Broadcom NetLink (TM) Gigabit Ethernet: The network link is down. Check to make sure the network cable is properly connected.
System	Error	None	2015-04-28 20:59:59	Liem	DCOM	10010: The server {BF6C1E47-86EC-4194-9CE5-13C15DCB2001} did not register with DCOM within the required timeout.
System	Error	None	2015-04-29 11:34:20		EventLog	6008: The previous system shutdown at 9:11:36 PM on ?4/?28/?2015 was unexpected.
System	Warning	None	2015-04-29 11:34:20		BTHUSB	28: The local adapter does not support Bluetooth Low Energy.
System	Warning	None	2015-04-29 11:34:22		k57nd60a	4: Broadcom NetLink (TM) Gigabit Ethernet: The network link is down. Check to make sure the network cable is properly connected.

Database Software

Database Drivers:

Borland Database Engine	-
Borland InterBase Client	-
Easysoft ODBC-InterBase 6	-
Easysoft ODBC-InterBase 7	-
Firebird Client	-
Jet Engine	4.00.9765.0
MDAC	6.3.9600.17415 (winblue_r4.141028-1500)
ODBC	6.3.9600.17415 (winblue_r4.141028-1500)
MySQL Connector/ODBC	-
Oracle Client	-
PsqlODBC	-
Sybase ASE ODBC	-

Database Servers:

Borland InterBase Server	-
Firebird Server	-
Microsoft SQL Server	-
Microsoft SQL Server Compact Edition	-
Microsoft SQL Server Express Edition	-
MySQL Server	-
Oracle Server	-
PostgreSQL Server	-
Sybase SQL Server	-

ODBC Drivers

Driver Description	File Name	Version	File Extensions Supported
Driver da Microsoft para arquivos texto (*.txt; *.csv)	odbcjt32.dll	6.3.9600.17415 (winblue_r4.141028-1500)	*.,*.asc,*.csv,*.tab,*.txt,*.csv

Driver do Microsoft Access (*.mdb)	odbcjt32.dll	6.3.9600.17415 (winblue_r4.141028-1500)	*.mdb
Driver do Microsoft dBase (*.dbf)	odbcjt32.dll	6.3.9600.17415 (winblue_r4.141028-1500)	*.dbf,*.ndx,*.mdx
Driver do Microsoft Excel(*.xls)	odbcjt32.dll	6.3.9600.17415 (winblue_r4.141028-1500)	*.xls
Driver do Microsoft Paradox (*.db)	odbcjt32.dll	6.3.9600.17415 (winblue_r4.141028-1500)	*.db
Microsoft Access Driver (*.mdb)	odbcjt32.dll	6.3.9600.17415 (winblue_r4.141028-1500)	*.mdb
Microsoft Access Driver (*.mdb, *.accdb)	aceodbc.dll	15.0.4695.1000	*.mdb,*.accdb
Microsoft Access Text Driver (*.txt, *.csv)	aceodbc.dll	15.0.4695.1000	*.txt, *.csv
Microsoft Access-Treiber (*.mdb)	odbcjt32.dll	6.3.9600.17415 (winblue_r4.141028-1500)	*.mdb
Microsoft dBase Driver (*.dbf)	odbcjt32.dll	6.3.9600.17415 (winblue_r4.141028-1500)	*.dbf,*.ndx,*.mdx
Microsoft dBase-Treiber (*.dbf)	odbcjt32.dll	6.3.9600.17415 (winblue_r4.141028-1500)	*.dbf,*.ndx,*.mdx
Microsoft Excel Driver (*.xls)	odbcjt32.dll	6.3.9600.17415 (winblue_r4.141028-1500)	*.xls
Microsoft Excel Driver (*.xls, *.xlsx, *.xlsm, *.xlsb)	aceodbc.dll	15.0.4695.1000	*.xls,*.xlsx, *.xlsb
Microsoft Excel-Treiber (*.xls)	odbcjt32.dll	6.3.9600.17415 (winblue_r4.141028-1500)	*.xls
Microsoft ODBC for Oracle	msorcl32.dll	6.3.9600.17415 (winblue_r4.141028-1500)	
Microsoft Paradox Driver (*.db)	odbcjt32.dll	6.3.9600.17415 (winblue_r4.141028-1500)	*.db
Microsoft Paradox-Treiber (*.db)	odbcjt32.dll	6.3.9600.17415 (winblue_r4.141028-1500)	*.db
Microsoft Text Driver (*.txt; *.csv)	odbcjt32.dll	6.3.9600.17415 (winblue_r4.141028-1500)	*.,*.asc,*.csv,*.tab,*.txt,*.csv
Microsoft Text-Treiber (*.txt; *.csv)	odbcjt32.dll	6.3.9600.17415 (winblue_r4.141028-1500)	*.,*.asc,*.csv,*.tab,*.txt,*.csv
SQL Server	sqlsrv32.dll	6.3.9600.17415 (winblue_r4.141028-1500)	

ODBC Data Sources

Data Source Name	Data Source Description	Type	Driver File Name
Excel Files	Microsoft Excel Driver (*.xls, *.xlsx, *.xlsm, *.xlsb)	User	aceodbc.dll
MS Access Database	Microsoft Access Driver (*.mdb, *.accdb)	User	aceodbc.dll

Memory Read

CPU	CPU Clock	Motherboard	Chipset	Memory	CL-RCD-RP-RAS	Read Speed
16x Xeon E5-2670 HT	2600 MHz	Supermicro X9DR6-F	C600	Quad DDR3-1333	9-9-9-24	77243 MB/s
32x Opteron 6274	2200 MHz	Supermicro H8DGI-F	SR5690	Dual DDR3-1600R	11-11-11-28 CR1	67619 MB/s
6x Core i7-4930K HT	3400 MHz	Gigabyte GA-X79-UD3	X79	Quad DDR3-1866	9-10-9-27 CR2	52396 MB/s
6x Core i7-3960X Extreme HT	3300 MHz	Intel DX79SI	X79	Quad DDR3-1600	9-9-9-24 CR2	45162 MB/s
6x Core i7-5820K HT	3300 MHz	Gigabyte GA-X99-UD4	X99	Quad DDR4-2133	15-15-15-36 CR2	42431 MB/s
8x Xeon X5550 HT	2666 MHz	Supermicro X8DTN+	i5520	Triple DDR3-1333	9-9-9-24 CR1	37831 MB/s
8x FX-8150	3600 MHz	Asus M5A97	AMD970	Dual DDR3-1866	9-10-9-27 CR2	26428 MB/s
8x FX-8350	4000 MHz	Asus M5A99X Evo R2.0	AMD990X	Dual DDR3-1866	9-10-9-27 CR2	26020 MB/s
4x Core i7-3770K HT	3500 MHz	MSI Z77A-GD55	Z77 Int.	Dual DDR3-1600	9-9-9-24 CR2	23559 MB/s
4x Core i7-4770 HT	3400 MHz	Intel DZ87KLT-75K	Z87 Int.	Dual DDR3-1600	9-9-9-27 CR2	23218 MB/s
4x Xeon E3-1245 v3 HT	3400 MHz	Supermicro X10SAE	C226 Int.	Dual DDR3-1600	11-11-11-28 CR1	23157 MB/s
2x Core i7-3520M HT	**3400 MHz**	**Gateway EG50_HC_HR**	**HM70 Int.**	**Dual DDR3-1600**	**11-11-11-28 CR1**	**22813 MB/s**
8x Atom C2750	2400 MHz	Supermicro A1SAi-2750F	Avoton	Dual DDR3-1600	11-11-11-28 CR1	21726 MB/s
4x A10-5800K	3800 MHz	Asus F2A55-M	A55 Int.	Dual DDR3-1866	9-10-9-27 CR2	21404 MB/s
4x A10-6800K	4100 MHz	Gigabyte GA-F2A85X-UP4	A85X Int.	Dual DDR3-2133	9-11-10-27 CR2	21284 MB/s
4x Core i7-965 Extreme HT	3200 MHz	Asus P6T Deluxe	X58	Triple DDR3-1333	9-9-9-24 CR1	21210 MB/s
6x Core i7-990X Extreme HT	3466 MHz	Intel DX58SO2	X58	Triple DDR3-1333	9-9-9-24 CR1	21110 MB/s
4x A10-7850K	3700 MHz	Gigabyte GA-F2A88XM-D3H	A88X Int.	Dual DDR3-2133	9-11-10-31 CR2	21006 MB/s
12x Opteron 2431	2400 MHz	Supermicro H8DI3+-F	SR5690	Unganged Dual DDR2-800R	6-6-6-18 CR1	19763 MB/s
4x Core i7-2600 HT	3400 MHz	Asus P8P67	P67	Dual DDR3-1333	9-9-9-24 CR1	19552 MB/s

8x Opteron 2378	2400 MHz	Tyan Thunder n3600R	nForcePro-3600	Unganged Dual DDR2-800R	6-6-6-18 CR1	18834 MB/s
4x Xeon X3430	2400 MHz	Supermicro X8SIL-F	i3420	Dual DDR3-1333	9-9-9-24 CR1	17639 MB/s
4x A8-3850	2900 MHz	Gigabyte GA-A75M-UD2H	A75 Int.	Dual DDR3-1333	9-9-9-24 CR1	16638 MB/s
6x Phenom II X6 Black 1100T	3300 MHz	Gigabyte GA-890GPA-UD3H v2	AMD890GX Int.	Unganged Dual DDR3-1333	9-9-9-24 CR2	14730 MB/s
Celeron J1900	2000 MHz	Gigabyte GA-J1900N-D3V	BayTrailD Int.	Dual DDR3-1333	9-9-9-24 CR1	13453 MB/s
8x Opteron 2344 HE	1700 MHz	Supermicro H8DME-2	nForcePro-3600	Unganged Dual DDR2-667R	5-5-5-15 CR1	13118 MB/s
4x Opteron 2210 HE	1800 MHz	Tyan Thunder h2000M	BCM5785	Dual DDR2-600R	5-5-5-15 CR1	11534 MB/s
2x Core i5-650 HT	3200 MHz	Supermicro C7SIM-Q	Q57 Int.	Dual DDR3-1333	9-9-9-24 CR1	11178 MB/s
4x Phenom II X4 Black 940	3000 MHz	Asus M3N78-EM	GeForce8300 Int.	Ganged Dual DDR2-800	5-5-5-18 CR2	10112 MB/s
2x Athlon64 X2 Black 6400+	3200 MHz	MSI K9N SLI Platinum	nForce570SLI	Dual DDR2-800	4-4-4-11 CR1	9714 MB/s
4x Core 2 Extreme QX9650	3000 MHz	Gigabyte GA-EP35C-DS3R	P35	Dual DDR3-1066	8-8-8-20 CR2	9037 MB/s
4x Athlon 5350	2050 MHz	ASRock AM1B-ITX	Yangtze Int.	DDR3-1600 SDRAM	11-11-11-28 CR2	8716 MB/s
4x Phenom X4 9500	2200 MHz	Asus M3A	AMD770	Ganged Dual DDR2-800	5-5-5-18 CR2	8709 MB/s
2x Opteron 240	1400 MHz	MSI K8D Master3-133 FS	AMD8100	Dual DDR400R	3-4-4-8 CR1	8366 MB/s
2x Pentium EE 955 HT	3466 MHz	Intel D955XBK	i955X	Dual DDR2-667	4-4-4-11	8096 MB/s
P4EE HT	3733 MHz	Intel SE7230NH1LX	iE7230	Dual DDR2-667	5-5-5-15	7965 MB/s
8x Xeon E5462	2800 MHz	Intel S5400SF	i5400	Quad DDR2-640FB	5-5-5-15	7646 MB/s
2x Core 2 Extreme X6800	2933 MHz	Abit AB9	P965	Dual DDR2-800	5-5-5-18 CR2	7627 MB/s
2x Athlon64 X2 4000+	2100 MHz	ASRock ALiveNF7G-HDready	nForce7050-630a Int.	Dual DDR2-700	5-5-5-18 CR2	7616 MB/s
2x Core 2 Duo P8400	2266 MHz	MSI MegaBook PR201	GM45 Int.	Dual DDR2-667	5-5-5-15	6989 MB/s
4x Core 2 Extreme QX6700	2666 MHz	Intel D975XBX2	i975X	Dual DDR2-667	5-5-5-15	6593 MB/s
Nano X2 L4350	1600 MHz	VIA EPIA-M900	VX900H Int.	DDR3-1066 SDRAM	7-7-7-20 CR2	6414 MB/s
2x Pentium D 820	2800 MHz	Abit Fatal1ty F-I90HD	RS600 Int.	Dual DDR2-800	5-5-5-18 CR2	6206 MB/s
2x Atom D2500	1866 MHz	Intel D2500CC	NM10 Int.	DDR3-1066 SDRAM	7-7-7-20 CR2	6104 MB/s
2x E-350	1600 MHz	ASRock E350M1	A50M Int.	DDR3-1066 SDRAM	8-8-8-20 CR1	6082 MB/s
Athlon64 3200+	2000 MHz	ASRock 939S56-M	SiS756	Dual DDR400	2.5-3-3-8 CR2	6009 MB/s
Celeron 420	1600 MHz	Intel DQ965GF	Q965 Int.	Dual DDR2-667	5-5-5-15	5353 MB/s
2x Xeon HT	3400 MHz	Intel SE7320SP2	iE7320	Dual DDR333R	2.5-3-3-7	4539 MB/s
Celeron D 326	2533 MHz	ASRock 775Twins-HDTV	RC410 Ext.	DDR2-533 SDRAM	4-4-4-11	3967 MB/s
Opteron 248	2200 MHz	MSI K8T Master1-FAR	K8T800	Dual DDR266R	2-3-3-6 CR1	3907 MB/s
8x Xeon L5320	1866 MHz	Intel S5000VCL	i5000V	Dual DDR2-533FB	4-4-4-12	3672 MB/s
Atom 230 HT	1600 MHz	Intel D945GCLF	i945GC Int.	DDR2-533 SDRAM	4-4-4-12	3593 MB/s
Nano L2200	1600 MHz	VIA VB8001	CN896 Int.	DDR2-667 SDRAM	5-5-5-15 CR2	3362 MB/s
4x Xeon 5140	2333 MHz	Intel S5000VSA	i5000V	Dual DDR2-667FB	5-5-5-15	3323 MB/s
Sempron 2600+	1600 MHz	ASRock K8NF4G-SATA2	GeForce6100 Int.	DDR400 SDRAM	2.5-3-3-8 CR2	2919 MB/s

Memory Write

CPU	CPU Clock	Motherboard	Chipset	Memory	CL-RCD-RP-RAS	Write Speed
16x Xeon E5-2670 HT	2600 MHz	Supermicro X9DR6-F	C600	Quad DDR3-1333	9-9-9-24	77060 MB/s
32x Opteron 6274	2200 MHz	Supermicro H8DGI-F	SR5690	Dual DDR3-1600R	11-11-11-28 CR1	57844 MB/s
6x Core i7-4930K HT	3400 MHz	Gigabyte GA-X79-UD3	X79	Quad DDR3-1866	9-10-9-27 CR2	52243 MB/s
6x Core i7-3960X Extreme HT	3300 MHz	Intel DX79SI	X79	Quad DDR3-1600	9-9-9-24 CR2	45588 MB/s
6x Core i7-5820K HT	3300 MHz	Gigabyte GA-X99-UD4	X99	Quad DDR4-2133	15-15-15-36 CR2	45249 MB/s
8x Xeon X5550 HT	2666 MHz	Supermicro X8DTN+	i5520	Triple DDR3-1333	9-9-9-24 CR1	27392 MB/s
2x Core i7-3520M HT	**3400 MHz**	**Gateway EG50_HC_HR**	**HM70 Int.**	**Dual DDR3-1600**	**11-11-11-28 CR1**	**24170 MB/s**
4x Core i7-3770K HT	3500 MHz	MSI Z77A-GD55	Z77 Int.	Dual DDR3-1600	9-9-9-24 CR2	24093 MB/s
4x Core i7-4770 HT	3400 MHz	Intel DZ87KLT-75K	Z87 Int.	Dual DDR3-1600	9-9-9-27 CR2	23672 MB/s
4x Xeon E3-1245 v3 HT	3400 MHz	Supermicro X10SAE	C226 Int.	Dual DDR3-1600	11-11-11-28 CR1	23649 MB/s
4x Core i7-2600 HT	3400 MHz	Asus P8P67	P67	Dual DDR3-1333	9-9-9-24 CR1	19528 MB/s
8x FX-8150	3600 MHz	Asus M5A97	AMD970	Dual DDR3-1866	9-10-9-27 CR2	18063 MB/s
8x FX-8350	4000 MHz	Asus M5A99X Evo R2.0	AMD990X	Dual DDR3-1866	9-10-9-27 CR2	17607 MB/s

