

Speccy report for MIPAD2, [10/23/2016 3:03:28]

Summary

Operating System

Windows 10 Home 64-bit

CPU

Intel Atom x5 Z8500 @ 1.44GHz 58 °C

Cherry Trail 14nm Technology

RAM

2.00GB DDR3 @ 765MHz (12-15-20-34)

Motherboard

Xiaomi Inc Mipad (CHV) 38 °C

Graphics

LFP_Sharp (2048x1536@60Hz)

Intel HD Graphics (Unknown)

Storage

14GB Samsung AGND3R (SD)

14GB UFD 2.0 Silicon-Power16G USB Device (USB)

Optical Drives

No optical disk drives detected

Audio

Intel SST Audio Device (WDM)

Operating System

Windows 10 Home 64-bit

Computer type: Tablet

Installation Date: 10/23/2016 1:00:29 AM

Serial Number: Q8MMR-23RJY-JHR22-YKJP7-VT9QQ

Windows Security Center

User Account Control (UAC) Enabled

Notify level 2 - Default

Firewall Enabled

Windows Update

AutoUpdate Not configured

Windows Defender

Windows Defender Enabled

Antivirus

Antivirus Enabled

Display Name Windows Defender

Virus Signature Database Up to date

.NET Frameworks installed

v4.6 Full

v4.6 Client

Internet Explorer

Version 11.20.10586.0

PowerShell

Version 5.0.10586.0

Environment Variables

USERPROFILE C:\Users\Rawman

SystemRoot C:\Windows

User Variables

TEMP C:\Users\Rawman\AppData\Local\Temp

TMP C:\Users\Rawman\AppData\Local\Temp

Machine Variables

ComSpec C:\Windows\system32\cmd.exe

configsetroot C:\Windows\ConfigSetRoot

NUMBER_OF_PROCESSORS 4

RS

OS Windows_NT

Path C:\Windows\system32

C:\Windows

C:\Windows\System32\Wbem

C:\Windows\System32\WindowsPowerShell\v1.0\

PATHEXT .COM;.EXE;.BAT;.CMD;.VBS;.VBE;.JS;.JSE;.WSF;.WSH;.MSC

PROCESSOR_ARCHITECTURE AMD64

PROCESSOR_IDENTIFIER Intel64 Family 6 Model 76 Stepping 3, GenuineIntel

PROCESSOR_LEVEL 6

PROCESSOR_REVISION 4c03

PSModulePath %ProgramFiles%\WindowsPowerShell\Modules

C:\Windows\system32\WindowsPowerShell\v1.0\Modules

TEMP C:\Windows\TEMP

TMP C:\Windows\TEMP

USERNAME SYSTEM

windir C:\Windows

Battery

AC Line Offline

Battery Charge % 58 %

Battery State Unknown status

Remaining Battery Time 3 : 45

Power Profile

Active power scheme Balanced

Hibernation Enabled

Turn Off Monitor after: (On AC Power) 10 min

Turn Off Monitor after: (On Battery Power) 4 min

Turn Off Hard Disk after: (On AC Power) 30 sec

Turn Off Hard Disk after: (On Battery Power) 30 sec

Suspend after: (On AC Power) 10 min

Suspend after: (On Battery Power) 4 min

Screen saver Disabled

Uptime

Current Session

Current Time 10/23/2016 3:03:28 AM

Current Uptime 4,220 sec (0 d, 01 h, 10 m, 20 s)

Last Boot Time 10/23/2016 1:53:08 AM

Services

Runnin Application Information

g

Runnin Background Intelligent Transfer Service
g
Runnin Background Tasks Infrastructure Service
g
Runnin Base Filtering Engine
g
Runnin Bluetooth Handsfree Service
g
Runnin Bluetooth Support Service
g
Runnin CNG Key Isolation
g
Runnin COM+ Event System
g
Runnin Connected User Experiences and Telemetry
g
Runnin CoreMessaging
g
Runnin Credential Manager
g
Runnin Cryptographic Services
g
Runnin DCOM Server Process Launcher
g
Runnin Delivery Optimization
g
Runnin Device Association Service
g
Runnin DHCP Client
g
Runnin Diagnostic Policy Service
g
Runnin Diagnostic Service Host
g
Runnin Diagnostic System Host
g
Runnin Distributed Link Tracking Client
g
Runnin DNS Client
g
Runnin Geolocation Service
g
Runnin Group Policy Client
g
Runnin Human Interface Device Service
g
Runnin Intel Dynamic Platform & Thermal Framework Critical Service Application
g
Runnin Intel Dynamic Platform & Thermal Framework Low Power Mode Service
g Application

Runnin Intel Dynamic Platform & Thermal Framework Processor Participant Service
g Application
Runnin Intel HD Graphics Control Panel Service
g
Runnin IP Helper
g
Runnin Local Session Manager
g
Runnin Network Connection Broker
g
Runnin Network Connections
g
Runnin Network List Service
g
Runnin Network Location Awareness
g
Runnin Network Store Interface Service
g
Runnin Peer Name Resolution Protocol
g
Runnin Peer Networking Identity Manager
g
Runnin Plug and Play
g
Runnin Power
g
Runnin Print Spooler
g
Runnin Program Compatibility Assistant Service
g
Runnin Remote Procedure Call (RPC)
g
Runnin RPC Endpoint Mapper
g
Runnin RTK IIS Codec Service
g
Runnin Security Accounts Manager
g
Runnin Security Center
g
Runnin Sensor Service
g
Runnin Server
g
Runnin Shell Hardware Detection
g
Runnin SSDP Discovery
g
Runnin State Repository Service
g