4x Core i7-965 Extreme HT	3200 MHz	Asus P6T Deluxe	X58	Triple DDR3-1333	9-9-9-24 CR1	17088 MB/s
6x Core i7-990X Extreme HT	3466 MHz	Intel DX58SO2	X58	Triple DDR3-1333	9-9-9-24 CR1	16673 MB/s
4x A8-3850	2900 MHz	Gigabyte GA-A75M-UD2H	A75 Int.	Dual DDR3-1333	9-9-9-24 CR1	14866 MB/s
12x Opteron 2431	2400 MHz	Supermicro H8DI3+-F	SR5690	Unganged Dual DDR2-800R	6-6-6-18 CR1	14492 MB/s
4x Xeon X3430	2400 MHz	Supermicro X8SIL-F	i3420	Dual DDR3-1333	9-9-9-24 CR1	13215 MB/s
8x Opteron 2378	2400 MHz	Tyan Thunder n3600R	nForcePro-3600	Unganged Dual DDR2-800R	6-6-6-18 CR1	12776 MB/s
8x Atom C2750	2400 MHz	Supermicro A1SAi-2750F	Avoton	Dual DDR3-1600	11-11-11-28 CR1	12328 MB/s
4x A10-7850K	3700 MHz	Gigabyte GA-F2A88XM-D3H	A88X Int.	Dual DDR3-2133	9-11-10-31 CR2	11995 MB/s
4x A10-6800K	4100 MHz	Gigabyte GA-F2A85X-UP4	A85X Int.	Dual DDR3-2133	9-11-10-27 CR2	10777 MB/s
Celeron J1900	2000 MHz	Gigabyte GA-J1900N-D3V	BayTrailD Int.	Dual DDR3-1333	9-9-9-24 CR1	10154 MB/s
4x A10-5800K	3800 MHz	Asus F2A55-M	A55 Int.	Dual DDR3-1866	9-10-9-27 CR2	9970 MB/s
2x Core i5-650 HT	3200 MHz	Supermicro C7SIM-Q	Q57 Int.	Dual DDR3-1333	9-9-9-24 CR1	9937 MB/s
2x Athlon64 X2 Black 6400+	3200 MHz	MSI K9N SLI Platinum	nForce570SLI	Dual DDR2-800	4-4-4-11 CR1	8869 MB/s
8x Opteron 2344 HE	1700 MHz	Supermicro H8DME-2	nForcePro-3600	Unganged Dual DDR2-667R	5-5-5-15 CR1	8662 MB/s
Nano X2 L4350	1600 MHz	VIA EPIA-M900	VX900H Int.	DDR3-1066 SDRAM	7-7-7-20 CR2	7913 MB/s
4x Opteron 2210 HE	1800 MHz	Tyan Thunder h2000M	BCM5785	Dual DDR2-600R	5-5-5-15 CR1	7779 MB/s
4x Phenom II X4 Black 940	3000 MHz	Asus M3N78-EM	GeForce8300 Int.	Ganged Dual DDR2-800	5-5-5-18 CR2	7115 MB/s
6x Phenom II X6 Black 1100T	3300 MHz	Gigabyte GA-890GPA-UD3H v2	AMD890GX Int.	Unganged Dual DDR3-1333	9-9-9-24 CR2	7091 MB/s
4x Core 2 Extreme QX9650	3000 MHz	Gigabyte GA-EP35C-DS3R	P35	Dual DDR3-1066	8-8-8-20 CR2	7083 MB/s
8x Xeon E5462	2800 MHz	Intel S5400SF	i5400	Quad DDR2-640FB	5-5-5-15	6733 MB/s
2x Athlon64 X2 4000+	2100 MHz	ASRock ALiveNF7G-HDready	nForce7050-630a Int.	Dual DDR2-700	5-5-5-18 CR2	5762 MB/s
2x Pentium EE 955 HT	3466 MHz	Intel D955XBK	i955X	Dual DDR2-667	4-4-4-11	5654 MB/s
P4EE HT	3733 MHz	Intel SE7230NH1LX	iE7230	Dual DDR2-667	5-5-5-15	5639 MB/s
4x Phenom X4 9500	2200 MHz	Asus M3A	AMD770	Ganged Dual DDR2-800	5-5-5-18 CR2	5504 MB/s
2x Core 2 Duo P8400	2266 MHz	MSI MegaBook PR201	GM45 Int.	Dual DDR2-667	5-5-5-15	5461 MB/s
2x Core 2 Extreme X6800	2933 MHz	Abit AB9	P965	Dual DDR2-800	5-5-5-18 CR2	4869 MB/s
4x Core 2 Extreme QX6700	2666 MHz	Intel D975XBX2	i975X	Dual DDR2-667	5-5-5-15	4856 MB/s
2x Atom D2500	1866 MHz	Intel D2500CC	NM10 Int.	DDR3-1066 SDRAM	7-7-7-20 CR2	4712 MB/s
4x Athlon 5350	2050 MHz	ASRock AM1B-ITX	Yangtze Int.	DDR3-1600 SDRAM	11-11-11-28 CR2	4694 MB/s
2x Pentium D 820	2800 MHz	Abit Fatal1ty F-I90HD	RS600 Int.	Dual DDR2-800	5-5-5-18 CR2	4260 MB/s
2x Xeon HT	3400 MHz	Intel SE7320SP2	iE7320	Dual DDR333R	2.5-3-3-7	4220 MB/s
2x E-350	1600 MHz	ASRock E350M1	A50M Int.	DDR3-1066 SDRAM	8-8-8-20 CR1	4117 MB/s
Athlon64 3200+	2000 MHz	ASRock 939S56-M	SiS756	Dual DDR400	2.5-3-3-8 CR2	4093 MB/s
2x Opteron 240	1400 MHz	MSI K8D Master3-133 FS	AMD8100	Dual DDR400R	3-4-4-8 CR1	4029 MB/s
Opteron 248	2200 MHz	MSI K8T Master1-FAR	K8T800	Dual DDR266R	2-3-3-6 CR1	3800 MB/s
Celeron 420	1600 MHz	Intel DQ965GF	Q965 Int.	Dual DDR2-667	5-5-5-15	3568 MB/s
Nano L2200	1600 MHz	VIA VB8001	CN896 Int.	DDR2-667 SDRAM	5-5-5-15 CR2	3159 MB/s
Atom 230 HT	1600 MHz	Intel D945GCLF	i945GC Int.	DDR2-533 SDRAM	4-4-4-12	2831 MB/s
Celeron D 326	2533 MHz	ASRock 775Twins-HDTV	RC410 Ext.	DDR2-533 SDRAM	4-4-4-11	2796 MB/s
4x Xeon 5140	2333 MHz	Intel S5000VSA	i5000V	Dual DDR2-667FB	5-5-5-15	2474 MB/s
8x Xeon L5320	1866 MHz	Intel S5000VCL	i5000V	Dual DDR2-533FB	4-4-4-12	2348 MB/s
Sempron 2600+	1600 MHz	ASRock K8NF4G-SATA2	GeForce6100 Int.	DDR400 SDRAM	2.5-3-3-8 CR2	2337 MB/s

Memory Copy

CPU	CPU Clock	Motherboard	Chipset	Memory	CL-RCD-RP-RAS	Copy Speed
32x Opteron 6274	2200 MHz	Supermicro H8DGI-F	SR5690	Dual DDR3-1600R	11-11-11-28 CR1	69009 MB/s
16x Xeon E5-2670 HT	2600 MHz	Supermicro X9DR6-F	C600	Quad DDR3-1333	9-9-9-24	67052 MB/s
6x Core i7-4930K HT	3400 MHz	Gigabyte GA-X79-UD3	X79	Quad DDR3-1866	9-10-9-27 CR2	50043 MB/s
6x Core i7-5820K HT	3300 MHz	Gigabyte GA-X99-UD4	X99	Quad DDR4-2133	15-15-15-36 CR2	44987 MB/s
6x Core i7-3960X Extreme HT	3300 MHz	Intel DX79SI	X79	Quad DDR3-1600	9-9-9-24 CR2	42150 MB/s
8x Xeon X5550 HT	2666 MHz	Supermicro X8DTN+	i5520	Triple DDR3-1333	9-9-9-24 CR1	34882 MB/s

6x Core i7-990X Extreme HT	3466 MHz	Intel DX58SO2	X58	Triple DDR3-1333	9-9-9-24 CR1	24509 MB/s
8x FX-8150	3600 MHz	Asus M5A97	AMD970	Dual DDR3-1866	9-10-9-27 CR2	23799 MB/s
8x FX-8350	4000 MHz	Asus M5A99X Evo R2.0	AMD990X	Dual DDR3-1866	9-10-9-27 CR2	22896 MB/s
4x Core i7-3770K HT	3500 MHz	MSI Z77A-GD55	Z77 Int.	Dual DDR3-1600	9-9-9-24 CR2	22772 MB/s
2x Core i7-3520M HT	**3600 MHz**	**Gateway EG50_HC_HR**	**HM70 Int.**	**Dual DDR3-1600**	**11-11-11-28 CR1**	**21747 MB/s**
4x Xeon E3-1245 v3 HT	3400 MHz	Supermicro X10SAE	C226 Int.	Dual DDR3-1600	11-11-11-28 CR1	21695 MB/s
4x Core i7-965 Extreme HT	3200 MHz	Asus P6T Deluxe	X58	Triple DDR3-1333	9-9-9-24 CR1	21530 MB/s
4x Core i7-4770 HT	3400 MHz	Intel DZ87KLT-75K	Z87 Int.	Dual DDR3-1600	9-9-9-27 CR2	21283 MB/s
4x A10-7850K	3700 MHz	Gigabyte GA-F2A88XM-D3H	A88X Int.	Dual DDR3-2133	9-11-10-31 CR2	20802 MB/s
4x A10-5800K	3800 MHz	Asus F2A55-M	A55 Int.	Dual DDR3-1866	9-10-9-27 CR2	17897 MB/s
4x Core i7-2600 HT	3400 MHz	Asus P8P67	P67	Dual DDR3-1333	9-9-9-24 CR1	17836 MB/s
4x A10-6800K	4100 MHz	Gigabyte GA-F2A85X-UP4	A85X Int.	Dual DDR3-2133	9-11-10-27 CR2	17735 MB/s
8x Opteron 2378	2400 MHz	Tyan Thunder n3600R	nForcePro-3600	Unganged Dual DDR2-800R	6-6-6-18 CR1	17362 MB/s
12x Opteron 2431	2400 MHz	Supermicro H8DI3+-F	SR5690	Unganged Dual DDR2-800R	6-6-6-18 CR1	17174 MB/s
8x Atom C2750	2400 MHz	Supermicro A1SAi-2750F	Avoton	Dual DDR3-1600	11-11-11-28 CR1	16882 MB/s
4x Xeon X3430	2400 MHz	Supermicro X8SIL-F	i3420	Dual DDR3-1333	9-9-9-24 CR1	15347 MB/s
4x A8-3850	2900 MHz	Gigabyte GA-A75M-UD2H	A75 Int.	Dual DDR3-1333	9-9-9-24 CR1	13993 MB/s
2x Core i5-650 HT	3200 MHz	Supermicro C7SIM-Q	Q57 Int.	Dual DDR3-1333	9-9-9-24 CR1	13993 MB/s
6x Phenom II X6 Black 1100T	3300 MHz	Gigabyte GA-890GPA-UD3H v2	AMD890GX Int.	Unganged Dual DDR3-1333	9-9-9-24 CR2	12444 MB/s
8x Opteron 2344 HE	1700 MHz	Supermicro H8DME-2	nForcePro-3600	Unganged Dual DDR2-667R	5-5-5-15 CR1	11945 MB/s
Celeron J1900	2000 MHz	Gigabyte GA-J1900N-D3V	BayTrailD Int.	Dual DDR3-1333	9-9-9-24 CR1	11370 MB/s
4x Phenom II X4 Black 940	3000 MHz	Asus M3N78-EM	GeForce8300 Int.	Ganged Dual DDR2-800	5-5-5-18 CR2	9671 MB/s
4x Opteron 2210 HE	1800 MHz	Tyan Thunder h2000M	BCM5785	Dual DDR2-600R	5-5-5-15 CR1	9468 MB/s
2x Athlon64 X2 Black 6400+	3200 MHz	MSI K9N SLI Platinum	nForce570SLI	Dual DDR2-800	4-4-4-11 CR1	9054 MB/s
8x Xeon E5462	2800 MHz	Intel S5400SF	i5400	Quad DDR2-640FB	5-5-5-15	8216 MB/s
4x Phenom X4 9500	2200 MHz	Asus M3A	AMD770	Ganged Dual DDR2-800	5-5-5-18 CR2	7792 MB/s
4x Athlon 5350	2050 MHz	ASRock AM1B-ITX	Yangtze Int.	DDR3-1600 SDRAM	11-11-11-28 CR2	7740 MB/s
4x Core 2 Extreme QX9650	3000 MHz	Gigabyte GA-EP35C-DS3R	P35	Dual DDR3-1066	8-8-8-20 CR2	7403 MB/s
2x Athlon64 X2 4000+	2100 MHz	ASRock ALiveNF7G-HDready	nForce7050-630a Int.	Dual DDR2-700	5-5-5-18 CR2	6881 MB/s
2x Opteron 240	1400 MHz	MSI K8D Master3-133 FS	AMD8100	Dual DDR400R	3-4-4-8 CR1	6774 MB/s
2x Pentium EE 955 HT	3466 MHz	Intel D955XBK	i955X	Dual DDR2-667	4-4-4-11	6282 MB/s
P4EE HT	3733 MHz	Intel SE7230NH1LX	iE7230	Dual DDR2-667	5-5-5-15	6139 MB/s
Nano X2 L4350	1600 MHz	VIA EPIA-M900	VX900H Int.	DDR3-1066 SDRAM	7-7-7-20 CR2	5921 MB/s
2x Core 2 Duo P8400	2266 MHz	MSI MegaBook PR201	GM45 Int.	Dual DDR2-667	5-5-5-15	5551 MB/s
2x Core 2 Extreme X6800	2933 MHz	Abit AB9	P965	Dual DDR2-800	5-5-5-18 CR2	5396 MB/s
4x Core 2 Extreme QX6700	2666 MHz	Intel D975XBX2	i975X	Dual DDR2-667	5-5-5-15	5284 MB/s
2x E-350	1600 MHz	ASRock E350M1	A50M Int.	DDR3-1066 SDRAM	8-8-8-20 CR1	4951 MB/s
2x Pentium D 820	2800 MHz	Abit Fatal1ty F-I90HD	RS600 Int.	Dual DDR2-800	5-5-5-18 CR2	4891 MB/s
2x Atom D2500	1866 MHz	Intel D2500CC	NM10 Int.	DDR3-1066 SDRAM	7-7-7-20 CR2	4764 MB/s
Athlon64 3200+	2000 MHz	ASRock 939S56-M	SiS756	Dual DDR400	2.5-3-3-8 CR2	4572 MB/s
2x Xeon HT	3400 MHz	Intel SE7320SP2	iE7320	Dual DDR333R	2.5-3-3-7	4213 MB/s
Celeron 420	1600 MHz	Intel DQ965GF	Q965 Int.	Dual DDR2-667	5-5-5-15	4195 MB/s
Opteron 248	2200 MHz	MSI K8T Master1-FAR	K8T800	Dual DDR266R	2-3-3-6 CR1	3673 MB/s
Nano L2200	1600 MHz	VIA VB8001	CN896 Int.	DDR2-667 SDRAM	5-5-5-15 CR2	3270 MB/s
Celeron D 326	2533 MHz	ASRock 775Twins-HDTV	RC410 Ext.	DDR2-533 SDRAM	4-4-4-11	3147 MB/s
Atom 230 HT	1600 MHz	Intel D945GCLF	i945GC Int.	DDR2-533 SDRAM	4-4-4-12	3051 MB/s
4x Xeon 5140	2333 MHz	Intel S5000VSA	i5000V	Dual DDR2-667FB	5-5-5-15	3009 MB/s
8x Xeon L5320	1866 MHz	Intel S5000VCL	i5000V	Dual DDR2-533FB	4-4-4-12	2987 MB/s
Sempron 2600+	1600 MHz	ASRock K8NF4G-SATA2	GeForce6100 Int.	DDR400 SDRAM	2.5-3-3-8 CR2	2578 MB/s

Memory Latency

CPU	CPU Clock	Motherboard	Chipset	Memory	CL-RCD-RP-RAS	Latency
Athlon64 X2 Black 6400+	3200 MHz	MSI K9N SLI Platinum	nForce570SLI	Dual DDR2-800	4-4-4-11 CR1	55.2 ns
Core i7-3770K	3500 MHz	MSI Z77A-GD55	Z77 Int.	Dual DDR3-1600	9-9-9-24 CR2	57.5 ns
Xeon E3-1245 v3	3400 MHz	Supermicro X10SAE	C226 Int.	Dual DDR3-1600	11-11-11-28 CR1	57.9 ns
Core i7-4770	3400 MHz	Intel DZ87KLT-75K	Z87 Int.	Dual DDR3-1600	9-9-9-27 CR2	58.3 ns
A10-6800K	4100 MHz	Gigabyte GA-F2A85X-UP4	A85X Int.	Dual DDR3-2133	9-11-10-27 CR2	59.6 ns
FX-8150	3600 MHz	Asus M5A97	AMD970	Dual DDR3-1866	9-10-9-27 CR2	60.3 ns
FX-8350	4000 MHz	Asus M5A99X Evo R2.0	AMD990X	Dual DDR3-1866	9-10-9-27 CR2	61.4 ns
A10-5800K	3800 MHz	Asus F2A55-M	A55 Int.	Dual DDR3-1866	9-10-9-27 CR2	62.0 ns
Core i7-4930K	3400 MHz	Gigabyte GA-X79-UD3	X79	Quad DDR3-1866	9-10-9-27 CR2	62.1 ns
Core i7-965 Extreme	3200 MHz	Asus P6T Deluxe	X58	Triple DDR3-1333	9-9-9-24 CR1	62.9 ns
Core i7-2600	3400 MHz	Asus P8P67	P67	Dual DDR3-1333	9-9-9-24 CR1	66.7 ns
Core i7-990X Extreme	3466 MHz	Intel DX58SO2	X58	Triple DDR3-1333	9-9-9-24 CR1	67.1 ns
Core i7-3960X Extreme	3300 MHz	Intel DX79SI	X79	Quad DDR3-1600	9-9-9-24 CR2	67.5 ns
Xeon X3430	2400 MHz	Supermicro X8SIL-F	i3420	Dual DDR3-1333	9-9-9-24 CR1	69.6 ns
Xeon X5550	2666 MHz	Supermicro X8DTN+	i5520	Triple DDR3-1333	9-9-9-24 CR1	70.3 ns
Core i7-3520M	**3600 MHz**	**Gateway EG50_HC_HR**	**HM70 Int.**	**Dual DDR3-1600**	**11-11-11-28 CR1**	**70.5 ns**
Athlon64 3200+	2000 MHz	ASRock 939S56-M	SiS756	Dual DDR400	2.5-3-3-8 CR2	72.4 ns
Phenom II X6 Black 1100T	3300 MHz	Gigabyte GA-890GPA-UD3H v2	AMD890GX Int.	Unganged Dual DDR3-1333	9-9-9-24 CR2	74.1 ns
Phenom II X4 Black 940	3000 MHz	Asus M3N78-EM	GeForce8300 Int.	Ganged Dual DDR2-800	5-5-5-18 CR2	74.2 ns
Core i7-5820K	3300 MHz	Gigabyte GA-X99-UD4	X99	Quad DDR4-2133	15-15-15-36 CR2	74.4 ns
A8-3850	2900 MHz	Gigabyte GA-A75M-UD2H	A75 Int.	Dual DDR3-1333	9-9-9-24 CR1	75.9 ns
Sempron 2600+	1600 MHz	ASRock K8NF4G-SATA2	GeForce6100 Int.	DDR400 SDRAM	2.5-3-3-8 CR2	77.0 ns
Athlon64 X2 4000+	2100 MHz	ASRock ALiveNF7G-HDready	nForce7050-630a Int.	Dual DDR2-700	5-5-5-18 CR2	77.9 ns
Pentium EE 955	3466 MHz	Intel D955XBK	i955X	Dual DDR2-667	4-4-4-11	78.0 ns
Xeon E5-2670	2600 MHz	Supermicro X9DR6-F	C600	Quad DDR3-1333	9-9-9-24	79.6 ns
A10-7850K	3700 MHz	Gigabyte GA-F2A88XM-D3H	A88X Int.	Dual DDR3-2133	9-11-10-31 CR2	79.6 ns
Core 2 Extreme X6800	2933 MHz	Abit AB9	P965	Dual DDR2-800	5-5-5-18 CR2	79.9 ns
Core 2 Extreme QX6700	2666 MHz	Intel D975XBX2	i975X	Dual DDR2-667	5-5-5-15	81.2 ns
P4EE	3733 MHz	Intel SE7230NH1LX	iE7230	Dual DDR2-667	5-5-5-15	82.4 ns
Opteron 6274	2200 MHz	Supermicro H8DGI-F	SR5690	Dual DDR3-1600R	11-11-11-28 CR1	87.0 ns
Opteron 248	2200 MHz	MSI K8T Master1-FAR	K8T800	Dual DDR266R	2-3-3-6 CR1	88.2 ns
Atom D2500	1866 MHz	Intel D2500CC	NM10 Int.	DDR3-1066 SDRAM	7-7-7-20 CR2	88.6 ns
Opteron 240	1400 MHz	MSI K8D Master3-133 FS	AMD8100	Dual DDR400R	3-4-4-8 CR1	89.9 ns
Core 2 Extreme QX9650	3000 MHz	Gigabyte GA-EP35C-DS3R	P35	Dual DDR3-1066	8-8-8-20 CR2	91.3 ns
Atom C2750	2400 MHz	Supermicro A1SAi-2750F	Avoton	Dual DDR3-1600	11-11-11-28 CR1	93.2 ns
Celeron J1900	2000 MHz	Gigabyte GA-J1900N-D3V	BayTrailD Int.	Dual DDR3-1333	9-9-9-24 CR1	93.7 ns
Opteron 2378	2400 MHz	Tyan Thunder n3600R	nForcePro-3600	Unganged Dual DDR2-800R	6-6-6-18 CR1	99.1 ns
Celeron 420	1600 MHz	Intel DQ965GF	Q965 Int.	Dual DDR2-667	5-5-5-15	99.5 ns
Core i5-650	3200 MHz	Supermicro C7SIM-Q	Q57 Int.	Dual DDR3-1333	9-9-9-24 CR1	100.3 ns
Core 2 Duo P8400	2266 MHz	MSI MegaBook PR201	GM45 Int.	Dual DDR2-667	5-5-5-15	101.4 ns
Pentium D 820	2800 MHz	Abit Fatal1ty F-I90HD	RS600 Int.	Dual DDR2-800	5-5-5-18 CR2	103.9 ns
Atom 230	1600 MHz	Intel D945GCLF	i945GC Int.	DDR2-533 SDRAM	4-4-4-12	105.7 ns
E-350	1600 MHz	ASRock E350M1	A50M Int.	DDR3-1066 SDRAM	8-8-8-20 CR1	107.0 ns
Opteron 2210 HE	1800 MHz	Tyan Thunder h2000M	BCM5785	Dual DDR2-600R	5-5-5-15 CR1	111.9 ns
Xeon 5140	2333 MHz	Intel S5000VSA	i5000V	Dual DDR2-667FB	5-5-5-15	113.3 ns
Xeon E5462	2800 MHz	Intel S5400SF	i5400	Quad DDR2-640FB	5-5-5-15	114.8 ns
Nano X2 L4350	1600 MHz	VIA EPIA-M900	VX900H Int.	DDR3-1066 SDRAM	7-7-7-20 CR2	120.0 ns
Opteron 2431	2400 MHz	Supermicro H8DI3+-F	SR5690	Unganged Dual DDR2-800R	6-6-6-18 CR1	124.4 ns
Xeon	3400 MHz	Intel SE7320SP2	iE7320	Dual DDR333R	2.5-3-3-7	124.7 ns
Xeon L5320	1866 MHz	Intel S5000VCL	i5000V	Dual DDR2-533FB	4-4-4-12	127.8 ns
Athlon 5350	2050 MHz	ASRock AM1B-ITX	Yangtze Int.	DDR3-1600 SDRAM	11-11-11-28 CR2	128.3 ns
Phenom X4 9500	2200 MHz	Asus M3A	AMD770	Ganged Dual DDR2-800	5-5-5-18 CR2	129.7 ns
Nano L2200	1600 MHz	VIA VB8001	CN896 Int.	DDR2-667 SDRAM	5-5-5-15 CR2	138.4 ns

Celeron D 326	2533 MHz	ASRock 775Twins-HDTV	RC410 Ext.	DDR2-533 SDRAM	4-4-4-11	153.7 ns
Opteron 2344 HE	1700 MHz	Supermicro H8DME-2	nForcePro-3600	Unganged Dual DDR2-667R	5-5-5-15 CR1	159.0 ns

CPU Queen

CPU	CPU Clock	Motherboard	Chipset	Memory	CL-RCD-RP-RAS	Score
16x Xeon E5-2670 HT	2600 MHz	Supermicro X9DR6-F	C600	Quad DDR3-1333	9-9-9-24	100531
6x Core i7-4930K HT	3400 MHz	Gigabyte GA-X79-UD3	X79	Quad DDR3-1866	9-10-9-27 CR2	62643
6x Core i7-3960X Extreme HT	3300 MHz	Intel DX79SI	X79	Quad DDR3-1600	9-9-9-24 CR2	62484
6x Core i7-5820K HT	3300 MHz	Gigabyte GA-X99-UD4	X99	Quad DDR4-2133	15-15-15-36 CR2	59940
6x Core i7-990X Extreme HT	3466 MHz	Intel DX58SO2	X58	Triple DDR3-1333	9-9-9-24 CR1	56836
32x Opteron 6274	2200 MHz	Supermicro H8DGI-F	SR5690	Dual DDR3-1600R	11-11-11-28 CR1	53879
8x Xeon X5550 HT	2666 MHz	Supermicro X8DTN+	i5520	Triple DDR3-1333	9-9-9-24 CR1	53544
4x Core i7-4770 HT	3400 MHz	Intel DZ87KLT-75K	Z87 Int.	Dual DDR3-1600	9-9-9-27 CR2	47291
4x Core i7-3770K HT	3500 MHz	MSI Z77A-GD55	Z77 Int.	Dual DDR3-1600	9-9-9-24 CR2	46747
4x Xeon E3-1245 v3 HT	3400 MHz	Supermicro X10SAE	C226 Int.	Dual DDR3-1600	11-11-11-28 CR1	45915
4x Core i7-2600 HT	3400 MHz	Asus P8P67	P67	Dual DDR3-1333	9-9-9-24 CR1	43907
12x Opteron 2431	2400 MHz	Supermicro H8DI3+-F	SR5690	Unganged Dual DDR2-800R	6-6-6-18 CR1	42550
8x Xeon E5462	2800 MHz	Intel S5400SF	i5400	Quad DDR2-640FB	5-5-5-15	41740
4x Core i7-965 Extreme HT	3200 MHz	Asus P6T Deluxe	X58	Triple DDR3-1333	9-9-9-24 CR1	37778
8x FX-8350	4000 MHz	Asus M5A99X Evo R2.0	AMD990X	Dual DDR3-1866	9-10-9-27 CR2	36089
8x Atom C2750	2400 MHz	Supermicro A1SAi-2750F	Avoton	Dual DDR3-1600	11-11-11-28 CR1	34010
6x Phenom II X6 Black 1100T	3300 MHz	Gigabyte GA-890GPA-UD3H v2	AMD890GX Int.	Unganged Dual DDR3-1333	9-9-9-24 CR2	32366
8x FX-8150	3600 MHz	Asus M5A97	AMD970	Dual DDR3-1866	9-10-9-27 CR2	31680
8x Opteron 2378	2400 MHz	Tyan Thunder n3600R	nForcePro-3600	Unganged Dual DDR2-800R	6-6-6-18 CR1	30784
8x Xeon L5320	1866 MHz	Intel S5000VCL	i5000V	Dual DDR2-533FB	4-4-4-12	26997
4x Core 2 Extreme QX9650	3000 MHz	Gigabyte GA-EP35C-DS3R	P35	Dual DDR3-1066	8-8-8-20 CR2	25523
2x Core i7-3520M HT	**3400 MHz**	**Gateway EG50_HC_HR**	**HM70 Int.**	**Dual DDR3-1600**	**11-11-11-28 CR1**	**23959**
4x A8-3850	2900 MHz	Gigabyte GA-A75M-UD2H	A75 Int.	Dual DDR3-1333	9-9-9-24 CR1	22162
4x Core 2 Extreme QX6700	2666 MHz	Intel D975XBX2	i975X	Dual DDR2-667	5-5-5-15	22013
8x Opteron 2344 HE	1700 MHz	Supermicro H8DME-2	nForcePro-3600	Unganged Dual DDR2-667R	5-5-5-15 CR1	21945
4x Phenom II X4 Black 940	3000 MHz	Asus M3N78-EM	GeForce8300 Int.	Ganged Dual DDR2-800	5-5-5-18 CR2	21896
4x A10-6800K	4100 MHz	Gigabyte GA-F2A85X-UP4	A85X Int.	Dual DDR3-2133	9-11-10-27 CR2	21655
2x Core i5-650 HT	3200 MHz	Supermicro C7SIM-Q	Q57 Int.	Dual DDR3-1333	9-9-9-24 CR1	21434
4x Xeon X3430	2400 MHz	Supermicro X8SIL-F	i3420	Dual DDR3-1333	9-9-9-24 CR1	21225
4x A10-5800K	3800 MHz	Asus F2A55-M	A55 Int.	Dual DDR3-1866	9-10-9-27 CR2	20154
4x A10-7850K	3700 MHz	Gigabyte GA-F2A88XM-D3H	A88X Int.	Dual DDR3-2133	9-11-10-31 CR2	19397
4x Xeon 5140	2333 MHz	Intel S5000VSA	i5000V	Dual DDR2-667FB	5-5-5-15	19226
Celeron J1900	2000 MHz	Gigabyte GA-J1900N-D3V	BayTrailD Int.	Dual DDR3-1333	9-9-9-24 CR1	18012
4x Phenom X4 9500	2200 MHz	Asus M3A	AMD770	Ganged Dual DDR2-800	5-5-5-18 CR2	16094
4x Athlon 5350	2050 MHz	ASRock AM1B-ITX	Yangtze Int.	DDR3-1600 SDRAM	11-11-11-28 CR2	14695
4x Opteron 2210 HE	1800 MHz	Tyan Thunder h2000M	BCM5785	Dual DDR2-600R	5-5-5-15 CR1	12584
2x Core 2 Extreme X6800	2933 MHz	Abit AB9	P965	Dual DDR2-800	5-5-5-18 CR2	12140
2x Athlon64 X2 Black 6400+	3200 MHz	MSI K9N SLI Platinum	nForce570SLI	Dual DDR2-800	4-4-4-11 CR1	11236
2x Core 2 Duo P8400	2266 MHz	MSI MegaBook PR201	GM45 Int.	Dual DDR2-667	5-5-5-15	9614
2x Pentium EE 955 HT	3466 MHz	Intel D955XBK	i955X	Dual DDR2-667	4-4-4-11	7485
2x Xeon HT	3400 MHz	Intel SE7320SP2	iE7320	Dual DDR333R	2.5-3-3-7	7304
2x Athlon64 X2 4000+	2100 MHz	ASRock ALiveNF7G-HDready	nForce7050-630a Int.	Dual DDR2-700	5-5-5-18 CR2	7300
2x Atom D2500	1866 MHz	Intel D2500CC	NM10 Int.	DDR3-1066 SDRAM	7-7-7-20 CR2	5904
Nano X2 L4350	1600 MHz	VIA EPIA-M900	VX900H Int.	DDR3-1066 SDRAM	7-7-7-20 CR2	5452
2x E-350	1600 MHz	ASRock E350M1	A50M Int.	DDR3-1066 SDRAM	8-8-8-20 CR1	5164
2x Opteron 240	1400 MHz	MSI K8D Master3-133 FS	AMD8100	Dual DDR400R	3-4-4-8 CR1	4879

2x Pentium D 820	2800 MHz	Abit Fatal1ty F-I90HD	RS600 Int.	Dual DDR2-800	5-5-5-18 CR2	4086
P4EE HT	3733 MHz	Intel SE7230NH1LX	iE7230	Dual DDR2-667	5-5-5-15	4021
Opteron 248	2200 MHz	MSI K8T Master1-FAR	K8T800	Dual DDR266R	2-3-3-6 CR1	3855
Atom 230 HT	1600 MHz	Intel D945GCLF	i945GC Int.	DDR2-533 SDRAM	4-4-4-12	3791
Athlon64 3200+	2000 MHz	ASRock 939S56-M	SiS756	Dual DDR400	2.5-3-3-8 CR2	3514
Celeron 420	1600 MHz	Intel DQ965GF	Q965 Int.	Dual DDR2-667	5-5-5-15	3301
Sempron 2600+	1600 MHz	ASRock K8NF4G-SATA2	GeForce6100 Int.	DDR400 SDRAM	2.5-3-3-8 CR2	2814
Nano L2200	1600 MHz	VIA VB8001	CN896 Int.	DDR2-667 SDRAM	5-5-5-15 CR2	2586
Celeron D 326	2533 MHz	ASRock 775Twins-HDTV	RC410 Ext.	DDR2-533 SDRAM	4-4-4-11	1839

CPU PhotoWorxx

CPU	CPU Clock	Motherboard	Chipset	Memory	CL-RCD-RP-RAS	Score
16x Xeon E5-2670 HT	2600 MHz	Supermicro X9DR6-F	C600	Quad DDR3-1333	9-9-9-24	38725 MPixel/s
32x Opteron 6274	2200 MHz	Supermicro H8DGI-F	SR5690	Dual DDR3-1600R	11-11-11-28 CR1	35478 MPixel/s
6x Core i7-5820K HT	3300 MHz	Gigabyte GA-X99-UD4	X99	Quad DDR4-2133	15-15-15-36 CR2	25266 MPixel/s
6x Core i7-4930K HT	3400 MHz	Gigabyte GA-X79-UD3	X79	Quad DDR3-1866	9-10-9-27 CR2	23599 MPixel/s
6x Core i7-3960X Extreme HT	3300 MHz	Intel DX79SI	X79	Quad DDR3-1600	9-9-9-24 CR2	22806 MPixel/s
8x Xeon X5550 HT	2666 MHz	Supermicro X8DTN+	i5520	Triple DDR3-1333	9-9-9-24 CR1	20428 MPixel/s
4x Core i7-3770K HT	3500 MHz	MSI Z77A-GD55	Z77 Int.	Dual DDR3-1600	9-9-9-24 CR2	14178 MPixel/s
4x Xeon E3-1245 v3 HT	3400 MHz	Supermicro X10SAE	C226 Int.	Dual DDR3-1600	11-11-11-28 CR1	14090 MPixel/s
4x Core i7-4770 HT	3400 MHz	Intel DZ87KLT-75K	Z87 Int.	Dual DDR3-1600	9-9-9-27 CR2	14001 MPixel/s
6x Core i7-990X Extreme HT	3466 MHz	Intel DX58SO2	X58	Triple DDR3-1333	9-9-9-24 CR1	12962 MPixel/s
8x FX-8350	4000 MHz	Asus M5A99X Evo R2.0	AMD990X	Dual DDR3-1866	9-10-9-27 CR2	12477 MPixel/s
8x FX-8150	3600 MHz	Asus M5A97	AMD970	Dual DDR3-1866	9-10-9-27 CR2	12457 MPixel/s
4x Core i7-965 Extreme HT	3200 MHz	Asus P6T Deluxe	X58	Triple DDR3-1333	9-9-9-24 CR1	11872 MPixel/s
12x Opteron 2431	2400 MHz	Supermicro H8DI3+-F	SR5690	Unganged Dual DDR2-800R	6-6-6-18 CR1	11495 MPixel/s
4x Core i7-2600 HT	3400 MHz	Asus P8P67	P67	Dual DDR3-1333	9-9-9-24 CR1	11115 MPixel/s
8x Opteron 2378	2400 MHz	Tyan Thunder n3600R	nForcePro-3600	Unganged Dual DDR2-800R	6-6-6-18 CR1	10673 MPixel/s
2x Core i7-3520M HT	**3600 MHz**	**Gateway EG50_HC_HR**	**HM70 Int.**	**Dual DDR3-1600**	**11-11-11-28 CR1**	**9932 MPixel/s**
4x A10-6800K	4100 MHz	Gigabyte GA-F2A85X-UP4	A85X Int.	Dual DDR3-2133	9-11-10-27 CR2	9603 MPixel/s
4x A10-5800K	3800 MHz	Asus F2A55-M	A55 Int.	Dual DDR3-1866	9-10-9-27 CR2	9078 MPixel/s
4x A10-7850K	3700 MHz	Gigabyte GA-F2A88XM-D3H	A88X Int.	Dual DDR3-2133	9-11-10-31 CR2	8913 MPixel/s
8x Atom C2750	2400 MHz	Supermicro A1SAi-2750F	Avoton	Dual DDR3-1600	11-11-11-28 CR1	8886 MPixel/s
4x Xeon X3430	2400 MHz	Supermicro X8SIL-F	i3420	Dual DDR3-1333	9-9-9-24 CR1	8581 MPixel/s
4x A8-3850	2900 MHz	Gigabyte GA-A75M-UD2H	A75 Int.	Dual DDR3-1333	9-9-9-24 CR1	8064 MPixel/s
6x Phenom II X6 Black 1100T	3300 MHz	Gigabyte GA-890GPA-UD3H v2	AMD890GX Int.	Unganged Dual DDR3-1333	9-9-9-24 CR2	6975 MPixel/s
2x Core i5-650 HT	3200 MHz	Supermicro C7SIM-Q	Q57 Int.	Dual DDR3-1333	9-9-9-24 CR1	6862 MPixel/s
8x Opteron 2344 HE	1700 MHz	Supermicro H8DME-2	nForcePro-3600	Unganged Dual DDR2-667R	5-5-5-15 CR1	6131 MPixel/s
4x Phenom II X4 Black 940	3000 MHz	Asus M3N78-EM	GeForce8300 Int.	Ganged Dual DDR2-800	5-5-5-18 CR2	5627 MPixel/s
Celeron J1900	2000 MHz	Gigabyte GA-J1900N-D3V	BayTrailD Int.	Dual DDR3-1333	9-9-9-24 CR1	5276 MPixel/s
8x Xeon E5462	2800 MHz	Intel S5400SF	i5400	Quad DDR2-640FB	5-5-5-15	4730 MPixel/s
4x Core 2 Extreme QX9650	3000 MHz	Gigabyte GA-EP35C-DS3R	P35	Dual DDR3-1066	8-8-8-20 CR2	4183 MPixel/s
4x Athlon 5350	2050 MHz	ASRock AM1B-ITX	Yangtze Int.	DDR3-1600 SDRAM	11-11-11-28 CR2	4179 MPixel/s
4x Phenom X4 9500	2200 MHz	Asus M3A	AMD770	Ganged Dual DDR2-800	5-5-5-18 CR2	3840 MPixel/s
4x Opteron 2210 HE	1800 MHz	Tyan Thunder h2000M	BCM5785	Dual DDR2-600R	5-5-5-15 CR1	3707 MPixel/s
2x Core 2 Extreme X6800	2933 MHz	Abit AB9	P965	Dual DDR2-800	5-5-5-18 CR2	3462 MPixel/s
2x Core 2 Duo P8400	2266 MHz	MSI MegaBook PR201	GM45 Int.	Dual DDR2-667	5-5-5-15	3041 MPixel/s
2x Athlon64 X2 Black 6400+	3200 MHz	MSI K9N SLI Platinum	nForce570SLI	Dual DDR2-800	4-4-4-11 CR1	3025 MPixel/s
2x Pentium EE 955 HT	3466 MHz	Intel D955XBK	i955X	Dual DDR2-667	4-4-4-11	2926 MPixel/s
4x Core 2 Extreme QX6700	2666 MHz	Intel D975XBX2	i975X	Dual DDR2-667	5-5-5-15	2793 MPixel/s
Nano X2 L4350	1600 MHz	VIA EPIA-M900	VX900H Int.	DDR3-1066 SDRAM	7-7-7-20 CR2	2536 MPixel/s