Runnin Superfetch
g
Runnin System Event Notification Service
g
Runnin System Events Broker
g
Runnin Task Scheduler
g
Runnin TCP/IP NetBIOS Helper
g
Runnin Themes
g
Runnin Tile Data model server
g
Runnin Time Broker
g
Runnin Touch Keyboard and Handwriting Panel Service
g
Runnin User Manager
g
Runnin User Profile Service
g
Runnin Windows Audio
g
Runnin Windows Audio Endpoint Builder
g
Runnin Windows Backup
g
Runnin Windows Connection Manager
g
Runnin Windows Defender Network Inspection Service
g
Runnin Windows Defender Service
g
Runnin Windows Driver Foundation - User-mode Driver Framework
g
Runnin Windows Event Log
g
Runnin Windows Firewall
g
Runnin Windows Font Cache Service
g
Runnin Windows Installer
g
Runnin Windows License Manager Service
g
Runnin Windows Management Instrumentation
g
Runnin Windows Modules Installer
g

Runnin Windows Search
g
Runnin Windows Update
g
Runnin WinHTTP Web Proxy Auto-Discovery Service
g
Runnin WLAN AutoConfig
g
Runnin Workstation
g
Runnin WPS Office Cloud Service
g
Stoppe ActiveX Installer (AxInstSV)
d
Stoppe AllJoyn Router Service
d
Stoppe App Readiness
d
Stoppe Application Identity
d
Stoppe Application Layer Gateway Service
d
Stoppe AppX Deployment Service (AppXSVC)
d
Stoppe Auto Time Zone Updater
d
Stoppe BitLocker Drive Encryption Service
d
Stoppe Block Level Backup Engine Service
d
Stoppe Bluetooth Driver Management Service
d
Stoppe Certificate Propagation
d
Stoppe Client License Service (ClipSVC)
d
Stoppe COM+ System Application
d
Stoppe Computer Browser
d
Stoppe Connected Device Platform Service
d
Stoppe Data Sharing Service
d
Stoppe DataCollectionPublishingService
d
Stoppe Device Install Service
d
Stoppe Device Management Enrollment Service
d

Stoppe Device Setup Manager
d
Stoppe DevQuery Background Discovery Broker
d
Stoppe Distributed Transaction Coordinator
d
Stoppe dmwappushsvc
d
Stoppe Downloaded Maps Manager
d
Stoppe embeddedmode
d
Stoppe Encrypting File System (EFS)
d
Stoppe Enterprise App Management Service
d
Stoppe Extensible Authentication Protocol
d
Stoppe Fax
d
Stoppe File History Service
d
Stoppe Function Discovery Provider Host
d
Stoppe Function Discovery Resource Publication
d
Stoppe Google Update Service (gupdate)
d
Stoppe Google Update Service (gupdatem)
d
Stoppe HomeGroup Listener
d
Stoppe HomeGroup Provider
d
Stoppe Hyper-V Data Exchange Service
d
Stoppe Hyper-V Guest Service Interface
d
Stoppe Hyper-V Guest Shutdown Service
d
Stoppe Hyper-V Heartbeat Service
d
Stoppe Hyper-V Remote Desktop Virtualization Service
d
Stoppe Hyper-V Time Synchronization Service
d
Stoppe Hyper-V VM Session Service
d
Stoppe Hyper-V Volume Shadow Copy Requestor
d

Stoppe IKE and AuthIP IPsec Keying Modules
d
Stoppe Intel Content Protection HECI Service
d
Stoppe Intel Dynamic Platform & Thermal Framework Wireless Participant Service
d Application
Stoppe Interactive Services Detection
d
Stoppe Internet Connection Sharing (ICS)
d
Stoppe Internet Explorer ETW Collector Service
d
Stoppe IPsec Policy Agent
d
Stoppe KtmRm for Distributed Transaction Coordinator
d
Stoppe Link-Layer Topology Discovery Mapper
d
Stoppe Microsoft Diagnostics Hub Standard Collector Service
d
Stoppe Microsoft Account Sign-in Assistant
d
Stoppe Microsoft iSCSI Initiator Service
d
Stoppe Microsoft Passport
d
Stoppe Microsoft Passport Container
d
Stoppe Microsoft Software Shadow Copy Provider
d
Stoppe Microsoft Storage Spaces SMP
d
Stoppe Microsoft Windows SMS Router Service.
d
Stoppe Net.Tcp Port Sharing Service
d
Stoppe Netlogon
d
Stoppe Network Connected Devices Auto-Setup
d
Stoppe Network Connectivity Assistant
d
Stoppe Network Setup Service
d
Stoppe Optimize drives
d
Stoppe Peer Networking Grouping
d
Stoppe Performance Counter DLL Host
d

Stoppe Performance Logs & Alerts
d
Stoppe Phone Service
d
Stoppe PNRP Machine Name Publication Service
d
Stoppe Portable Device Enumerator Service
d
Stoppe Printer Extensions and Notifications
d
Stoppe Problem Reports and Solutions Control Panel Support
d
Stoppe Quality Windows Audio Video Experience
d
Stoppe Remote Access Auto Connection Manager
d
Stoppe Remote Access Connection Manager
d
Stoppe Remote Desktop Configuration
d
Stoppe Remote Desktop Services
d
Stoppe Remote Desktop Services UserMode Port Redirector
d
Stoppe Remote Procedure Call (RPC) Locator
d
Stoppe Remote Registry
d
Stoppe Retail Demo Service
d
Stoppe Routing and Remote Access
d
Stoppe Secondary Logon
d
Stoppe Secure Socket Tunneling Protocol Service
d
Stoppe Sensor Data Service
d
Stoppe Sensor Monitoring Service
d
Stoppe Smart Card
d
Stoppe Smart Card Device Enumeration Service
d
Stoppe Smart Card Removal Policy
d
Stoppe SNMP Trap
d
Stoppe Software Protection
d