2x Athlon64 X2 4000+	2100 MHz	ASRock ALiveNF7G-HDready	nForce7050-630a Int.	Dual DDR2-700	5-5-5-18 CR2	2390 MPixel/s
P4EE HT	3733 MHz	Intel SE7230NH1LX	iE7230	Dual DDR2-667	5-5-5-15	2147 MPixel/s
2x E-350	1600 MHz	ASRock E350M1	A50M Int.	DDR3-1066 SDRAM	8-8-8-20 CR1	1936 MPixel/s
8x Xeon L5320	1866 MHz	Intel S5000VCL	i5000V	Dual DDR2-533FB	4-4-4-12	1904 MPixel/s
2x Pentium D 820	2800 MHz	Abit Fatal1ty F-I90HD	RS600 Int.	Dual DDR2-800	5-5-5-18 CR2	1895 MPixel/s
4x Xeon 5140	2333 MHz	Intel S5000VSA	i5000V	Dual DDR2-667FB	5-5-5-15	1864 MPixel/s
Celeron 420	1600 MHz	Intel DQ965GF	Q965 Int.	Dual DDR2-667	5-5-5-15	1852 MPixel/s
2x Opteron 240	1400 MHz	MSI K8D Master3-133 FS	AMD8100	Dual DDR400R	3-4-4-8 CR1	1850 MPixel/s
2x Atom D2500	1866 MHz	Intel D2500CC	NM10 Int.	DDR3-1066 SDRAM	7-7-7-20 CR2	1844 MPixel/s
2x Xeon HT	3400 MHz	Intel SE7320SP2	iE7320	Dual DDR333R	2.5-3-3-7	1676 MPixel/s
Athlon64 3200+	2000 MHz	ASRock 939S56-M	SiS756	Dual DDR400	2.5-3-3-8 CR2	1224 MPixel/s
Nano L2200	1600 MHz	VIA VB8001	CN896 Int.	DDR2-667 SDRAM	5-5-5-15 CR2	1167 MPixel/s
Opteron 248	2200 MHz	MSI K8T Master1-FAR	K8T800	Dual DDR266R	2-3-3-6 CR1	1100 MPixel/s
Atom 230 HT	1600 MHz	Intel D945GCLF	i945GC Int.	DDR2-533 SDRAM	4-4-4-12	1099 MPixel/s
Celeron D 326	2533 MHz	ASRock 775Twins-HDTV	RC410 Ext.	DDR2-533 SDRAM	4-4-4-11	879 MPixel/s
Sempron 2600+	1600 MHz	ASRock K8NF4G-SATA2	GeForce6100 Int.	DDR400 SDRAM	2.5-3-3-8 CR2	826 MPixel/s

CPU ZLib

CPU	CPU Clock	Motherboard	Chipset	Memory	CL-RCD-RP-RAS	Score
16x Xeon E5-2670 HT	2600 MHz	Supermicro X9DR6-F	C600	Quad DDR3-1333	9-9-9-24	975.4 MB/s
32x Opteron 6274	2200 MHz	Supermicro H8DGI-F	SR5690	Dual DDR3-1600R	11-11-11-28 CR1	672.7 MB/s
6x Core i7-4930K HT	3400 MHz	Gigabyte GA-X79-UD3	X79	Quad DDR3-1866	9-10-9-27 CR2	455.0 MB/s
6x Core i7-3960X Extreme HT	3300 MHz	Intel DX79SI	X79	Quad DDR3-1600	9-9-9-24 CR2	444.5 MB/s
6x Core i7-5820K HT	3300 MHz	Gigabyte GA-X99-UD4	X99	Quad DDR4-2133	15-15-15-36 CR2	436.1 MB/s
12x Opteron 2431	2400 MHz	Supermicro H8DI3+-F	SR5690	Unganged Dual DDR2-800R	6-6-6-18 CR1	366.5 MB/s
6x Core i7-990X Extreme HT	3466 MHz	Intel DX58SO2	X58	Triple DDR3-1333	9-9-9-24 CR1	358.7 MB/s
8x Xeon X5550 HT	2666 MHz	Supermicro X8DTN+	i5520	Triple DDR3-1333	9-9-9-24 CR1	358.1 MB/s
8x FX-8350	4000 MHz	Asus M5A99X Evo R2.0	AMD990X	Dual DDR3-1866	9-10-9-27 CR2	346.1 MB/s
4x Core i7-4770 HT	3400 MHz	Intel DZ87KLT-75K	Z87 Int.	Dual DDR3-1600	9-9-9-27 CR2	320.0 MB/s
4x Core i7-3770K HT	3500 MHz	MSI Z77A-GD55	Z77 Int.	Dual DDR3-1600	9-9-9-24 CR2	317.2 MB/s
4x Xeon E3-1245 v3 HT	3400 MHz	Supermicro X10SAE	C226 Int.	Dual DDR3-1600	11-11-11-28 CR1	308.6 MB/s
4x Core i7-2600 HT	3400 MHz	Asus P8P67	P67	Dual DDR3-1333	9-9-9-24 CR1	289.2 MB/s
8x Xeon E5462	2800 MHz	Intel S5400SF	i5400	Quad DDR2-640FB	5-5-5-15	281.4 MB/s
8x FX-8150	3600 MHz	Asus M5A97	AMD970	Dual DDR3-1866	9-10-9-27 CR2	276.3 MB/s
6x Phenom II X6 Black 1100T	3300 MHz	Gigabyte GA-890GPA-UD3H v2	AMD890GX Int.	Unganged Dual DDR3-1333	9-9-9-24 CR2	256.7 MB/s
8x Opteron 2378	2400 MHz	Tyan Thunder n3600R	nForcePro-3600	Unganged Dual DDR2-800R	6-6-6-18 CR1	244.3 MB/s
4x Core i7-965 Extreme HT	3200 MHz	Asus P6T Deluxe	X58	Triple DDR3-1333	9-9-9-24 CR1	222.7 MB/s
8x Atom C2750	2400 MHz	Supermicro A1SAi-2750F	Avoton	Dual DDR3-1600	11-11-11-28 CR1	209.2 MB/s
8x Xeon L5320	1866 MHz	Intel S5000VCL	i5000V	Dual DDR2-533FB	4-4-4-12	189.4 MB/s
4x A10-6800K	4100 MHz	Gigabyte GA-F2A85X-UP4	A85X Int.	Dual DDR3-2133	9-11-10-27 CR2	183.0 MB/s
4x A10-7850K	3700 MHz	Gigabyte GA-F2A88XM-D3H	A88X Int.	Dual DDR3-2133	9-11-10-31 CR2	174.8 MB/s
8x Opteron 2344 HE	1700 MHz	Supermicro H8DME-2	nForcePro-3600	Unganged Dual DDR2-667R	5-5-5-15 CR1	174.3 MB/s
4x A10-5800K	3800 MHz	Asus F2A55-M	A55 Int.	Dual DDR3-1866	9-10-9-27 CR2	167.7 MB/s
4x Phenom II X4 Black 940	3000 MHz	Asus M3N78-EM	GeForce8300 Int.	Ganged Dual DDR2-800	5-5-5-18 CR2	154.7 MB/s
4x Core 2 Extreme QX9650	3000 MHz	Gigabyte GA-EP35C-DS3R	P35	Dual DDR3-1066	8-8-8-20 CR2	153.2 MB/s
4x A8-3850	2900 MHz	Gigabyte GA-A75M-UD2H	A75 Int.	Dual DDR3-1333	9-9-9-24 CR1	152.5 MB/s
2x Core i7-3520M HT	**3400 MHz**	**Gateway EG50_HC_HR**	**HM70 Int.**	**Dual DDR3-1600**	**11-11-11-28 CR1**	**146.3 MB/s**
4x Core 2 Extreme QX6700	2666 MHz	Intel D975XBX2	i975X	Dual DDR2-667	5-5-5-15	136.2 MB/s
4x Xeon 5140	2333 MHz	Intel S5000VSA	i5000V	Dual DDR2-667FB	5-5-5-15	117.7 MB/s
4x Phenom X4 9500	2200 MHz	Asus M3A	AMD770	Ganged Dual DDR2-800	5-5-5-18 CR2	112.5 MB/s
4x Xeon X3430	2400 MHz	Supermicro X8SIL-F	i3420	Dual DDR3-1333	9-9-9-24 CR1	108.3 MB/s

2x Core i5-650 HT	3200 MHz	Supermicro C7SIM-Q	Q57 Int.	Dual DDR3-1333	9-9-9-24 CR1	105.8 MB/s
Celeron J1900	2000 MHz	Gigabyte GA-J1900N-D3V	BayTrailD Int.	Dual DDR3-1333	9-9-9-24 CR1	97.1 MB/s
4x Athlon 5350	2050 MHz	ASRock AM1B-ITX	Yangtze Int.	DDR3-1600 SDRAM	11-11-11-28 CR2	95.6 MB/s
4x Opteron 2210 HE	1800 MHz	Tyan Thunder h2000M	BCM5785	Dual DDR2-600R	5-5-5-15 CR1	82.8 MB/s
2x Core 2 Extreme X6800	2933 MHz	Abit AB9	P965	Dual DDR2-800	5-5-5-18 CR2	75.0 MB/s
2x Athlon64 X2 Black 6400+	3200 MHz	MSI K9N SLI Platinum	nForce570SLI	Dual DDR2-800	4-4-4-11 CR1	73.7 MB/s
2x Pentium EE 955 HT	3466 MHz	Intel D955XBK	i955X	Dual DDR2-667	4-4-4-11	59.6 MB/s
2x Xeon HT	3400 MHz	Intel SE7320SP2	iE7320	Dual DDR333R	2.5-3-3-7	57.8 MB/s
2x Core 2 Duo P8400	2266 MHz	MSI MegaBook PR201	GM45 Int.	Dual DDR2-667	5-5-5-15	57.5 MB/s
2x Athlon64 X2 4000+	2100 MHz	ASRock ALiveNF7G-HDready	nForce7050-630a Int.	Dual DDR2-700	5-5-5-18 CR2	47.3 MB/s
2x Pentium D 820	2800 MHz	Abit Fatal1ty F-I90HD	RS600 Int.	Dual DDR2-800	5-5-5-18 CR2	41.5 MB/s
Nano X2 L4350	1600 MHz	VIA EPIA-M900	VX900H Int.	DDR3-1066 SDRAM	7-7-7-20 CR2	33.3 MB/s
2x E-350	1600 MHz	ASRock E350M1	A50M Int.	DDR3-1066 SDRAM	8-8-8-20 CR1	32.9 MB/s
P4EE HT	3733 MHz	Intel SE7230NH1LX	iE7230	Dual DDR2-667	5-5-5-15	32.2 MB/s
2x Atom D2500	1866 MHz	Intel D2500CC	NM10 Int.	DDR3-1066 SDRAM	7-7-7-20 CR2	31.6 MB/s
2x Opteron 240	1400 MHz	MSI K8D Master3-133 FS	AMD8100	Dual DDR400R	3-4-4-8 CR1	30.8 MB/s
Opteron 248	2200 MHz	MSI K8T Master1-FAR	K8T800	Dual DDR266R	2-3-3-6 CR1	24.3 MB/s
Athlon64 3200+	2000 MHz	ASRock 939S56-M	SiS756	Dual DDR400	2.5-3-3-8 CR2	22.8 MB/s
Celeron 420	1600 MHz	Intel DQ965GF	Q965 Int.	Dual DDR2-667	5-5-5-15	20.3 MB/s
Atom 230 HT	1600 MHz	Intel D945GCLF	i945GC Int.	DDR2-533 SDRAM	4-4-4-12	18.5 MB/s
Celeron D 326	2533 MHz	ASRock 775Twins-HDTV	RC410 Ext.	DDR2-533 SDRAM	4-4-4-11	17.4 MB/s
Sempron 2600+	1600 MHz	ASRock K8NF4G-SATA2	GeForce6100 Int.	DDR400 SDRAM	2.5-3-3-8 CR2	16.3 MB/s
Nano L2200	1600 MHz	VIA VB8001	CN896 Int.	DDR2-667 SDRAM	5-5-5-15 CR2	15.2 MB/s

CPU AES

CPU	CPU Clock	Motherboard	Chipset	Memory	CL-RCD-RP-RAS	Score
16x Xeon E5-2670 HT	2600 MHz	Supermicro X9DR6-F	C600	Quad DDR3-1333	9-9-9-24	46884 MB/s
32x Opteron 6274	2200 MHz	Supermicro H8DGI-F	SR5690	Dual DDR3-1600R	11-11-11-28 CR1	38007 MB/s
6x Core i7-5820K HT	3300 MHz	Gigabyte GA-X99-UD4	X99	Quad DDR4-2133	15-15-15-36 CR2	23204 MB/s
6x Core i7-3960X Extreme HT	3300 MHz	Intel DX79SI	X79	Quad DDR3-1600	9-9-9-24 CR2	21097 MB/s
6x Core i7-4930K HT	3400 MHz	Gigabyte GA-X79-UD3	X79	Quad DDR3-1866	9-10-9-27 CR2	21094 MB/s
8x FX-8350	4000 MHz	Asus M5A99X Evo R2.0	AMD990X	Dual DDR3-1866	9-10-9-27 CR2	17312 MB/s
4x Core i7-4770 HT	3400 MHz	Intel DZ87KLT-75K	Z87 Int.	Dual DDR3-1600	9-9-9-27 CR2	16800 MB/s
4x Xeon E3-1245 v3 HT	3400 MHz	Supermicro X10SAE	C226 Int.	Dual DDR3-1600	11-11-11-28 CR1	16333 MB/s
8x FX-8150	3600 MHz	Asus M5A97	AMD970	Dual DDR3-1866	9-10-9-27 CR2	15406 MB/s
4x Core i7-3770K HT	3500 MHz	MSI Z77A-GD55	Z77 Int.	Dual DDR3-1600	9-9-9-24 CR2	14455 MB/s
4x Core i7-2600 HT	3400 MHz	Asus P8P67	P67	Dual DDR3-1333	9-9-9-24 CR1	13681 MB/s
6x Core i7-990X Extreme HT	3466 MHz	Intel DX58SO2	X58	Triple DDR3-1333	9-9-9-24 CR1	12247 MB/s
4x A10-6800K	4100 MHz	Gigabyte GA-F2A85X-UP4	A85X Int.	Dual DDR3-2133	9-11-10-27 CR2	9124 MB/s
4x A10-7850K	3700 MHz	Gigabyte GA-F2A88XM-D3H	A88X Int.	Dual DDR3-2133	9-11-10-31 CR2	8465 MB/s
4x A10-5800K	3800 MHz	Asus F2A55-M	A55 Int.	Dual DDR3-1866	9-10-9-27 CR2	8460 MB/s
2x Core i7-3520M HT	**3400 MHz**	**Gateway EG50_HC_HR**	**HM70 Int.**	**Dual DDR3-1600**	**11-11-11-28 CR1**	**6610 MB/s**
4x Athlon 5350	2050 MHz	ASRock AM1B-ITX	Yangtze Int.	DDR3-1600 SDRAM	11-11-11-28 CR2	6532 MB/s
8x Atom C2750	2400 MHz	Supermicro A1SAi-2750F	Avoton	Dual DDR3-1600	11-11-11-28 CR1	4053 MB/s
2x Core i5-650 HT	3200 MHz	Supermicro C7SIM-Q	Q57 Int.	Dual DDR3-1333	9-9-9-24 CR1	3782 MB/s
Nano X2 L4350	1600 MHz	VIA EPIA-M900	VX900H Int.	DDR3-1066 SDRAM	7-7-7-20 CR2	2908 MB/s
12x Opteron 2431	2400 MHz	Supermicro H8DI3+-F	SR5690	Unganged Dual DDR2-800R	6-6-6-18 CR1	1930 MB/s
Nano L2200	1600 MHz	VIA VB8001	CN896 Int.	DDR2-667 SDRAM	5-5-5-15 CR2	1447 MB/s
6x Phenom II X6 Black 1100T	3300 MHz	Gigabyte GA-890GPA-UD3H v2	AMD890GX Int.	Unganged Dual DDR3-1333	9-9-9-24 CR2	1332 MB/s
8x Opteron 2378	2400 MHz	Tyan Thunder n3600R	nForcePro-3600	Unganged Dual DDR2-800R	6-6-6-18 CR1	1286 MB/s
8x Xeon E5462	2800 MHz	Intel S5400SF	i5400	Quad DDR2-640FB	5-5-5-15	1212 MB/s