Stoppe Spot Verifier
d
Stoppe Still Image Acquisition Events
d
Stoppe Storage Service
d
Stoppe Storage Tiers Management
d
Stoppe Telephony
d
Stoppe Update Orchestrator Service
d
Stoppe UPnP Device Host
d
Stoppe Virtual Disk
d
Stoppe Volume Shadow Copy
d
Stoppe WalletService
d
Stoppe WebClient
d
Stoppe Windows Biometric Service
d
Stoppe Windows Color System
d
Stoppe Windows Connect Now - Config Registrar
d
Stoppe Windows Encryption Provider Host Service
d
Stoppe Windows Error Reporting Service
d
Stoppe Windows Event Collector
d
Stoppe Windows Image Acquisition (WIA)
d
Stoppe Windows Media Player Network Sharing Service
d
Stoppe Windows Mobile Hotspot Service
d
Stoppe Windows Push Notifications Service
d
Stoppe Windows Remote Management (WS-Management)
d
Stoppe Windows Store Service (WSService)
d
Stoppe Windows Time
d
Stoppe Wired AutoConfig
d

Stoppe WMI Performance Adapter
d
Stoppe Work Folders
d
Stoppe WWAN AutoConfig
d
Stoppe Xbox Live Auth Manager
d
Stoppe Xbox Live Game Save
d
Stoppe Xbox Live Networking Service
d

TimeZone

TimeZone GMT +8:00 Hours
Language English (United States)
Location United States
Format English (United States)
Currency \$
Date Format M/d/yyyy
Time Format h:mm:ss tt

Scheduler

10/23/2016 3:01 AM; GoogleUpdateTaskMachineCore
10/23/2016 3:01 AM; GoogleUpdateTaskMachineUA
10/23/2016 3:45 AM; WpsNotifyTask_Administrator
10/23/2016 4:10 AM; WpsExternal_20151229080309

Hotfixes

Installed

10/22/2016 Update for Windows 10 Version 1511 for x64-based Systems (KB3116278)

Install this update to resolve issues in Windows. For a complete listing of the issues that are included in this update, see the associated Microsoft Knowledge Base article for more information. After you install this item, you may have to restart your computer.

Not Installed

System Folders

Application Data	C:\ProgramData
Cookies	C:\Users\Rawman\AppData\Local\Microsoft\Windows\INetCookies
Desktop	C:\Users\Rawman\Desktop
Documents	C:\Users\Public\Documents
Fonts	C:\Windows\Fonts
Global Favorites	C:\Users\Rawman\Favorites
Internet History	C:\Users\Rawman\AppData\Local\Microsoft\Windows\History
Local Application Data	C:\Users\Rawman\AppData\Local
Music	C:\Users\Public\Music
Path for burning CD	C:\Users\Rawman\AppData\Local\Microsoft\Windows\Burn\Burn
Physical Desktop	C:\Users\Rawman\Desktop
Pictures	C:\Users\Public\Pictures
Program Files	C:\Program Files

Public Desktop	C:\Users\Public\Desktop
Start Menu	C:\ProgramData\Microsoft\Windows\Start Menu
Start Menu Programs	C:\ProgramData\Microsoft\Windows\Start Menu\Programs
Startup	C:\ProgramData\Microsoft\Windows\Start Menu\Programs\Startup
Templates	C:\ProgramData\Microsoft\Windows\Templates
Temporary Internet Files	C:\Users\Rawman\AppData\Local\Microsoft\Windows\INetCache
User Favorites	C:\Users\Rawman\Favorites
Videos	C:\Users\Public\Videos
Windows Directory	C:\Windows
Windows/System	C:\Windows\system32

Process List

ApplicationFrameHost.exe

Process ID	5904
User	Rawman
Domain	MIPAD2
Path	C:\Windows\System32\ApplicationFrameHost.exe
Memory Usage	16 MB
Peak Memory Usage	40 MB

browser_broker.exe

Process ID	832
User	Rawman
Domain	MIPAD2
Path	C:\Windows\System32\browser_broker.exe
Memory Usage	16 MB
Peak Memory Usage	19 MB

chrome.exe

Process ID	6540
User	Rawman
Domain	MIPAD2
Path	C:\Program Files (x86)\Google\Chrome\Application\chrome.exe
Memory Usage	6.91 MB
Peak Memory Usage	6.91 MB

chrome.exe

Process ID	7632
User	Rawman
Domain	MIPAD2
Path	C:\Program Files (x86)\Google\Chrome\Application\chrome.exe
Memory Usage	21 MB
Peak Memory Usage	21 MB

chrome.exe

Process ID	4564
User	Rawman
Domain	MIPAD2
Path	C:\Program Files (x86)\Google\Chrome\Application\chrome.exe
Memory Usage	6.09 MB
Peak Memory Usage	6.09 MB

conhost.exe

Process ID	4812
------------	------

User Rawman
Domain MIPAD2
Path C:\Windows\System32\conhost.exe
Memory Usage 3.98 MB
Peak Memory Usage 17 MB

conhost.exe

Process ID 1712
User SYSTEM
Domain NT AUTHORITY
Path C:\Windows\System32\conhost.exe
Memory Usage 4.32 MB
Peak Memory Usage 4.88 MB

csrss.exe

Process ID 580
User SYSTEM
Domain NT AUTHORITY
Path C:\Windows\System32\csrss.exe
Memory Usage 1.61 MB
Peak Memory Usage 3.82 MB

csrss.exe

Process ID 664
User SYSTEM
Domain NT AUTHORITY
Path C:\Windows\System32\csrss.exe
Memory Usage 5.86 MB
Peak Memory Usage 28 MB

ctfmon.exe

Process ID 5296
User Rawman
Domain MIPAD2
Path C:\Windows\System32\ctfmon.exe
Memory Usage 1.51 MB
Peak Memory Usage 4.85 MB

dllhost.exe

Process ID 6240
User LOCAL SERVICE
Domain NT AUTHORITY
Path C:\Windows\System32\dllhost.exe
Memory Usage 5.09 MB
Peak Memory Usage 9.23 MB

dllhost.exe

Process ID 520
User Rawman
Domain MIPAD2
Path C:\Windows\System32\dllhost.exe
Memory Usage 33 MB
Peak Memory Usage 40 MB