8x Xeon X5550 HT	2666 MHz	Supermicro X8DTN+	i5520	Triple DDR3-1333	9-9-9-24 CR1	1153 MB/s
8x Opteron 2344 HE	1700 MHz	Supermicro H8DME-2	nForcePro-3600	Unganged Dual DDR2-667R	5-5-5-15 CR1	913 MB/s
4x Phenom II X4 Black 940	3000 MHz	Asus M3N78-EM	GeForce8300 Int.	Ganged Dual DDR2-800	5-5-5-18 CR2	802 MB/s
8x Xeon L5320	1866 MHz	Intel S5000VCL	i5000V	Dual DDR2-533FB	4-4-4-12	790 MB/s
4x A8-3850	2900 MHz	Gigabyte GA-A75M-UD2H	A75 Int.	Dual DDR3-1333	9-9-9-24 CR1	789 MB/s
4x Core i7-965 Extreme HT	3200 MHz	Asus P6T Deluxe	X58	Triple DDR3-1333	9-9-9-24 CR1	721 MB/s
4x Core 2 Extreme QX9650	3000 MHz	Gigabyte GA-EP35C-DS3R	P35	Dual DDR3-1066	8-8-8-20 CR2	651 MB/s
4x Phenom X4 9500	2200 MHz	Asus M3A	AMD770	Ganged Dual DDR2-800	5-5-5-18 CR2	587 MB/s
4x Core 2 Extreme QX6700	2666 MHz	Intel D975XBX2	i975X	Dual DDR2-667	5-5-5-15	566 MB/s
4x Xeon X3430	2400 MHz	Supermicro X8SIL-F	i3420	Dual DDR3-1333	9-9-9-24 CR1	524 MB/s
4x Xeon 5140	2333 MHz	Intel S5000VSA	i5000V	Dual DDR2-667FB	5-5-5-15	493 MB/s
4x Opteron 2210 HE	1800 MHz	Tyan Thunder h2000M	BCM5785	Dual DDR2-600R	5-5-5-15 CR1	473 MB/s
2x Athlon64 X2 Black 6400+	3200 MHz	MSI K9N SLI Platinum	nForce570SLI	Dual DDR2-800	4-4-4-11 CR1	421 MB/s
Celeron J1900	2000 MHz	Gigabyte GA-J1900N-D3V	BayTrailD Int.	Dual DDR3-1333	9-9-9-24 CR1	387 MB/s
2x Core 2 Extreme X6800	2933 MHz	Abit AB9	P965	Dual DDR2-800	5-5-5-18 CR2	311 MB/s
2x Pentium EE 955 HT	3466 MHz	Intel D955XBK	i955X	Dual DDR2-667	4-4-4-11	277 MB/s
2x Athlon64 X2 4000+	2100 MHz	ASRock ALiveNF7G-HDready	nForce7050-630a Int.	Dual DDR2-700	5-5-5-18 CR2	274 MB/s
2x Xeon HT	3400 MHz	Intel SE7320SP2	iE7320	Dual DDR333R	2.5-3-3-7	269 MB/s
2x Core 2 Duo P8400	2266 MHz	MSI MegaBook PR201	GM45 Int.	Dual DDR2-667	5-5-5-15	245 MB/s
2x Pentium D 820	2800 MHz	Abit Fatal1ty F-I90HD	RS600 Int.	Dual DDR2-800	5-5-5-18 CR2	242 MB/s
2x Opteron 240	1400 MHz	MSI K8D Master3-133 FS	AMD8100	Dual DDR400R	3-4-4-8 CR1	184 MB/s
2x E-350	1600 MHz	ASRock E350M1	A50M Int.	DDR3-1066 SDRAM	8-8-8-20 CR1	153 MB/s
P4EE HT	3733 MHz	Intel SE7230NH1LX	iE7230	Dual DDR2-667	5-5-5-15	148 MB/s
Opteron 248	2200 MHz	MSI K8T Master1-FAR	K8T800	Dual DDR266R	2-3-3-6 CR1	144 MB/s
Athlon64 3200+	2000 MHz	ASRock 939S56-M	SiS756	Dual DDR400	2.5-3-3-8 CR2	131 MB/s
Celeron D 326	2533 MHz	ASRock 775Twins-HDTV	RC410 Ext.	DDR2-533 SDRAM	4-4-4-11	109 MB/s
Sempron 2600+	1600 MHz	ASRock K8NF4G-SATA2	GeForce6100 Int.	DDR400 SDRAM	2.5-3-3-8 CR2	105 MB/s
2x Atom D2500	1866 MHz	Intel D2500CC	NM10 Int.	DDR3-1066 SDRAM	7-7-7-20 CR2	98 MB/s
Celeron 420	1600 MHz	Intel DQ965GF	Q965 Int.	Dual DDR2-667	5-5-5-15	84 MB/s
Atom 230 HT	1600 MHz	Intel D945GCLF	i945GC Int.	DDR2-533 SDRAM	4-4-4-12	44 MB/s

CPU Hash

CPU	CPU Clock	Motherboard	Chipset	Memory	CL-RCD-RP-RAS	Score
32x Opteron 6274	2200 MHz	Supermicro H8DGI-F	SR5690	Dual DDR3-1600R	11-11-11-28 CR1	9056 MB/s
16x Xeon E5-2670 HT	2600 MHz	Supermicro X9DR6-F	C600	Quad DDR3-1333	9-9-9-24	8724 MB/s
6x Core i7-5820K HT	3300 MHz	Gigabyte GA-X99-UD4	X99	Quad DDR4-2133	15-15-15-36 CR2	5231 MB/s
12x Opteron 2431	2400 MHz	Supermicro H8DI3+-F	SR5690	Unganged Dual DDR2-800R	6-6-6-18 CR1	4783 MB/s
6x Core i7-4930K HT	3400 MHz	Gigabyte GA-X79-UD3	X79	Quad DDR3-1866	9-10-9-27 CR2	4368 MB/s
8x FX-8350	4000 MHz	Asus M5A99X Evo R2.0	AMD990X	Dual DDR3-1866	9-10-9-27 CR2	4104 MB/s
6x Core i7-3960X Extreme HT	3300 MHz	Intel DX79SI	X79	Quad DDR3-1600	9-9-9-24 CR2	3924 MB/s
4x Core i7-4770 HT	3400 MHz	Intel DZ87KLT-75K	Z87 Int.	Dual DDR3-1600	9-9-9-27 CR2	3786 MB/s
4x Xeon E3-1245 v3 HT	3400 MHz	Supermicro X10SAE	C226 Int.	Dual DDR3-1600	11-11-11-28 CR1	3679 MB/s
8x FX-8150	3600 MHz	Asus M5A97	AMD970	Dual DDR3-1866	9-10-9-27 CR2	3674 MB/s
8x Xeon E5462	2800 MHz	Intel S5400SF	i5400	Quad DDR2-640FB	5-5-5-15	3604 MB/s
6x Phenom II X6 Black 1100T	3300 MHz	Gigabyte GA-890GPA-UD3H v2	AMD890GX Int.	Unganged Dual DDR3-1333	9-9-9-24 CR2	3304 MB/s
8x Opteron 2378	2400 MHz	Tyan Thunder n3600R	nForcePro-3600	Unganged Dual DDR2-800R	6-6-6-18 CR1	3188 MB/s
6x Core i7-990X Extreme HT	3466 MHz	Intel DX58SO2	X58	Triple DDR3-1333	9-9-9-24 CR1	3137 MB/s
8x Xeon X5550 HT	2666 MHz	Supermicro X8DTN+	i5520	Triple DDR3-1333	9-9-9-24 CR1	3094 MB/s
4x Core i7-3770K HT	3500 MHz	MSI Z77A-GD55	Z77 Int.	Dual DDR3-1600	9-9-9-24 CR2	2995 MB/s
4x A10-7850K	3700 MHz	Gigabyte GA-F2A88XM-D3H	A88X Int.	Dual DDR3-2133	9-11-10-31 CR2	2621 MB/s
4x Core i7-2600 HT	3400 MHz	Asus P8P67	P67	Dual DDR3-1333	9-9-9-24 CR1	2544 MB/s

8x Xeon L5320	1866 MHz	Intel S5000VCL	i5000V	Dual DDR2-533FB	4-4-4-12	2345 MB/s
8x Opteron 2344 HE	1700 MHz	Supermicro H8DME-2	nForcePro-3600	Unganged Dual DDR2-667R	5-5-5-15 CR1	2242 MB/s
4x A10-6800K	4100 MHz	Gigabyte GA-F2A85X-UP4	A85X Int.	Dual DDR3-2133	9-11-10-27 CR2	2159 MB/s
4x Phenom II X4 Black 940	3000 MHz	Asus M3N78-EM	GeForce8300 Int.	Ganged Dual DDR2-800	5-5-5-18 CR2	1989 MB/s
4x A10-5800K	3800 MHz	Asus F2A55-M	A55 Int.	Dual DDR3-1866	9-10-9-27 CR2	1986 MB/s
8x Atom C2750	2400 MHz	Supermicro A1SAi-2750F	Avoton	Dual DDR3-1600	11-11-11-28 CR1	1965 MB/s
4x Core 2 Extreme QX9650	3000 MHz	Gigabyte GA-EP35C-DS3R	P35	Dual DDR3-1066	8-8-8-20 CR2	1942 MB/s
4x Core i7-965 Extreme HT	3200 MHz	Asus P6T Deluxe	X58	Triple DDR3-1333	9-9-9-24 CR1	1936 MB/s
4x A8-3850	2900 MHz	Gigabyte GA-A75M-UD2H	A75 Int.	Dual DDR3-1333	9-9-9-24 CR1	1914 MB/s
4x Core 2 Extreme QX6700	2666 MHz	Intel D975XBX2	i975X	Dual DDR2-667	5-5-5-15	1680 MB/s
4x Xeon X3430	2400 MHz	Supermicro X8SIL-F	i3420	Dual DDR3-1333	9-9-9-24 CR1	1677 MB/s
4x Xeon 5140	2333 MHz	Intel S5000VSA	i5000V	Dual DDR2-667FB	5-5-5-15	1464 MB/s
4x Phenom X4 9500	2200 MHz	Asus M3A	AMD770	Ganged Dual DDR2-800	5-5-5-18 CR2	1441 MB/s
2x Core i7-3520M HT	**3400 MHz**	**Gateway EG50_HC_HR**	**HM70 Int.**	**Dual DDR3-1600**	**11-11-11-28 CR1**	**1366 MB/s**
4x Opteron 2210 HE	1800 MHz	Tyan Thunder h2000M	BCM5785	Dual DDR2-600R	5-5-5-15 CR1	1101 MB/s
4x Athlon 5350	2050 MHz	ASRock AM1B-ITX	Yangtze Int.	DDR3-1600 SDRAM	11-11-11-28 CR2	998 MB/s
2x Athlon64 X2 Black 6400+	3200 MHz	MSI K9N SLI Platinum	nForce570SLI	Dual DDR2-800	4-4-4-11 CR1	980 MB/s
Nano X2 L4350	1600 MHz	VIA EPIA-M900	VX900H Int.	DDR3-1066 SDRAM	7-7-7-20 CR2	976 MB/s
2x Core i5-650 HT	3200 MHz	Supermicro C7SIM-Q	Q57 Int.	Dual DDR3-1333	9-9-9-24 CR1	969 MB/s
2x Core 2 Extreme X6800	2933 MHz	Abit AB9	P965	Dual DDR2-800	5-5-5-18 CR2	925 MB/s
Celeron J1900	2000 MHz	Gigabyte GA-J1900N-D3V	BayTrailD Int.	Dual DDR3-1333	9-9-9-24 CR1	911 MB/s
2x Pentium EE 955 HT	3466 MHz	Intel D955XBK	i955X	Dual DDR2-667	4-4-4-11	828 MB/s
2x Xeon HT	3400 MHz	Intel SE7320SP2	iE7320	Dual DDR333R	2.5-3-3-7	809 MB/s
2x Core 2 Duo P8400	2266 MHz	MSI MegaBook PR201	GM45 Int.	Dual DDR2-667	5-5-5-15	730 MB/s
2x Athlon64 X2 4000+	2100 MHz	ASRock ALiveNF7G-HDready	nForce7050-630a Int.	Dual DDR2-700	5-5-5-18 CR2	641 MB/s
2x Pentium D 820	2800 MHz	Abit Fatal1ty F-I90HD	RS600 Int.	Dual DDR2-800	5-5-5-18 CR2	548 MB/s
Nano L2200	1600 MHz	VIA VB8001	CN896 Int.	DDR2-667 SDRAM	5-5-5-15 CR2	489 MB/s
P4EE HT	3733 MHz	Intel SE7230NH1LX	iE7230	Dual DDR2-667	5-5-5-15	443 MB/s
2x Opteron 240	1400 MHz	MSI K8D Master3-133 FS	AMD8100	Dual DDR400R	3-4-4-8 CR1	427 MB/s
2x Atom D2500	1866 MHz	Intel D2500CC	NM10 Int.	DDR3-1066 SDRAM	7-7-7-20 CR2	350 MB/s
Opteron 248	2200 MHz	MSI K8T Master1-FAR	K8T800	Dual DDR266R	2-3-3-6 CR1	336 MB/s
2x E-350	1600 MHz	ASRock E350M1	A50M Int.	DDR3-1066 SDRAM	8-8-8-20 CR1	326 MB/s
Athlon64 3200+	2000 MHz	ASRock 939S56-M	SiS756	Dual DDR400	2.5-3-3-8 CR2	306 MB/s
Celeron 420	1600 MHz	Intel DQ965GF	Q965 Int.	Dual DDR2-667	5-5-5-15	251 MB/s
Celeron D 326	2533 MHz	ASRock 775Twins-HDTV	RC410 Ext.	DDR2-533 SDRAM	4-4-4-11	246 MB/s
Sempron 2600+	1600 MHz	ASRock K8NF4G-SATA2	GeForce6100 Int.	DDR400 SDRAM	2.5-3-3-8 CR2	245 MB/s
Atom 230 HT	1600 MHz	Intel D945GCLF	i945GC Int.	DDR2-533 SDRAM	4-4-4-12	162 MB/s

FPU VP8

CPU	CPU Clock	Motherboard	Chipset	Memory	CL-RCD-RP-RAS	Score
6x Core i7-4930K HT	3400 MHz	Gigabyte GA-X79-UD3	X79	Quad DDR3-1866	9-10-9-27 CR2	6751
6x Core i7-5820K HT	3300 MHz	Gigabyte GA-X99-UD4	X99	Quad DDR4-2133	15-15-15-36 CR2	6539
4x Core i7-4770 HT	3400 MHz	Intel DZ87KLT-75K	Z87 Int.	Dual DDR3-1600	9-9-9-27 CR2	6391
6x Core i7-3960X Extreme HT	3300 MHz	Intel DX79SI	X79	Quad DDR3-1600	9-9-9-24 CR2	6381
4x Xeon E3-1245 v3 HT	3400 MHz	Supermicro X10SAE	C226 Int.	Dual DDR3-1600	11-11-11-28 CR1	6367
16x Xeon E5-2670 HT	2600 MHz	Supermicro X9DR6-F	C600	Quad DDR3-1333	9-9-9-24	6350
4x Core i7-3770K HT	3500 MHz	MSI Z77A-GD55	Z77 Int.	Dual DDR3-1600	9-9-9-24 CR2	6307
6x Core i7-990X Extreme HT	3466 MHz	Intel DX58SO2	X58	Triple DDR3-1333	9-9-9-24 CR1	5592
4x Core i7-2600 HT	3400 MHz	Asus P8P67	P67	Dual DDR3-1333	9-9-9-24 CR1	5279
8x Xeon E5462	2800 MHz	Intel S5400SF	i5400	Quad DDR2-640FB	5-5-5-15	4981
8x FX-8350	4000 MHz	Asus M5A99X Evo R2.0	AMD990X	Dual DDR3-1866	9-10-9-27 CR2	4943

4x Core i7-965 Extreme HT	3200 MHz	Asus P6T Deluxe	X58	Triple DDR3-1333	9-9-9-24 CR1	4777
8x Xeon X5550 HT	2666 MHz	Supermicro X8DTN+	i5520	Triple DDR3-1333	9-9-9-24 CR1	4589
6x Phenom II X6 Black 1100T	3300 MHz	Gigabyte GA-890GPA-UD3H v2	AMD890GX Int.	Unganged Dual DDR3-1333	9-9-9-24 CR2	4583
8x FX-8150	3600 MHz	Asus M5A97	AMD970	Dual DDR3-1866	9-10-9-27 CR2	3973
12x Opteron 2431	2400 MHz	Supermicro H8DI3+-F	SR5690	Unganged Dual DDR2-800R	6-6-6-18 CR1	3920
4x Core 2 Extreme QX9650	3000 MHz	Gigabyte GA-EP35C-DS3R	P35	Dual DDR3-1066	8-8-8-20 CR2	3864
4x Xeon X3430	2400 MHz	Supermicro X8SIL-F	i3420	Dual DDR3-1333	9-9-9-24 CR1	3766
8x Opteron 2378	2400 MHz	Tyan Thunder n3600R	nForcePro-3600	Unganged Dual DDR2-800R	6-6-6-18 CR1	3654
4x A10-7850K	3700 MHz	Gigabyte GA-F2A88XM-D3H	A88X Int.	Dual DDR3-2133	9-11-10-31 CR2	3623
2x Core i7-3520M HT	**3400 MHz**	**Gateway EG50_HC_HR**	**HM70 Int.**	**Dual DDR3-1600**	**11-11-11-28 CR1**	**3515**
2x Core i5-650 HT	3200 MHz	Supermicro C7SIM-Q	Q57 Int.	Dual DDR3-1333	9-9-9-24 CR1	3304
4x Phenom II X4 Black 940	3000 MHz	Asus M3N78-EM	GeForce8300 Int.	Ganged Dual DDR2-800	5-5-5-18 CR2	3294
4x A8-3850	2900 MHz	Gigabyte GA-A75M-UD2H	A75 Int.	Dual DDR3-1333	9-9-9-24 CR1	3238
4x A10-5800K	3800 MHz	Asus F2A55-M	A55 Int.	Dual DDR3-1866	9-10-9-27 CR2	3166
8x Atom C2750	2400 MHz	Supermicro A1SAi-2750F	Avoton	Dual DDR3-1600	11-11-11-28 CR1	3145
4x A10-6800K	4100 MHz	Gigabyte GA-F2A85X-UP4	A85X Int.	Dual DDR3-2133	9-11-10-27 CR2	3141
32x Opteron 6274	2200 MHz	Supermicro H8DGI-F	SR5690	Dual DDR3-1600R	11-11-11-28 CR1	3070
4x Core 2 Extreme QX6700	2666 MHz	Intel D975XBX2	i975X	Dual DDR2-667	5-5-5-15	2707
8x Xeon L5320	1866 MHz	Intel S5000VCL	i5000V	Dual DDR2-533FB	4-4-4-12	2499
8x Opteron 2344 HE	1700 MHz	Supermicro H8DME-2	nForcePro-3600	Unganged Dual DDR2-667R	5-5-5-15 CR1	2448
4x Athlon 5350	2050 MHz	ASRock AM1B-ITX	Yangtze Int.	DDR3-1600 SDRAM	11-11-11-28 CR2	2402
4x Phenom X4 9500	2200 MHz	Asus M3A	AMD770	Ganged Dual DDR2-800	5-5-5-18 CR2	2382
4x Xeon 5140	2333 MHz	Intel S5000VSA	i5000V	Dual DDR2-667FB	5-5-5-15	2369
Celeron J1900	2000 MHz	Gigabyte GA-J1900N-D3V	BayTrailD Int.	Dual DDR3-1333	9-9-9-24 CR1	2112
2x Athlon64 X2 Black 6400+	3200 MHz	MSI K9N SLI Platinum	nForce570SLI	Dual DDR2-800	4-4-4-11 CR1	1816
2x Core 2 Extreme X6800	2933 MHz	Abit AB9	P965	Dual DDR2-800	5-5-5-18 CR2	1786
2x Core 2 Duo P8400	2266 MHz	MSI MegaBook PR201	GM45 Int.	Dual DDR2-667	5-5-5-15	1779
4x Opteron 2210 HE	1800 MHz	Tyan Thunder h2000M	BCM5785	Dual DDR2-600R	5-5-5-15 CR1	1687
2x Athlon64 X2 4000+	2100 MHz	ASRock ALiveNF7G-HDready	nForce7050-630a Int.	Dual DDR2-700	5-5-5-18 CR2	1352
2x Pentium EE 955 HT	3466 MHz	Intel D955XBK	i955X	Dual DDR2-667	4-4-4-11	1215
2x Xeon HT	3400 MHz	Intel SE7320SP2	iE7320	Dual DDR333R	2.5-3-3-7	1189
Nano X2 L4350	1600 MHz	VIA EPIA-M900	VX900H Int.	DDR3-1066 SDRAM	7-7-7-20 CR2	1108
2x Pentium D 820	2800 MHz	Abit Fatal1ty F-I90HD	RS600 Int.	Dual DDR2-800	5-5-5-18 CR2	1057
P4EE HT	3733 MHz	Intel SE7230NH1LX	iE7230	Dual DDR2-667	5-5-5-15	954
2x E-350	1600 MHz	ASRock E350M1	A50M Int.	DDR3-1066 SDRAM	8-8-8-20 CR1	850
Athlon64 3200+	2000 MHz	ASRock 939S56-M	SiS756	Dual DDR400	2.5-3-3-8 CR2	803
2x Atom D2500	1866 MHz	Intel D2500CC	NM10 Int.	DDR3-1066 SDRAM	7-7-7-20 CR2	796
2x Opteron 240	1400 MHz	MSI K8D Master3-133 FS	AMD8100	Dual DDR400R	3-4-4-8 CR1	689
Celeron 420	1600 MHz	Intel DQ965GF	Q965 Int.	Dual DDR2-667	5-5-5-15	685
Sempron 2600+	1600 MHz	ASRock K8NF4G-SATA2	GeForce6100 Int.	DDR400 SDRAM	2.5-3-3-8 CR2	661
Opteron 248	2200 MHz	MSI K8T Master1-FAR	K8T800	Dual DDR266R	2-3-3-6 CR1	613
Celeron D 326	2533 MHz	ASRock 775Twins-HDTV	RC410 Ext.	DDR2-533 SDRAM	4-4-4-11	586
Atom 230 HT	1600 MHz	Intel D945GCLF	i945GC Int.	DDR2-533 SDRAM	4-4-4-12	511
Nano L2200	1600 MHz	VIA VB8001	CN896 Int.	DDR2-667 SDRAM	5-5-5-15 CR2	487