DptfParticipantProcessorService.exe

Process ID 2008
User SYSTEM

Domain NT AUTHORITY
Path C:\Windows\System32\DptfParticipantProcessorService.exe
Memory Usage 3.40 MB
Peak Memory Usage 3.94 MB

DptfPolicyCriticalService.exe

Process ID 2040
User SYSTEM
Domain NT AUTHORITY
Path C:\Windows\System32\DptfPolicyCriticalService.exe
Memory Usage 2.06 MB
Peak Memory Usage 3.86 MB

DptfPolicyLpmService.exe

Process ID 1316
User SYSTEM
Domain NT AUTHORITY
Path C:\Windows\System32\DptfPolicyLpmService.exe
Memory Usage 1.66 MB
Peak Memory Usage 3.83 MB

DptfPolicyLpmServiceHelper.exe

Process ID 4236
User Rawman
Domain MIPAD2
Path C:\Windows\System32\DptfPolicyLpmServiceHelper.exe
Memory Usage 160 KB
Peak Memory Usage 2.82 MB

dwm.exe

Process ID 380
User DWM-1
Domain Window Manager
Path C:\Windows\System32\dwm.exe
Memory Usage 52 MB
Peak Memory Usage 156 MB

explorer.exe

Process ID 3972
User Rawman
Domain MIPAD2
Path C:\Windows\explorer.exe
Memory Usage 61 MB
Peak Memory Usage 191 MB

FlashUtil_ActiveX.exe

Process ID 6192
User Rawman
Domain MIPAD2
Path C:\Windows\System32\Macromed\Flash\FlashUtil_ActiveX.exe
Memory Usage 3.29 MB
Peak Memory Usage 16 MB

fodhelper.exe

Process ID 1660
User Rawman
Domain MIPAD2

Path C:\Windows\System32\fodhelper.exe
Memory Usage 12 MB
Peak Memory Usage 13 MB

igfxCUIService.exe

Process ID 1352
User SYSTEM
Domain NT AUTHORITY
Path C:\Windows\System32\igfxCUIService.exe
Memory Usage 6.76 MB
Peak Memory Usage 8.00 MB

igfxEM.exe

Process ID 3632
User Rawman
Domain MIPAD2
Path C:\Windows\System32\igfxEM.exe
Memory Usage 2.95 MB
Peak Memory Usage 11 MB

igfxHK.exe

Process ID 3708
User Rawman
Domain MIPAD2
Path C:\Windows\System32\igfxHK.exe
Memory Usage 1.87 MB
Peak Memory Usage 8.41 MB

igfxTray.exe

Process ID 3744
User Rawman
Domain MIPAD2
Path C:\Windows\System32\igfxTray.exe
Memory Usage 2.98 MB
Peak Memory Usage 11 MB

InstallAgent.exe

Process ID 3416
User Rawman
Domain MIPAD2
Path C:\Windows\System32\InstallAgent.exe
Memory Usage 1.18 MB
Peak Memory Usage 13 MB

lsass.exe

Process ID 740
User SYSTEM
Domain NT AUTHORITY
Path C:\Windows\System32\lsass.exe
Memory Usage 14 MB
Peak Memory Usage 15 MB

MicrosoftEdge.exe

Process ID 5192
User Rawman
Domain MIPAD2

Path C:\Windows\SystemApps\Microsoft.MicrosoftEdge_8wekyb3d8bbwe
\MicrosoftEdge.exe
Memory Usage 42 MB
Peak Memory 100 MB
Usage

MicrosoftEdgeCP.exe

Process ID 6552
User Rawman
Domain MIPAD2
Path C:\Windows\SystemApps\Microsoft.MicrosoftEdge_8wekyb3d8bbwe
\MicrosoftEdgeCP.exe
Memory Usage 215 MB
Peak Memory 340 MB
Usage

MicrosoftEdgeCP.exe

Process ID 7380
User Rawman
Domain MIPAD2
Path C:\Windows\SystemApps\Microsoft.MicrosoftEdge_8wekyb3d8bbwe
\MicrosoftEdgeCP.exe
Memory Usage 28 MB
Peak Memory 156 MB
Usage

MicrosoftEdgeCP.exe

Process ID 2956
User Rawman
Domain MIPAD2
Path C:\Windows\SystemApps\Microsoft.MicrosoftEdge_8wekyb3d8bbwe
\MicrosoftEdgeCP.exe
Memory Usage 22 MB
Peak Memory 280 MB
Usage

MicrosoftEdgeCP.exe

Process ID 5300
User Rawman
Domain MIPAD2
Path C:\Windows\SystemApps\Microsoft.MicrosoftEdge_8wekyb3d8bbwe
\MicrosoftEdgeCP.exe
Memory Usage 11 MB
Peak Memory 159 MB
Usage

MicrosoftEdgeCP.exe

Process ID 4276
User Rawman
Domain MIPAD2
Path C:\Windows\SystemApps\Microsoft.MicrosoftEdge_8wekyb3d8bbwe
\MicrosoftEdgeCP.exe
Memory Usage 67 MB
Peak Memory 234 MB
Usage

MicrosoftEdgeCP.exe

Process ID 1632
User Rawman
Domain MIPAD2
Path C:\Windows\SystemApps\Microsoft.MicrosoftEdge_8wekyb3d8bbwe
\MicrosoftEdgeCP.exe
Memory Usage 17 MB
Peak Memory Usage 104 MB

mmc.exe

Process ID 7496
User Rawman
Domain MIPAD2
Path C:\Windows\System32\mmc.exe
Memory Usage 13 MB
Peak Memory Usage 21 MB

MpCmdRun.exe

Process ID 5984
User NETWORK SERVICE
Domain NT AUTHORITY
Path C:\Program Files\Windows Defender\MpCmdRun.exe
Memory Usage 6.51 MB
Peak Memory Usage 11 MB

msiexec.exe

Process ID 5532
User SYSTEM
Domain NT AUTHORITY
Path C:\Windows\System32\msiexec.exe
Memory Usage 14 MB
Peak Memory Usage 17 MB

msinfo32.exe

Process ID 5816
User Rawman
Domain MIPAD2
Path C:\Windows\System32\msinfo32.exe
Memory Usage 12 MB
Peak Memory Usage 15 MB

MsMpEng.exe

Process ID 2156
User SYSTEM
Domain NT AUTHORITY
Path C:\Program Files\Windows Defender\MsMpEng.exe
Memory Usage 76 MB
Peak Memory Usage 121 MB

NetworkUXBroker.exe

Process ID 1484
User Rawman
Domain MIPAD2
Path C:\Windows\System32\NetworkUXBroker.exe
Memory Usage 6.64 MB

Peak Memory Usage 16 MB

NisSrv.exe

Process ID 2884
User LOCAL SERVICE
Domain NT AUTHORITY
Path C:\Program Files\Windows Defender\NisSrv.exe
Memory Usage 7.21 MB
Peak Memory Usage 36 MB

notepad.exe

Process ID 6248
User Rawman
Domain MIPAD2
Path C:\Windows\System32\notepad.exe
Memory Usage 4.34 MB
Peak Memory Usage 12 MB

OneDrive.exe

Process ID 5888
User Rawman
Domain MIPAD2
Path C:\Users\Rawman\AppData\Local\Microsoft\OneDrive\OneDrive.exe
Memory Usage 4.28 MB
Peak Memory Usage 18 MB

powershell.exe

Process ID 5124
User Rawman
Domain MIPAD2
Path C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
Memory Usage 46 MB
Peak Memory Usage 84 MB

RemindersServer.exe

Process ID 3572
User Rawman
Domain MIPAD2
Path C:\Windows\SystemApps\Microsoft.Windows.Cortana_cw5n1h2txyewy\RemindersServer.exe
Memory Usage 4.54 MB
Peak Memory Usage 19 MB

Rtl2SBgProc64.exe

Process ID 5840
User Rawman
Domain MIPAD2
Path C:\Program Files\Realtek\Audio\IIS\Rtl2SBgProc64.exe
Memory Usage 1.59 MB
Peak Memory Usage 9.27 MB

Rtl2SBgProc64.exe

Process ID 2288
User SYSTEM
Domain NT AUTHORITY
Path C:\Program Files\Realtek\Audio\IIS\Rtl2SBgProc64.exe
Memory Usage 1.68 MB
Peak Memory Usage 7.30 MB

Rtkl2SAudioService64.exe

Process ID 2232
User SYSTEM
Domain NT AUTHORITY
Path C:\Program Files\Realtek\Audio\IIS\Rtkl2SAudioService64.exe
Memory Usage 2.82 MB
Peak Memory Usage 7.64 MB

RtkNGUI64.exe

Process ID 4432
User Rawman
Domain MIPAD2
Path C:\Program Files\Realtek\Audio\AP\RtkNGUI64.exe
Memory Usage 5.45 MB
Peak Memory Usage 12 MB

RuntimeBroker.exe

Process ID 3480
User Rawman
Domain MIPAD2
Path C:\Windows\System32\RuntimeBroker.exe
Memory Usage 26 MB
Peak Memory Usage 46 MB

SearchIndexer.exe

Process ID 4232
User SYSTEM
Domain NT AUTHORITY
Path C:\Windows\System32\SearchIndexer.exe
Memory Usage 20 MB
Peak Memory Usage 28 MB

SearchUI.exe

Process ID 4704
User Rawman
Domain MIPAD2
Path C:\Windows\SystemApps\Microsoft.Windows.Cortana_cw5n1h2txyewy\SearchUI.exe
Memory Usage 12 MB
Peak Memory Usage 146 MB
Usage

services.exe

Process ID 728
User SYSTEM
Domain NT AUTHORITY
Path C:\Windows\System32\services.exe
Memory Usage 5.16 MB
Peak Memory Usage 6.75 MB

ShellExperienceHost.exe

Process ID 4612
User Rawman
Domain MIPAD2
Path C:\Windows\SystemApps\ShellExperienceHost_cw5n1h2txyewy\ShellExperienceHost.exe
Memory Usage 9.31 MB
Peak Memory Usage 88 MB

sihost.exe

Process ID 3204
User Rawman
Domain MIPAD2
Path C:\Windows\System32\sihost.exe
Memory Usage 14 MB
Peak Memory Usage 22 MB

smss.exe

Process ID 340
User SYSTEM
Domain NT AUTHORITY
Path C:\Windows\System32\smss.exe
Memory Usage 356 KB
Peak Memory Usage 1.14 MB