FPU Julia

CPU	CPU Clock	Motherboard	Chipset	Memory	CL-RCD-RP-RAS	Score
16x Xeon E5-2670 HT	2600 MHz	Supermicro X9DR6-F	C600	Quad DDR3-1333	9-9-9-24	62590
6x Core i7-5820K HT	3300 MHz	Gigabyte GA-X99-UD4	X99	Quad DDR4-2133	15-15-15-36 CR2	40502
32x Opteron 6274	2200 MHz	Supermicro H8DGI-F	SR5690	Dual DDR3-1600R	11-11-11-28 CR1	30193
6x Core i7-4930K HT	3400 MHz	Gigabyte GA-X79-UD3	X79	Quad DDR3-1866	9-10-9-27 CR2	28480

4x Core i7-4770 HT	3400 MHz	Intel DZ87KLT-75K	Z87 Int.	Dual DDR3-1600	9-9-9-27 CR2	26953
4x Xeon E3-1245 v3 HT	3400 MHz	Supermicro X10SAE	C226 Int.	Dual DDR3-1600	11-11-11-28 CR1	26917
6x Core i7-3960X Extreme HT	3300 MHz	Intel DX79SI	X79	Quad DDR3-1600	9-9-9-24 CR2	26898
4x Core i7-3770K HT	3500 MHz	MSI Z77A-GD55	Z77 Int.	Dual DDR3-1600	9-9-9-24 CR2	19516
4x Core i7-2600 HT	3400 MHz	Asus P8P67	P67	Dual DDR3-1333	9-9-9-24 CR1	18457
12x Opteron 2431	2400 MHz	Supermicro H8DI3+-F	SR5690	Unganged Dual DDR2-800R	6-6-6-18 CR1	18309
6x Core i7-990X Extreme HT	3466 MHz	Intel DX58SO2	X58	Triple DDR3-1333	9-9-9-24 CR1	17993
8x Xeon X5550 HT	2666 MHz	Supermicro X8DTN+	i5520	Triple DDR3-1333	9-9-9-24 CR1	17671
8x Xeon E5462	2800 MHz	Intel S5400SF	i5400	Quad DDR2-640FB	5-5-5-15	15300
8x FX-8350	4000 MHz	Asus M5A99X Evo R2.0	AMD990X	Dual DDR3-1866	9-10-9-27 CR2	13504
6x Phenom II X6 Black 1100T	3300 MHz	Gigabyte GA-890GPA-UD3H v2	AMD890GX Int.	Unganged Dual DDR3-1333	9-9-9-24 CR2	12634
8x Opteron 2378	2400 MHz	Tyan Thunder n3600R	nForcePro-3600	Unganged Dual DDR2-800R	6-6-6-18 CR1	12208
8x FX-8150	3600 MHz	Asus M5A97	AMD970	Dual DDR3-1866	9-10-9-27 CR2	11912
4x Core i7-965 Extreme HT	3200 MHz	Asus P6T Deluxe	X58	Triple DDR3-1333	9-9-9-24 CR1	11125
8x Xeon L5320	1866 MHz	Intel S5000VCL	i5000V	Dual DDR2-533FB	4-4-4-12	8956
2x Core i7-3520M HT	**3400 MHz**	**Gateway EG50_HC_HR**	**HM70 Int.**	**Dual DDR3-1600**	**11-11-11-28 CR1**	**8929**
8x Atom C2750	2400 MHz	Supermicro A1SAi-2750F	Avoton	Dual DDR3-1600	11-11-11-28 CR1	8747
8x Opteron 2344 HE	1700 MHz	Supermicro H8DME-2	nForcePro-3600	Unganged Dual DDR2-667R	5-5-5-15 CR1	8681
4x Core 2 Extreme QX9650	3000 MHz	Gigabyte GA-EP35C-DS3R	P35	Dual DDR3-1066	8-8-8-20 CR2	8201
4x Xeon X3430	2400 MHz	Supermicro X8SIL-F	i3420	Dual DDR3-1333	9-9-9-24 CR1	8070
4x Phenom II X4 Black 940	3000 MHz	Asus M3N78-EM	GeForce8300 Int.	Ganged Dual DDR2-800	5-5-5-18 CR2	7608
4x A8-3850	2900 MHz	Gigabyte GA-A75M-UD2H	A75 Int.	Dual DDR3-1333	9-9-9-24 CR1	7438
4x A10-6800K	4100 MHz	Gigabyte GA-F2A85X-UP4	A85X Int.	Dual DDR3-2133	9-11-10-27 CR2	6999
4x A10-5800K	3800 MHz	Asus F2A55-M	A55 Int.	Dual DDR3-1866	9-10-9-27 CR2	6474
4x Core 2 Extreme QX6700	2666 MHz	Intel D975XBX2	i975X	Dual DDR2-667	5-5-5-15	6411
4x A10-7850K	3700 MHz	Gigabyte GA-F2A88XM-D3H	A88X Int.	Dual DDR3-2133	9-11-10-31 CR2	6207
4x Xeon 5140	2333 MHz	Intel S5000VSA	i5000V	Dual DDR2-667FB	5-5-5-15	5587
4x Phenom X4 9500	2200 MHz	Asus M3A	AMD770	Ganged Dual DDR2-800	5-5-5-18 CR2	5579
2x Core i5-650 HT	3200 MHz	Supermicro C7SIM-Q	Q57 Int.	Dual DDR3-1333	9-9-9-24 CR1	5551
4x Athlon 5350	2050 MHz	ASRock AM1B-ITX	Yangtze Int.	DDR3-1600 SDRAM	11-11-11-28 CR2	5235
Celeron J1900	2000 MHz	Gigabyte GA-J1900N-D3V	BayTrailD Int.	Dual DDR3-1333	9-9-9-24 CR1	4059
2x Core 2 Extreme X6800	2933 MHz	Abit AB9	P965	Dual DDR2-800	5-5-5-18 CR2	3534
2x Core 2 Duo P8400	2266 MHz	MSI MegaBook PR201	GM45 Int.	Dual DDR2-667	5-5-5-15	3079
2x Pentium EE 955 HT	3466 MHz	Intel D955XBK	i955X	Dual DDR2-667	4-4-4-11	2440
2x Xeon HT	3400 MHz	Intel SE7320SP2	iE7320	Dual DDR333R	2.5-3-3-7	2393
4x Opteron 2210 HE	1800 MHz	Tyan Thunder h2000M	BCM5785	Dual DDR2-600R	5-5-5-15 CR1	2309
2x Athlon64 X2 Black 6400+	3200 MHz	MSI K9N SLI Platinum	nForce570SLI	Dual DDR2-800	4-4-4-11 CR1	2053
2x Pentium D 820	2800 MHz	Abit Fatal1ty F-I90HD	RS600 Int.	Dual DDR2-800	5-5-5-18 CR2	1988
Nano X2 L4350	1600 MHz	VIA EPIA-M900	VX900H Int.	DDR3-1066 SDRAM	7-7-7-20 CR2	1865
2x Athlon64 X2 4000+	2100 MHz	ASRock ALiveNF7G-HDready	nForce7050-630a Int.	Dual DDR2-700	5-5-5-18 CR2	1342
P4EE HT	3733 MHz	Intel SE7230NH1LX	iE7230	Dual DDR2-667	5-5-5-15	1308
2x Atom D2500	1866 MHz	Intel D2500CC	NM10 Int.	DDR3-1066 SDRAM	7-7-7-20 CR2	1117
Celeron 420	1600 MHz	Intel DQ965GF	Q965 Int.	Dual DDR2-667	5-5-5-15	958
2x E-350	1600 MHz	ASRock E350M1	A50M Int.	DDR3-1066 SDRAM	8-8-8-20 CR1	911
2x Opteron 240	1400 MHz	MSI K8D Master3-133 FS	AMD8100	Dual DDR400R	3-4-4-8 CR1	896
Celeron D 326	2533 MHz	ASRock 775Twins-HDTV	RC410 Ext.	DDR2-533 SDRAM	4-4-4-11	893
Nano L2200	1600 MHz	VIA VB8001	CN896 Int.	DDR2-667 SDRAM	5-5-5-15 CR2	792
Opteron 248	2200 MHz	MSI K8T Master1-FAR	K8T800	Dual DDR266R	2-3-3-6 CR1	702
Athlon64 3200+	2000 MHz	ASRock 939S56-M	SiS756	Dual DDR400	2.5-3-3-8 CR2	641
Atom 230 HT	1600 MHz	Intel D945GCLF	i945GC Int.	DDR2-533 SDRAM	4-4-4-12	589
Sempron 2600+	1600 MHz	ASRock K8NF4G-SATA2	GeForce6100 Int.	DDR400 SDRAM	2.5-3-3-8 CR2	513

FPU Mandel

CPU	CPU Clock	Motherboard	Chipset	Memory	CL-RCD-RP-RAS	Score
16x Xeon E5-2670 HT	2600 MHz	Supermicro X9DR6-F	C600	Quad DDR3-1333	9-9-9-24	33143
6x Core i7-5820K HT	3300 MHz	Gigabyte GA-X99-UD4	X99	Quad DDR4-2133	15-15-15-36 CR2	21649
32x Opteron 6274	2200 MHz	Supermicro H8DGI-F	SR5690	Dual DDR3-1600R	11-11-11-28 CR1	15402
6x Core i7-4930K HT	3400 MHz	Gigabyte GA-X79-UD3	X79	Quad DDR3-1866	9-10-9-27 CR2	15100
4x Core i7-4770 HT	3400 MHz	Intel DZ87KLT-75K	Z87 Int.	Dual DDR3-1600	9-9-9-27 CR2	14429
4x Xeon E3-1245 v3 HT	3400 MHz	Supermicro X10SAE	C226 Int.	Dual DDR3-1600	11-11-11-28 CR1	14418
6x Core i7-3960X Extreme HT	3300 MHz	Intel DX79SI	X79	Quad DDR3-1600	9-9-9-24 CR2	14253
4x Core i7-3770K HT	3500 MHz	MSI Z77A-GD55	Z77 Int.	Dual DDR3-1600	9-9-9-24 CR2	10344
4x Core i7-2600 HT	3400 MHz	Asus P8P67	P67	Dual DDR3-1333	9-9-9-24 CR1	9777
12x Opteron 2431	2400 MHz	Supermicro H8DI3+-F	SR5690	Unganged Dual DDR2-800R	6-6-6-18 CR1	9318
6x Core i7-990X Extreme HT	3466 MHz	Intel DX58SO2	X58	Triple DDR3-1333	9-9-9-24 CR1	8672
8x Xeon X5550 HT	2666 MHz	Supermicro X8DTN+	i5520	Triple DDR3-1333	9-9-9-24 CR1	8614
8x Xeon E5462	2800 MHz	Intel S5400SF	i5400	Quad DDR2-640FB	5-5-5-15	8066
8x FX-8350	4000 MHz	Asus M5A99X Evo R2.0	AMD990X	Dual DDR3-1866	9-10-9-27 CR2	6901
6x Phenom II X6 Black 1100T	3300 MHz	Gigabyte GA-890GPA-UD3H v2	AMD890GX Int.	Unganged Dual DDR3-1333	9-9-9-24 CR2	6434
8x Opteron 2378	2400 MHz	Tyan Thunder n3600R	nForcePro-3600	Unganged Dual DDR2-800R	6-6-6-18 CR1	6211
8x FX-8150	3600 MHz	Asus M5A97	AMD970	Dual DDR3-1866	9-10-9-27 CR2	6094
4x Core i7-965 Extreme HT	3200 MHz	Asus P6T Deluxe	X58	Triple DDR3-1333	9-9-9-24 CR1	5395
2x Core i7-3520M HT	**3400 MHz**	**Gateway EG50_HC_HR**	**HM70 Int.**	**Dual DDR3-1600**	**11-11-11-28 CR1**	**4729**
8x Xeon L5320	1866 MHz	Intel S5000VCL	i5000V	Dual DDR2-533FB	4-4-4-12	4626
8x Opteron 2344 HE	1700 MHz	Supermicro H8DME-2	nForcePro-3600	Unganged Dual DDR2-667R	5-5-5-15 CR1	4418
4x Core 2 Extreme QX9650	3000 MHz	Gigabyte GA-EP35C-DS3R	P35	Dual DDR3-1066	8-8-8-20 CR2	4333
4x Xeon X3430	2400 MHz	Supermicro X8SIL-F	i3420	Dual DDR3-1333	9-9-9-24 CR1	4179
4x A8-3850	2900 MHz	Gigabyte GA-A75M-UD2H	A75 Int.	Dual DDR3-1333	9-9-9-24 CR1	3973
4x Phenom II X4 Black 940	3000 MHz	Asus M3N78-EM	GeForce8300 Int.	Ganged Dual DDR2-800	5-5-5-18 CR2	3874
4x A10-6800K	4100 MHz	Gigabyte GA-F2A85X-UP4	A85X Int.	Dual DDR3-2133	9-11-10-27 CR2	3474
4x Core 2 Extreme QX6700	2666 MHz	Intel D975XBX2	i975X	Dual DDR2-667	5-5-5-15	3308
4x A10-5800K	3800 MHz	Asus F2A55-M	A55 Int.	Dual DDR3-1866	9-10-9-27 CR2	3228
4x A10-7850K	3700 MHz	Gigabyte GA-F2A88XM-D3H	A88X Int.	Dual DDR3-2133	9-11-10-31 CR2	3176
8x Atom C2750	2400 MHz	Supermicro A1SAi-2750F	Avoton	Dual DDR3-1600	11-11-11-28 CR1	2982
4x Xeon 5140	2333 MHz	Intel S5000VSA	i5000V	Dual DDR2-667FB	5-5-5-15	2889
4x Phenom X4 9500	2200 MHz	Asus M3A	AMD770	Ganged Dual DDR2-800	5-5-5-18 CR2	2840
2x Core i5-650 HT	3200 MHz	Supermicro C7SIM-Q	Q57 Int.	Dual DDR3-1333	9-9-9-24 CR1	2676
4x Athlon 5350	2050 MHz	ASRock AM1B-ITX	Yangtze Int.	DDR3-1600 SDRAM	11-11-11-28 CR2	2335
2x Core 2 Extreme X6800	2933 MHz	Abit AB9	P965	Dual DDR2-800	5-5-5-18 CR2	1823
2x Core 2 Duo P8400	2266 MHz	MSI MegaBook PR201	GM45 Int.	Dual DDR2-667	5-5-5-15	1626
2x Pentium EE 955 HT	3466 MHz	Intel D955XBK	i955X	Dual DDR2-667	4-4-4-11	1482
2x Xeon HT	3400 MHz	Intel SE7320SP2	iE7320	Dual DDR333R	2.5-3-3-7	1449
Celeron J1900	2000 MHz	Gigabyte GA-J1900N-D3V	BayTrailD Int.	Dual DDR3-1333	9-9-9-24 CR1	1383
4x Opteron 2210 HE	1800 MHz	Tyan Thunder h2000M	BCM5785	Dual DDR2-600R	5-5-5-15 CR1	1182
2x Pentium D 820	2800 MHz	Abit Fatal1ty F-I90HD	RS600 Int.	Dual DDR2-800	5-5-5-18 CR2	1062
2x Athlon64 X2 Black 6400+	3200 MHz	MSI K9N SLI Platinum	nForce570SLI	Dual DDR2-800	4-4-4-11 CR1	1051
Nano X2 L4350	1600 MHz	VIA EPIA-M900	VX900H Int.	DDR3-1066 SDRAM	7-7-7-20 CR2	856
P4EE HT	3733 MHz	Intel SE7230NH1LX	iE7230	Dual DDR2-667	5-5-5-15	795
2x Athlon64 X2 4000+	2100 MHz	ASRock ALiveNF7G-HDready	nForce7050-630a Int.	Dual DDR2-700	5-5-5-18 CR2	688
Celeron 420	1600 MHz	Intel DQ965GF	Q965 Int.	Dual DDR2-667	5-5-5-15	494
Celeron D 326	2533 MHz	ASRock 775Twins-HDTV	RC410 Ext.	DDR2-533 SDRAM	4-4-4-11	476
2x Opteron 240	1400 MHz	MSI K8D Master3-133 FS	AMD8100	Dual DDR400R	3-4-4-8 CR1	458
2x E-350	1600 MHz	ASRock E350M1	A50M Int.	DDR3-1066 SDRAM	8-8-8-20 CR1	427
Nano L2200	1600 MHz	VIA VB8001	CN896 Int.	DDR2-667 SDRAM	5-5-5-15 CR2	404
2x Atom D2500	1866 MHz	Intel D2500CC	NM10 Int.	DDR3-1066 SDRAM	7-7-7-20 CR2	402