Speccy64.exe

Process ID 4140
User Rawman
Domain MIPAD2
Path C:\Program Files\Speccy\Speccy64.exe
Memory Usage 25 MB
Peak Memory Usage 25 MB

spoolsv.exe

Process ID 1616
User SYSTEM
Domain NT AUTHORITY
Path C:\Windows\System32\spoolsv.exe
Memory Usage 11 MB
Peak Memory Usage 14 MB

svchost.exe

Process ID 1168
User LOCAL SERVICE
Domain NT AUTHORITY
Path C:\Windows\System32\svchost.exe
Memory Usage 15 MB
Peak Memory Usage 90 MB

svchost.exe

Process ID 1040
User SYSTEM
Domain NT AUTHORITY
Path C:\Windows\System32\svchost.exe
Memory Usage 11 MB

Peak Memory Usage 40 MB

svchost.exe

Process ID 80
User LOCAL SERVICE
Domain NT AUTHORITY
Path C:\Windows\System32\svchost.exe
Memory Usage 9.69 MB
Peak Memory Usage 28 MB

svchost.exe

Process ID 388
User LOCAL SERVICE
Domain NT AUTHORITY
Path C:\Windows\System32\svchost.exe
Memory Usage 8.20 MB
Peak Memory Usage 8.64 MB

svchost.exe

Process ID 724
User LOCAL SERVICE
Domain NT AUTHORITY
Path C:\Windows\System32\svchost.exe
Memory Usage 15 MB
Peak Memory Usage 28 MB

svchost.exe

Process ID 584
User SYSTEM
Domain NT AUTHORITY
Path C:\Windows\System32\svchost.exe
Memory Usage 34 MB
Peak Memory Usage 330 MB

svchost.exe

Process ID 908
User SYSTEM
Domain NT AUTHORITY
Path C:\Windows\System32\svchost.exe
Memory Usage 9.96 MB
Peak Memory Usage 21 MB

svchost.exe

Process ID 2016
User SYSTEM
Domain NT AUTHORITY
Path C:\Windows\System32\svchost.exe
Memory Usage 11 MB
Peak Memory Usage 24 MB

svchost.exe

Process ID 2140
User SYSTEM
Domain NT AUTHORITY
Path C:\Windows\System32\svchost.exe
Memory Usage 14 MB
Peak Memory Usage 21 MB

svchost.exe

Process ID 984
User NETWORK SERVICE
Domain NT AUTHORITY
Path C:\Windows\System32\svchost.exe
Memory Usage 9.84 MB
Peak Memory Usage 10 MB

svchost.exe

Process ID 5264
User SYSTEM
Domain NT AUTHORITY
Path C:\Windows\System32\svchost.exe
Memory Usage 5.27 MB
Peak Memory Usage 8.71 MB

svchost.exe

Process ID 1532
User NETWORK SERVICE
Domain NT AUTHORITY
Path C:\Windows\System32\svchost.exe
Memory Usage 14 MB
Peak Memory Usage 17 MB

svchost.exe

Process ID 4908
User Rawman
Domain MIPAD2
Path C:\Windows\System32\svchost.exe
Memory Usage 8.67 MB
Peak Memory Usage 26 MB

svchost.exe

Process ID 7172
User LOCAL SERVICE
Domain NT AUTHORITY
Path C:\Windows\System32\svchost.exe
Memory Usage 7.82 MB
Peak Memory Usage 7.82 MB

System

Process ID 4
Memory Usage 139 MB
Peak Memory Usage 159 MB

System Idle Process

Process ID 0

SystemSettingsBroker.exe

Process ID 6160
User Rawman
Domain MIPAD2
Path C:\Windows\System32\SystemSettingsBroker.exe
Memory Usage 6.79 MB
Peak Memory Usage 19 MB

TabTip.exe

Process ID 3260

User	Rawman
Domain	MIPAD2
Path	C:\Program Files\Common Files\microsoft shared\ink\TabTip.exe
Memory Usage	11 MB
Peak Memory Usage	43 MB
TabTip32.exe	
Process ID	540
User	Rawman
Domain	MIPAD2
Path	C:\Program Files (x86)\Common Files\Microsoft Shared\Ink\TabTip32.exe
Memory Usage	2.98 MB
Peak Memory Usage	4.02 MB
taskeng.exe	
Process ID	6808
User	SYSTEM
Domain	NT AUTHORITY
Path	C:\Windows\System32\taskeng.exe
Memory Usage	5.71 MB
Peak Memory Usage	5.84 MB
taskhostw.exe	
Process ID	3216
User	Rawman
Domain	MIPAD2
Path	C:\Windows\System32\taskhostw.exe
Memory Usage	7.93 MB
Peak Memory Usage	57 MB
taskhostw.exe	
Process ID	5480
User	Rawman
Domain	MIPAD2
Path	C:\Windows\System32\taskhostw.exe
Memory Usage	2.07 MB
Peak Memory Usage	16 MB
TiWorker.exe	
Process ID	6884
User	SYSTEM
Domain	NT AUTHORITY
Path	C:\Windows\WinSxS\amd64_microsoft-windows-servicingstack_31bf3856ad364e35_10.0.10586.0_none_95e4f9a171a1ad95\TiWorker.exe
Memory Usage	9.66 MB
Peak Memory Usage	31 MB
TrustedInstaller.exe	
Process ID	7180

User SYSTEM
Domain NT AUTHORITY
Path C:\Windows\servicing\TrustedInstaller.exe
Memory Usage 5.37 MB
Peak Memory Usage 16 MB

wininit.exe

Process ID 656
User SYSTEM
Domain NT AUTHORITY
Path C:\Windows\System32\wininit.exe
Memory Usage 956 KB
Peak Memory Usage 4.63 MB

winlogon.exe

Process ID 816
User SYSTEM
Domain NT AUTHORITY
Path C:\Windows\System32\winlogon.exe
Memory Usage 6.40 MB
Peak Memory Usage 22 MB

wlanext.exe

Process ID 1696
User SYSTEM
Domain NT AUTHORITY
Path C:\Windows\System32\wlanext.exe
Memory Usage 4.50 MB
Peak Memory Usage 5.09 MB

WmiPrvSE.exe

Process ID 7572
User NETWORK SERVICE
Domain NT AUTHORITY
Path C:\Windows\System32\wbem\WmiPrvSE.exe
Memory Usage 11 MB
Peak Memory Usage 11 MB

WmiPrvSE.exe

Process ID 7664
User SYSTEM
Domain NT AUTHORITY
Path C:\Windows\System32\wbem\WmiPrvSE.exe
Memory Usage 5.69 MB
Peak Memory Usage 7.45 MB

wpscloudsvr.exe

Process ID 2128
User SYSTEM
Domain NT AUTHORITY
Path C:\Program Files (x86)\Kingsoft\WPS Office\wpscloudsvr.exe
Memory Usage 1.69 MB
Peak Memory Usage 5.17 MB

Security Options

Accounts: Administrator account status	Disabled
Accounts: Block Microsoft accounts	Not Defined
Accounts: Guest account status	Disabled
Accounts: Limit local account use of blank passwords to console logon only	Enabled
Accounts: Rename administrator account	Administrator
Accounts: Rename guest account	Guest
Audit: Audit the access of global system objects	Disabled
Audit: Audit the use of Backup and Restore privilege	Disabled
Audit: Force audit policy subcategory settings (Windows Vista or later) to override audit policy category settings	Not Defined

Audit: Shut Disabled
down system
immediately if
unable to log
security
audits

DCOM: Not Defined
Machine
Access
Restrictions
in Security
Descriptor
Definition
Language
(SDDL)
syntax

DCOM: Not Defined
Machine
Launch
Restrictions
in Security
Descriptor
Definition
Language
(SDDL)
syntax

Devices: Enabled
Allow undock
without
having to log
on

Devices: Not Defined
Allowed to
format and
eject
removable
media

Devices: Disabled
Prevent users
from
installing
printer drivers

Devices: Not Defined
Restrict
CD-ROM
access to
locally
logged-on
user only

Devices:	Not Defined
Restrict floppy access to locally logged-on user only	
Domain controller:	Not Defined
Allow server operators to schedule tasks	
Domain controller: LDAP server signing requirements	Not Defined
Domain controller: Refuse machine account password changes	Not Defined
Domain member: Digitally encrypt or sign secure channel data (always)	Enabled
Domain member: Digitally encrypt secure channel data (when possible)	Enabled
Domain member: Digitally sign secure channel data (when possible)	Enabled

Domain member: Disable machine account password changes	Disabled
Domain member: Maximum machine account password age	30 days
Domain member: Require strong (Windows 2000 or later) session key	Enabled
Interactive logon: Display user information when the session is locked	Not Defined
Interactive logon: Do not display last user name	Disabled
Interactive logon: Do not require CTRL+ALT+DEL	Not Defined
Interactive logon: Machine account lockout threshold	Not Defined
Interactive logon: Machine inactivity limit	Not Defined
Interactive logon: Message text for users attempting to log on	
Interactive logon: Message title for users attempting to log on	

Interactive logon: Number of previous logons to cache (in case domain controller is not available)	10 logons
Interactive logon: Prompt user to change password before expiration	5 days
Interactive logon: Require Domain Controller authentication to unlock workstation	Disabled
Interactive logon: Require smart card	Disabled
Interactive logon: Smart card removal behavior	No Action
Microsoft network client: Digitally sign communications (always)	Disabled
Microsoft network client: Digitally sign communications (if server agrees)	Enabled

Microsoft network client: Send unencrypted password to third-party SMB servers	Disabled
Microsoft network server: Amount of idle time required before suspending session	15 minutes
Microsoft network server: Attempt S4U2Self to obtain claim information	Not Defined
Microsoft network server: Digitally sign communications (always)	Disabled
Microsoft network server: Digitally sign communications (if client agrees)	Disabled
Microsoft network server: Disconnect clients when logon hours expire	Enabled
Microsoft network server: Server SPN target name validation level	Not Defined

Network Disabled

access: Allow
anonymous
SID/Name
translation

Network Enabled

access: Do
not allow
anonymous
enumeration
of SAM
accounts

Network Disabled

access: Do
not allow
anonymous
enumeration
of SAM
accounts and
shares

Network Disabled

access: Do
not allow
storage of
passwords
and
credentials
for network
authenticatio
n

Network Disabled

access: Let
Everyone
permissions
apply to
anonymous
users

Network access: Named Pipes that can be accessed anonymously

Network System\CurrentControlSet\Control\ProductOptions,System\CurrentContr
access: olSet\Control\Server Applications,Software\Microsoft\Windows

Remotely NT\CurrentVersion

accessible
registry paths

Network access: Remotely accessible registry paths and sub-paths System\CurrentControlSet\Control\Print\Printers, System\CurrentControlSet\Services\Eventlog, Software\Microsoft\OLAP Server, Software\Microsoft\Windows NT\CurrentVersion\Print, Software\Microsoft\Windows NT\CurrentVersion\Windows, System\CurrentControlSet\Control\ContentIndex, System\CurrentControlSet\Control\Terminal Server, System\CurrentControlSet\Control\Terminal Server\UserConfig, System\CurrentControlSet\Control\Terminal Server\DefaultUserConfiguration, Software\Microsoft\Windows NT\CurrentVersion\Perflib, System\CurrentControlSet\Services\SysmonLog
g
Enabled