Opteron 248	2200 MHz	MSI K8T Master1-FAR	K8T800	Dual DDR266R	2-3-3-6 CR1	359
Athlon64 3200+	2000 MHz	ASRock 939S56-M	SiS756	Dual DDR400	2.5-3-3-8 CR2	328
Sempron 2600+	1600 MHz	ASRock K8NF4G-SATA2	GeForce6100 Int.	DDR400 SDRAM	2.5-3-3-8 CR2	263
Atom 230 HT	1600 MHz	Intel D945GCLF	i945GC Int.	DDR2-533 SDRAM	4-4-4-12	193

FPU SinJulia

CPU	CPU Clock	Motherboard	Chipset	Memory	CL-RCD-RP-RAS	Score
16x Xeon E5-2670 HT	2600 MHz	Supermicro X9DR6-F	C600	Quad DDR3-1333	9-9-9-24	16035
6x Core i7-990X Extreme HT	3466 MHz	Intel DX58SO2	X58	Triple DDR3-1333	9-9-9-24 CR1	7471
6x Core i7-4930K HT	3400 MHz	Gigabyte GA-X79-UD3	X79	Quad DDR3-1866	9-10-9-27 CR2	7274
6x Core i7-3960X Extreme HT	3300 MHz	Intel DX79SI	X79	Quad DDR3-1600	9-9-9-24 CR2	7214
8x Xeon X5550 HT	2666 MHz	Supermicro X8DTN+	i5520	Triple DDR3-1333	9-9-9-24 CR1	6993
32x Opteron 6274	2200 MHz	Supermicro H8DGI-F	SR5690	Dual DDR3-1600R	11-11-11-28 CR1	6822
6x Core i7-5820K HT	3300 MHz	Gigabyte GA-X99-UD4	X99	Quad DDR4-2133	15-15-15-36 CR2	6513
4x Core i7-3770K HT	3500 MHz	MSI Z77A-GD55	Z77 Int.	Dual DDR3-1600	9-9-9-24 CR2	4984
4x Core i7-4770 HT	3400 MHz	Intel DZ87KLT-75K	Z87 Int.	Dual DDR3-1600	9-9-9-27 CR2	4716
4x Core i7-2600 HT	3400 MHz	Asus P8P67	P67	Dual DDR3-1333	9-9-9-24 CR1	4679
12x Opteron 2431	2400 MHz	Supermicro H8DI3+-F	SR5690	Unganged Dual DDR2-800R	6-6-6-18 CR1	4658
4x Core i7-965 Extreme HT	3200 MHz	Asus P6T Deluxe	X58	Triple DDR3-1333	9-9-9-24 CR1	4587
4x Xeon E3-1245 v3 HT	3400 MHz	Supermicro X10SAE	C226 Int.	Dual DDR3-1600	11-11-11-28 CR1	4583
8x Xeon E5462	2800 MHz	Intel S5400SF	i5400	Quad DDR2-640FB	5-5-5-15	4132
6x Phenom II X6 Black 1100T	3300 MHz	Gigabyte GA-890GPA-UD3H v2	AMD890GX Int.	Unganged Dual DDR3-1333	9-9-9-24 CR2	3213
8x Opteron 2378	2400 MHz	Tyan Thunder n3600R	nForcePro-3600	Unganged Dual DDR2-800R	6-6-6-18 CR1	3101
8x FX-8350	4000 MHz	Asus M5A99X Evo R2.0	AMD990X	Dual DDR3-1866	9-10-9-27 CR2	2833
8x FX-8150	3600 MHz	Asus M5A97	AMD970	Dual DDR3-1866	9-10-9-27 CR2	2645
8x Xeon L5320	1866 MHz	Intel S5000VCL	i5000V	Dual DDR2-533FB	4-4-4-12	2590
2x Core i5-650 HT	3200 MHz	Supermicro C7SIM-Q	Q57 Int.	Dual DDR3-1333	9-9-9-24 CR1	2306
2x Core i7-3520M HT	**3400 MHz**	**Gateway EG50_HC_HR**	**HM70 Int.**	**Dual DDR3-1600**	**11-11-11-28 CR1**	**2271**
4x Xeon X3430	2400 MHz	Supermicro X8SIL-F	i3420	Dual DDR3-1333	9-9-9-24 CR1	2268
4x Core 2 Extreme QX9650	3000 MHz	Gigabyte GA-EP35C-DS3R	P35	Dual DDR3-1066	8-8-8-20 CR2	2219
8x Opteron 2344 HE	1700 MHz	Supermicro H8DME-2	nForcePro-3600	Unganged Dual DDR2-667R	5-5-5-15 CR1	2210
8x Atom C2750	2400 MHz	Supermicro A1SAi-2750F	Avoton	Dual DDR3-1600	11-11-11-28 CR1	2042
4x Phenom II X4 Black 940	3000 MHz	Asus M3N78-EM	GeForce8300 Int.	Ganged Dual DDR2-800	5-5-5-18 CR2	1934
4x A8-3850	2900 MHz	Gigabyte GA-A75M-UD2H	A75 Int.	Dual DDR3-1333	9-9-9-24 CR1	1872
4x Core 2 Extreme QX6700	2666 MHz	Intel D975XBX2	i975X	Dual DDR2-667	5-5-5-15	1856
4x Xeon 5140	2333 MHz	Intel S5000VSA	i5000V	Dual DDR2-667FB	5-5-5-15	1618
4x A10-7850K	3700 MHz	Gigabyte GA-F2A88XM-D3H	A88X Int.	Dual DDR3-2133	9-11-10-31 CR2	1481
4x A10-6800K	4100 MHz	Gigabyte GA-F2A85X-UP4	A85X Int.	Dual DDR3-2133	9-11-10-27 CR2	1480
4x Phenom X4 9500	2200 MHz	Asus M3A	AMD770	Ganged Dual DDR2-800	5-5-5-18 CR2	1421
4x A10-5800K	3800 MHz	Asus F2A55-M	A55 Int.	Dual DDR3-1866	9-10-9-27 CR2	1377
4x Athlon 5350	2050 MHz	ASRock AM1B-ITX	Yangtze Int.	DDR3-1600 SDRAM	11-11-11-28 CR2	1260
4x Opteron 2210 HE	1800 MHz	Tyan Thunder h2000M	BCM5785	Dual DDR2-600R	5-5-5-15 CR1	1178
2x Athlon64 X2 Black 6400+	3200 MHz	MSI K9N SLI Platinum	nForce570SLI	Dual DDR2-800	4-4-4-11 CR1	1049
2x Core 2 Extreme X6800	2933 MHz	Abit AB9	P965	Dual DDR2-800	5-5-5-18 CR2	1021
2x Pentium EE 955 HT	3466 MHz	Intel D955XBK	i955X	Dual DDR2-667	4-4-4-11	960
Celeron J1900	2000 MHz	Gigabyte GA-J1900N-D3V	BayTrailD Int.	Dual DDR3-1333	9-9-9-24 CR1	948
2x Xeon HT	3400 MHz	Intel SE7320SP2	iE7320	Dual DDR333R	2.5-3-3-7	942
2x Core 2 Duo P8400	2266 MHz	MSI MegaBook PR201	GM45 Int.	Dual DDR2-667	5-5-5-15	835
2x Athlon64 X2 4000+	2100 MHz	ASRock ALiveNF7G-HDready	nForce7050-630a Int.	Dual DDR2-700	5-5-5-18 CR2	685
P4EE HT	3733 MHz	Intel SE7230NH1LX	iE7230	Dual DDR2-667	5-5-5-15	516
2x E-350	1600 MHz	ASRock E350M1	A50M Int.	DDR3-1066 SDRAM	8-8-8-20 CR1	505

2x Opteron 240	1400 MHz	MSI K8D Master3-133 FS	AMD8100	Dual DDR400R	3-4-4-8 CR1	457
2x Pentium D 820	2800 MHz	Abit Fatal1ty F-I90HD	RS600 Int.	Dual DDR2-800	5-5-5-18 CR2	452
Opteron 248	2200 MHz	MSI K8T Master1-FAR	K8T800	Dual DDR266R	2-3-3-6 CR1	359
Athlon64 3200+	2000 MHz	ASRock 939S56-M	SiS756	Dual DDR400	2.5-3-3-8 CR2	327
Nano X2 L4350	1600 MHz	VIA EPIA-M900	VX900H Int.	DDR3-1066 SDRAM	7-7-7-20 CR2	284
Celeron 420	1600 MHz	Intel DQ965GF	Q965 Int.	Dual DDR2-667	5-5-5-15	277
2x Atom D2500	1866 MHz	Intel D2500CC	NM10 Int.	DDR3-1066 SDRAM	7-7-7-20 CR2	262
Sempron 2600+	1600 MHz	ASRock K8NF4G-SATA2	GeForce6100 Int.	DDR400 SDRAM	2.5-3-3-8 CR2	262
Atom 230 HT	1600 MHz	Intel D945GCLF	i945GC Int.	DDR2-533 SDRAM	4-4-4-12	205
Celeron D 326	2533 MHz	ASRock 775Twins-HDTV	RC410 Ext.	DDR2-533 SDRAM	4-4-4-11	203
Nano L2200	1600 MHz	VIA VB8001	CN896 Int.	DDR2-667 SDRAM	5-5-5-15 CR2	131

Debug - PCI

B00 D00 F00: Intel Ivy Bridge-MB - Host Bridge/DRAM Controller

```
Offset 000:  86 80 54 01 06 00 90 20 09 00 00 06 00 00 00 00
Offset 010:  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
Offset 020:  00 00 00 00 00 00 00 00 00 00 00 00 25 10 49 06
Offset 030:  00 00 00 00 E0 00 00 00 00 00 00 00 00 00 00 00
Offset 040:  01 90 D1 FE 00 00 00 00 01 00 D1 FE 00 00 00 00
Offset 050:  11 02 00 00 11 00 00 00 07 00 90 AF 01 00 00 AB
Offset 060:  05 00 00 F0 00 00 00 00 01 80 D1 FE 00 00 00 00
Offset 070:  00 00 00 FF 03 00 00 00 00 0C 00 FF 7F 00 00 00
Offset 080:  10 11 11 11 11 33 33 00 1A 00 00 00 00 00 00 00
Offset 090:  01 00 00 FF 03 00 00 00 01 00 50 4F 04 00 00 00
Offset 0A0:  01 00 00 00 04 00 00 00 01 00 60 4F 04 00 00 00
Offset 0B0:  01 00 A0 AB 01 00 80 AB 01 00 00 AB 01 00 A0 AF
Offset 0C0:  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
Offset 0D0:  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 FF
Offset 0E0:  09 00 0C 01 9B 61 00 E2 D0 00 E0 76 00 00 00 00
Offset 0F0:  00 00 00 01 00 00 00 00 C8 0F 09 00 00 00 00 00
```

B00 D02 F00: Intel Ivy Bridge-MB - Integrated Graphics Controller (MB GT2)

```
Offset 000:  86 80 66 01 07 04 90 00 09 00 00 03 00 00 00 00
Offset 010:  04 00 00 C0 00 00 00 00 0C 00 00 B0 00 00 00 00
Offset 020:  01 20 00 00 00 00 00 00 00 00 00 00 25 10 49 06
Offset 030:  00 00 00 00 90 00 00 00 00 00 00 00 00 01 00 00
Offset 040:  09 00 0C 01 9B 61 00 E2 D0 00 E0 76 00 00 00 00
Offset 050:  11 02 00 00 11 00 00 00 00 00 00 00 01 00 A0 AB
Offset 060:  00 00 02 00 00 00 00 00 00 00 00 00 00 00 00 00
Offset 070:  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
Offset 080:  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
Offset 090:  05 D0 01 00 D8 01 E0 FE 00 00 00 00 00 00 00 00
Offset 0A0:  00 00 00 00 13 00 06 03 00 00 00 00 00 00 00 00
Offset 0B0:  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
Offset 0C0:  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
Offset 0D0:  01 A4 22 00 00 00 00 00 00 00 00 00 00 00 00 00
Offset 0E0:  00 00 00 00 00 00 00 00 00 80 00 00 00 00 00 00
Offset 0F0:  00 00 00 00 00 00 00 00 00 00 09 00 18 20 FB AA
```

B00 D1A F00: Intel Panther Point PCH - USB 2.0 EHCI Controller #2 [C-1]

Offset 000: 86 80 2D 1E 06 00 90 02 04 20 03 0C 00 00 00 00
Offset 010: 00 80 60 C0 00 00 00 00 00 00 00 00 00 00 00 00
Offset 020: 00 00 00 00 00 00 00 00 00 00 00 00 25 10 49 06
Offset 030: 00 00 00 00 50 00 00 00 00 00 00 00 10 01 00 00
Offset 040: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
Offset 050: 01 58 C2 C9 00 00 00 00 0A 98 A0 20 00 00 00 00
Offset 060: 20 20 81 07 00 00 00 00 01 00 00 01 00 20 00 00
Offset 070: 00 00 DF 3F 00 00 00 00 00 00 00 00 00 00 00 00
Offset 080: 00 00 80 00 11 88 0C 93 30 0D 00 24 00 00 00 00
Offset 090: 00 00 00 00 00 00 00 00 13 00 06 03 00 00 00 00
Offset 0A0: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
Offset 0B0: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
Offset 0C0: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
Offset 0D0: 00 00 00 00 00 AA FF 00 00 00 00 00 00 00 00 00
Offset 0E0: 00 00 00 00 00 00 00 00 00 00 00 00 04 40 A4 AA
Offset 0F0: 00 00 00 00 88 85 80 00 87 0F 04 08 08 17 5B 20

B00 D1B F00: Intel Panther Point PCH - High Definition Audio Controller [C-1]

Offset 000: 86 80 20 1E 06 00 10 00 04 00 03 04 10 00 00 00
Offset 010: 04 00 60 C0 00 00 00 00 00 00 00 00 00 00 00 00
Offset 020: 00 00 00 00 00 00 00 00 00 00 00 00 25 10 49 06
Offset 030: 00 00 00 00 50 00 00 00 00 00 00 00 16 01 00 00
Offset 040: 01 00 00 45 00 00 00 00 00 00 00 00 00 00 00 00
Offset 050: 01 60 42 C8 00 00 00 00 00 00 00 00 00 00 00 00
Offset 060: 05 70 80 00 00 00 00 00 00 00 00 00 00 00 00 00
Offset 070: 10 00 91 00 00 00 00 10 00 08 10 00 00 00 00 00
Offset 080: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
Offset 090: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
Offset 0A0: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
Offset 0B0: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
Offset 0C0: 00 04 02 01 02 24 00 40 00 0C A3 82 10 00 33 02
Offset 0D0: 00 0C A3 02 10 00 33 02 00 00 00 00 00 00 00 00
Offset 0E0: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
Offset 0F0: 00 00 00 00 00 00 00 00 87 0F 04 08 00 00 00 00

B00 D1C F00: Intel Panther Point PCH - PCI Express Port 1

Offset 000: 86 80 10 1E 06 00 10 00 C4 00 04 06 10 00 81 00
Offset 010: 00 00 00 00 00 00 00 00 02 02 00 F0 00 00 20
Offset 020: F0 FF 00 00 41 C0 41 C0 00 00 00 00 00 00 00 00
Offset 030: 00 00 00 00 40 00 00 00 00 00 00 00 11 01 00 00
Offset 040: 10 80 42 01 00 80 00 00 00 00 10 00 12 3C 12 01
Offset 050: 42 00 11 70 00 B2 04 00 00 00 40 01 00 00 00 00
Offset 060: 00 00 00 00 16 00 00 00 00 00 00 00 00 00 00 00
Offset 070: 02 00 01 00 00 00 00 00 00 00 00 00 00 00 00 00
Offset 080: 05 90 00 00 00 00 00 00 00 00 00 00 00 00 00 00
Offset 090: 0D A0 00 00 25 10 49 06 00 00 00 00 00 00 00 00
Offset 0A0: 01 00 02 C8 00 00 00 00 00 00 00 00 00 00 00 00
Offset 0B0: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
Offset 0C0: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
Offset 0D0: 00 00 00 01 02 0B 00 00 00 80 11 81 00 00 00 00

Offset 0E0: 00 3F 00 00 00 00 00 00 01 00 00 00 00 00 00 00
Offset 0F0: 00 00 00 00 00 00 00 00 87 0F 04 08 00 00 00 00

B00 D1C F01: Intel Panther Point PCH - PCI Express Port 2

Offset 000: 86 80 12 1E 06 00 10 00 C4 00 04 06 10 00 81 00
Offset 010: 00 00 00 00 00 00 00 00 00 03 03 00 F0 00 00 00
Offset 020: 50 C0 50 C0 F1 FF 01 00 00 00 00 00 00 00 00 00
Offset 030: 00 00 00 00 40 00 00 00 00 00 00 00 10 02 00 00
Offset 040: 10 80 42 01 00 80 00 00 00 00 10 00 12 3C 12 02
Offset 050: 42 00 11 70 00 B2 0C 00 00 00 40 01 00 00 00 00
Offset 060: 00 00 00 00 16 00 00 00 00 00 00 00 00 00 00 00
Offset 070: 02 00 01 00 00 00 00 00 00 00 00 00 00 00 00 00
Offset 080: 05 90 00 00 00 00 00 00 00 00 00 00 00 00 00 00
Offset 090: 0D A0 00 00 25 10 49 06 00 00 00 00 00 00 00 00
Offset 0A0: 01 00 02 C8 00 00 00 00 00 00 00 00 00 00 00 00
Offset 0B0: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
Offset 0C0: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
Offset 0D0: 00 00 00 01 02 0B 00 00 00 80 11 01 00 00 00 00
Offset 0E0: 00 03 00 00 00 00 00 00 01 00 00 00 00 00 00 00
Offset 0F0: 00 00 00 00 00 00 00 00 87 0F 04 08 00 00 00 00

B00 D1D F00: Intel Panther Point PCH - USB 2.0 EHCI Controller #1 [C-1]

Offset 000: 86 80 26 1E 06 00 90 02 04 20 03 0C 00 00 00 00
Offset 010: 00 70 60 C0 00 00 00 00 00 00 00 00 00 00 00 00
Offset 020: 00 00 00 00 00 00 00 00 00 00 00 00 25 10 49 06
Offset 030: 00 00 00 00 50 00 00 00 00 00 00 00 17 01 00 00
Offset 040: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
Offset 050: 01 58 C2 C9 00 00 00 00 0A 98 A0 20 00 00 00 00
Offset 060: 20 20 01 06 00 00 00 00 01 00 00 01 00 20 00 00
Offset 070: 00 00 DF 3F 00 00 00 00 00 00 00 00 00 00 00 00
Offset 080: 00 00 80 00 11 88 0C 93 30 0D 00 24 00 00 00 00
Offset 090: 00 00 00 00 00 00 00 00 13 00 06 03 00 01 00 00
Offset 0A0: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
Offset 0B0: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
Offset 0C0: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
Offset 0D0: 00 00 00 00 00 AA FF 00 00 00 00 00 00 00 00 00
Offset 0E0: 00 00 00 00 00 00 00 00 00 00 00 00 84 B0 90 A9
Offset 0F0: 00 00 00 00 88 85 80 00 87 0F 04 08 08 17 5B 20

B00 D1F F00: Intel HM70 Chipset - LPC Interface Controller [C-1]

Offset 000: 86 80 5E 1E 07 00 10 02 04 00 01 06 00 00 80 00
Offset 010: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
Offset 020: 00 00 00 00 00 00 00 00 00 00 00 00 25 10 49 06
Offset 030: 00 00 00 00 E0 00 00 00 00 00 00 00 00 00 00 00
Offset 040: 01 04 00 00 80 00 00 00 01 05 00 00 10 00 00 00
Offset 050: F8 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
Offset 060: 87 8B 80 8A D0 00 00 00 80 87 8A 8B F8 F0 00 00
Offset 070: 78 F0 78 F0 78 F0 78 F0 78 F0 78 F0 78 F0 78 F0
Offset 080: 10 00 03 3F 00 00 00 00 61 FD 04 00 69 00 04 00
Offset 090: 00 00 00 00 00 0F 00 00 01 00 00 FF 00 00 00 00
Offset 0A0: 14 0E A0 00 09 38 06 00 00 47 00 00 00 00 00 00

Offset 0B0: 00 00 00 00 00 00 00 00 00 80 01 80 00 00 00 00
Offset 0C0: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
Offset 0D0: 33 22 11 00 67 45 00 00 CE FF 00 00 00 00 00 00
Offset 0E0: 09 00 0C 10 00 00 00 00 1B 2E 64 06 00 00 00 00
Offset 0F0: 01 C0 D1 FE 00 00 00 00 87 0F 04 08 00 00 00 00

B00 D1F F02: Intel Panther Point-M PCH - SATA AHCI Controller [C-1]

Offset 000: 86 80 03 1E 07 00 B0 02 04 01 06 01 00 00 00 00
Offset 010: 89 20 00 00 95 20 00 00 81 20 00 00 91 20 00 00
Offset 020: 61 20 00 00 00 60 60 C0 00 00 00 00 25 10 49 06
Offset 030: 00 00 00 00 80 00 00 00 00 00 00 00 13 02 00 00
Offset 040: 00 80 00 80 00 00 00 00 00 00 00 00 00 00 00 00
Offset 050: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
Offset 060: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
Offset 070: 01 A8 03 40 08 00 00 00 00 00 00 00 00 00 00 00
Offset 080: 05 70 00 00 00 00 00 00 00 00 00 00 00 00 00 00
Offset 090: 60 3A 05 85 83 01 00 3A 08 42 5C 01 02 00 00 00
Offset 0A0: E0 00 00 00 39 00 00 00 12 B0 10 00 48 00 00 00
Offset 0B0: 13 00 06 03 00 00 00 00 00 00 00 00 00 00 00 00
Offset 0C0: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
Offset 0D0: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
Offset 0E0: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
Offset 0F0: 00 00 00 00 00 00 00 00 87 0F 04 08 00 00 00 00

B00 D1F F03: Intel Panther Point PCH - SMBus Controller [C-1]

Offset 000: 86 80 22 1E 03 00 80 02 04 00 05 0C 00 00 00 00
Offset 010: 04 40 60 C0 00 00 00 00 00 00 00 00 00 00 00 00
Offset 020: 41 20 00 00 00 00 00 00 00 00 00 00 25 10 49 06
Offset 030: 00 00 00 00 00 00 00 00 00 00 00 00 0A 03 00 00
Offset 040: 01 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
Offset 050: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
Offset 060: 03 04 04 00 00 00 08 08 00 00 00 00 00 00 00 00
Offset 070: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
Offset 080: 04 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
Offset 090: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
Offset 0A0: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
Offset 0B0: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
Offset 0C0: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
Offset 0D0: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
Offset 0E0: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
Offset 0F0: 00 00 00 00 00 00 00 00 87 0F 04 08 00 00 00 00

B00 D1F F06: Intel Panther Point PCH - Thermal Management Controller [C-1]

Offset 000: 86 80 24 1E 00 00 10 00 04 00 80 11 00 00 00 00
Offset 010: 04 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
Offset 020: 00 00 00 00 00 00 00 00 00 00 00 00 25 10 49 06
Offset 030: 00 00 00 00 50 00 00 00 00 00 00 00 07 01 00 00
Offset 040: 05 00 A0 AF 00 00 00 00 00 00 00 00 00 00 00 00
Offset 050: 01 00 23 00 08 00 00 00 00 00 00 00 00 00 00 00
Offset 060: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
Offset 070: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00

Offset 080: 05 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
Offset 090: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
Offset 0A0: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
Offset 0B0: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
Offset 0C0: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
Offset 0D0: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
Offset 0E0: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
Offset 0F0: 00 00 00 00 00 00 00 00 87 0F 04 08 00 00 00 00

B02 D00 F00: Broadcom NetLink BCM57785 PCI-E Gigabit Ethernet Controller

Offset 000: E4 14 B5 16 06 04 10 00 10 00 00 02 10 00 80 00
Offset 010: 0C 00 43 C0 00 00 00 00 0C 00 44 C0 00 00 00 00
Offset 020: 00 00 00 00 00 00 00 00 00 00 00 00 25 10 47 06
Offset 030: 00 00 00 00 48 00 00 00 00 00 00 00 00 01 00 00
Offset 040: 00 00 00 00 00 00 00 01 01 58 03 C8 08 20 00 08
Offset 050: 03 00 00 00 00 00 00 00 05 A0 86 00 00 00 00 00
Offset 060: 00 00 00 00 00 00 00 00 98 02 00 F1 D0 02 F8 01
Offset 070: 92 10 00 00 00 00 00 00 CC FC 03 00 F0 0D 00 00
Offset 080: 01 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
Offset 090: 00 00 00 00 00 00 00 00 00 00 00 00 C8 00 00 00
Offset 0A0: 11 AC 04 80 02 00 00 00 22 01 00 00 10 00 02 00
Offset 0B0: 80 8D 90 05 00 50 10 00 11 5C 07 00 42 01 11 10
Offset 0C0: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
Offset 0D0: 1F 00 00 00 00 00 00 00 00 00 00 00 01 00 00 00
Offset 0E0: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
Offset 0F0: 00 00 00 00 00 00 00 00 00 00 00 00 00 51 78 57

B02 D00 F01: Broadcom SD Card Reader

Offset 000: E4 14 BC 16 06 00 10 00 10 01 05 08 10 00 80 00
Offset 010: 0C 00 40 C0 00 00 00 00 00 00 00 00 00 00 00 00
Offset 020: 00 00 00 00 00 00 00 00 00 00 00 00 25 10 47 06
Offset 030: 00 00 00 00 48 00 00 00 00 00 00 00 11 02 00 00
Offset 040: 00 00 00 00 00 00 00 00 01 58 03 C8 08 20 00 00
Offset 050: 03 00 00 00 00 00 00 00 05 AC 80 00 00 00 00 00
Offset 060: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
Offset 070: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
Offset 080: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
Offset 090: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
Offset 0A0: 11 00 05 00 02 00 00 00 22 01 00 00 10 00 02 00
Offset 0B0: 80 8D 90 05 10 5C 19 00 11 CC 04 00 42 01 11 10
Offset 0C0: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
Offset 0D0: 1F 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
Offset 0E0: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
Offset 0F0: 00 00 00 00 00 00 00 00 00 00 00 00 00 51 78 57

B02 D00 F02: Broadcom Memory Stick Card Reader

Offset 000: E4 14 BE 16 06 00 10 00 10 00 80 08 10 00 80 00
Offset 010: 0C 00 41 C0 00 00 00 00 00 00 00 00 00 00 00 00
Offset 020: 00 00 00 00 00 00 00 00 00 00 00 00 25 10 47 06
Offset 030: 00 00 00 00 48 00 00 00 00 00 00 00 11 02 00 00
Offset 040: 00 00 00 00 00 00 00 00 01 58 03 C8 08 20 00 00

Offset 050: 03 00 00 00 00 00 00 00 05 AC 80 00 00 00 00 00
Offset 060: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
Offset 070: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
Offset 080: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
Offset 090: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
Offset 0A0: 11 00 05 00 02 00 00 00 22 01 00 00 10 00 02 00
Offset 0B0: 80 8D 90 05 10 5C 19 00 11 CC 04 00 42 01 11 10
Offset 0C0: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
Offset 0D0: 1F 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
Offset 0E0: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
Offset 0F0: 00 00 00 00 00 00 00 00 00 00 00 00 00 51 78 57

B02 D00 F03: Broadcom xD Card Reader

Offset 000: E4 14 BF 16 06 00 10 00 10 00 80 08 10 00 80 00
Offset 010: 0C 00 42 C0 00 00 00 00 00 00 00 00 00 00 00 00
Offset 020: 00 00 00 00 00 00 00 00 00 00 00 00 25 10 47 06
Offset 030: 00 00 00 00 48 00 00 00 00 00 00 00 0B 02 00 00
Offset 040: 00 00 00 00 00 00 00 00 01 58 03 C8 08 20 00 00
Offset 050: 03 00 00 00 00 00 00 00 05 AC 80 00 00 00 00 00
Offset 060: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
Offset 070: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
Offset 080: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
Offset 090: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
Offset 0A0: 11 00 05 00 02 00 00 00 22 01 00 00 10 00 02 00
Offset 0B0: 80 8D 90 05 10 5C 19 00 11 CC 04 00 42 01 11 10
Offset 0C0: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
Offset 0D0: 1F 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
Offset 0E0: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
Offset 0F0: 00 00 00 00 00 00 00 00 00 00 00 00 00 51 78 57

B03 D00 F00: Intel Dual Band Wireless-AC 7260 AC 2x2 HMC WiFi Adapter

Offset 000: 86 80 B1 08 06 04 10 00 BB 00 80 02 10 00 00 00
Offset 010: 04 00 50 C0 00 00 00 00 00 00 00 00 00 00 00 00
Offset 020: 00 00 00 00 00 00 00 00 00 00 00 00 86 80 70 40
Offset 030: 00 00 00 00 C8 00 00 00 00 00 00 00 00 01 00 00
Offset 040: 10 00 02 00 C0 8E 00 10 10 0C 10 00 11 EC 06 00
Offset 050: 42 01 11 10 00 00 00 00 00 00 00 00 00 00 00 00
Offset 060: 00 00 00 00 12 08 08 00 05 00 00 00 00 00 00 00
Offset 070: 01 00 01 00 00 00 00 00 00 00 00 00 00 00 00 00
Offset 080: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
Offset 090: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
Offset 0A0: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
Offset 0B0: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
Offset 0C0: 00 00 00 00 00 00 00 00 01 D0 23 C8 00 00 00 0D
Offset 0D0: 05 40 81 00 B8 01 E0 FE 00 00 00 00 00 00 00 00
Offset 0E0: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
Offset 0F0: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00

PCI-8086-0154: Intel SNB/IVB/HSW/CRW/BDW MCHBAR

Offset 4000: BB 8B 1C 00 65 64 18 0C 20 22 04 0A B4 58 00 00
Offset 4010: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 10 00

Offset 4020: 05 00 10 00 27 27 20 20 23 00 0E 00 00 00 00 00

PCI-8086-0154: Intel SNB/IVB/HSW/CRW/BDW MCHBAR

Offset 4280: 00 00 00 00 00 00 0C 00 00 00 00 00 44 00 00 00
Offset 4290: 80 40 00 00 FF 98 00 00 60 18 D0 6C 58 02 00 00
Offset 42A0: 03 10 00 00 00 82 F8 41 00 00 00 00 01 00 00 00

PCI-8086-0154: Intel SNB/IVB/HSW/CRW/BDW MCHBAR

Offset 4400: BB 8B 1C 00 65 64 18 0C 20 22 04 0A B4 58 00 00
Offset 4410: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 10 00
Offset 4420: 05 00 10 00 28 28 20 20 33 00 0E 00 00 00 00 00

PCI-8086-0154: Intel SNB/IVB/HSW/CRW/BDW MCHBAR

Offset 4680: 00 00 00 00 00 00 0C 00 00 00 00 00 44 00 00 00
Offset 4690: 80 40 00 00 FF 98 00 00 60 18 D0 6C 58 02 00 00
Offset 46A0: 03 10 00 00 00 82 F8 41 00 00 00 00 01 00 00 00

PCI-8086-0154: Intel SNB/IVB/HSW/CRW/BDW MCHBAR

Offset 4800: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
Offset 4810: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00

PCI-8086-0154: Intel SNB/IVB/HSW/CRW/BDW MCHBAR

Offset 4A80: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
Offset 4A90: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00

PCI-8086-0154: Intel SNB/IVB/HSW/CRW/BDW MCHBAR

Offset 5000: 24 00 00 00 20 00 62 00 20 00 62 00 00 00 60 00
Offset 5010: 00 00 00 00 00 00 40 20 00 00 00 00 00 00 00 00

PCI-8086-0154: Intel SNB/IVB/HSW/CRW/BDW MCHBAR

Offset 5880: E7 71 91 CA 00 00 00 00 D0 DA E4 00 00 00 00 00
Offset 5890: C5 D1 31 01 3D D5 36 01 00 00 00 00 00 00 00 00
Offset 58A0: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
Offset 58B0: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
Offset 58C0: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
Offset 58D0: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
Offset 58E0: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
Offset 58F0: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
Offset 5900: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
Offset 5910: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
Offset 5920: 00 00 00 00 08 00 00 00 DF ED DC 10 C4 3D 33 00
Offset 5930: 18 01 C0 00 00 00 00 00 03 10 0A 00 E8 80 14 15
Offset 5940: 1F F3 26 04 99 8D 06 00 00 07 00 00 00 00 00 00
Offset 5950: 00 00 00 00 00 00 10 00 00 1D 01 F0 00 0C 08 00
Offset 5960: F1 56 5F 0A 85 E4 B2 B5 D8 D8 B2 B5 5B C0 83 D4
Offset 5970: 06 BA AE 30 04 BA AE 30 4D 00 00 00 4D 00 00 00
Offset 5980: 41 00 00 00 74 EC 2F 34 00 00 00 00 00 00 00 00

```
Offset 5990:      FF 00 00 00 FF 00 00 00 19 0D 07 00 00 12 69 00
Offset 59A0:      00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
Offset 59B0:      80 03 00 80 94 14 14 18 90 01 00 80 94 14 14 18
Offset 59C0:      08 00 2B 88 00 00 00 00 00 00 00 00 00 00 00 00

PCI-8086-0154:  Intel SNB/IVB/HSW/CRW/BDW MCHBAR

Offset 5E00:      06 00 00 00 06 00 00 00 00 00 00 00 00 00 00 00
Offset 5E10:      00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00

PCI-8086-1E24:  Intel 5/6/7/8/9-series PCH TBARB

Offset 00:        01 BA 00 D6 2B 3A 00 00 03 00 03 00 00 00 40 00
Offset 10:        00 00 40 1A 87 DE 8C 80 00 00 00 00 00 00 00 00
Offset 20:        00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
Offset 30:        00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
Offset 40:        00 02 00 FF 00 00 00 00 00 00 00 00 00 00 00 00
Offset 50:        00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
Offset 60:        00 00 00 00 00 00 00 00 00 00 00 00 20 1B 16 05
Offset 70:        00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
Offset 80:        00 00 00 00 57 57 00 FF 00 00 00 00 00 00 00 00
Offset 90:        9F 90 4B 06 00 00 00 00 00 00 00 00 00 00 00 00
Offset A0:        00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
Offset B0:        00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
Offset C0:        00 00 00 00 00 00 00 FF 00 00 00 00 00 00 00 00
Offset D0:        00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
Offset E0:        00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
Offset F0:        00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
```

Debug - Video BIOS

```
C000:0000  U.x...000000000000.$..#a@...00IBM VGA Compatible BIOS. .n.~.....
C000:0040  PCIR..f.....................&.V.f.v.....n.....................
C000:0080  ..........7.............................................DH.....DH
C000:00C0  .....DH....0DH.....DI.....DI.....DJ.....DJ....0DJ.....DI....0DI.
C000:0100  ....DJ.....DK.....DK.....DK....0.L......L......L....0.L......M..
C000:0140  ....M.....0.D..2.h..4....8....:....<....A.D..C.h..E....I....K...
C000:0180  .M....P D..R h..T ...X ...Z ...\ ...`.T..a.T..b T..c.n..d.n..e n
C000:01C0  ..f....g....h ...i....j....k ...l....m....n ...o....p....q ...}.
C000:0200  ...~.... ........ .-..`.............. .1..l...........rQ.. n(U...
C000:0240  !........ ....`"............ ....@.......... .1X. (.........V. .1X
C000:0280  . .P........d..@A.&0..6.......... A. 0.`.........0*..Q.*@0p......
C000:02C0  ...4..Q.*@..........H?@0b.2@@.........h[..r.<P...................
C000:0300  ..E.............................................E.................
C000:0340  ....................For Evaluation Use Only....(........c-'(.+...
C000:0380  ................................................(........c-'(.+...
C000:03C0  ................................................P........c_OP.U...
```

Debug - Unknown

HDD	OCZ-AGILITY4
Optical	MATSHITA DVD-RAM UJ8C0