Network access: Restrict anonymous access to Named Pipes and Shares

Not Defined

Network access: Shares that can be accessed anonymously

Classic - local users authenticate as themselves

Network access: Sharing and security model for local accounts

Not Defined

Network security: Allow Local System to use computer identity for NTLM

Not Defined

Network security: Allow LocalSystem NULL session fallback

Network security: Allow PKU2U authentication requests to this computer to use online identities.	Not Defined
Network security: Configure encryption types allowed for Kerberos	Not Defined
Network security: Do not store LAN Manager hash value on next password change	Enabled
Network security: Force logoff when logon hours expire	Disabled
Network security: LAN Manager authentication level	Not Defined
Network security: LDAP client signing requirements	Negotiate signing
Network security: Minimum session security for NTLM SSP based (including secure RPC) clients	Require 128-bit encryption

Network security: Minimum session security for NTLM SSP based (including secure RPC) servers

Require 128-bit encryption

Not Defined

Network security: Restrict NTLM: Add remote server exceptions for NTLM authentication

Not Defined

Network security: Restrict NTLM: Add server exceptions in this domain

Not Defined

Network security: Restrict NTLM: Audit Incoming NTLM Traffic

Not Defined

Network security: Restrict NTLM authentication in this domain

Not Defined

Network security: Restrict NTLM: Incoming NTLM traffic

Network security: Restrict NTLM: NTLM authentication in this domain	Not Defined
Network security: Restrict NTLM: Outgoing NTLM traffic to remote servers	Not Defined
Recovery console: Allow automatic administrative logon	Disabled
Recovery console: Allow floppy copy and access to all drives and all folders	Disabled
Shutdown: Allow system to be shut down without having to log on	Enabled
Shutdown: Clear virtual memory pagefile	Disabled
System cryptography: Force strong key protection for user keys stored on the computer	Not Defined

System Disabled

cryptography:
Use FIPS
compliant
algorithms for
encryption,
hashing, and
signing

System Enabled

objects:
Require case
insensitivity
for
non-Windows
subsystems

System Enabled

objects:
Strengthen
default
permissions
of internal
system
objects (e.g.
Symbolic
Links)

System settings: Optional subsystems

System Disabled

settings: Use
Certificate
Rules on
Windows
Executables
for Software
Restriction
Policies

User Account Not Defined

Control:
Admin
Approval
Mode for the
Built-in
Administrator
account

User Account Disabled

Control: Allow

UIAccess applications to prompt for elevation without using the secure desktop

User Account Prompt for consent for non-Windows binaries

Control:

Behavior of the elevation prompt for administrators in Administrators in Administrative Approval Mode

User Account Prompt for credentials

Control:

Behavior of the elevation prompt for standard users

User Account Enabled

Control:

Detect application installations and prompt for elevation

User Account Disabled

Control: Only

elevate executables that are signed and validated

User Account Enabled

Control: Only

elevate UIAccess applications that are installed in secure locations

User Account Enabled
Control: Run
all
administrators
in Administrators
Approval
Mode

User Account Enabled
Control:
Switch to the
secure
desktop
when
prompting for
elevation

User Account Enabled
Control:
Virtualize file
and registry
write failures
to per-user
locations

Device Tree

ACPI x64-based PC

Microsoft ACPI-Compliant System

- ACPI Fixed Feature Button
- ACPI Lid
- ACPI Power Button
- ACPI Processor Aggregator
- ACPI Thermal Zone
- High precision event timer
- Intel Serial IO GPIO Controller
- Intel Serial IO GPIO Controller
- Intel Serial IO GPIO Controller
- Intel Serial IO GPIO Controller
- Intel Serial IO GPIO Controller
- Intel Atom x5-Z8500 CPU @ 1.44GHz
- Intel Atom x5-Z8500 CPU @ 1.44GHz
- Intel Atom x5-Z8500 CPU @ 1.44GHz
- Intel Atom x5-Z8500 CPU @ 1.44GHz
- Intel Dynamic Platform & Thermal Framework Display Participant Driver
- Intel Dynamic Platform & Thermal Framework Driver
- Intel Dynamic Platform & Thermal Framework Generic Participant Driver
- Intel Dynamic Platform & Thermal Framework Generic Participant Driver
- Intel Dynamic Platform & Thermal Framework Generic Participant Driver
- Intel Dynamic Platform & Thermal Framework Power Participant Driver
- Intel Sideband Fabric Device
- Microsoft AC Adapter
- System CMOS/real time clock
- Trusted Platform Module 2.0

PCI Express Root Complex

- Intel Dynamic Platform & Thermal Framework Processor Participant Driver
- Intel Imaging Signal Processor 2401
- Intel Integrated Sensor Solution
- Intel Power Engine Plug-in
- Intel Serial IO DMA Controller
- Intel Serial IO DMA Controller
- Intel Serial IO I2C ES Controller
- Intel Serial IO I2C ES Controller
- Intel Serial IO I2C ES Controller
- Intel Serial IO SPI Controller
- Intel Serial IO SPI Controller
- Intel Serial IO SPI Controller
- Intel Serial IO UART Controller
- Intel Trusted Execution Engine Interface
- Motherboard resources
- Motherboard resources
- PCI standard host CPU bridge

Intel(R) HD Graphics

- Generic PnP Monitor
- Intel AVStream Camera

Intel(R) USB 3.0 eXtensible Host Controller - 1.0 (Microsoft)

USB Root Hub (xHCI)

USB Composite Device

Logitech USB Input Device

- HID Keyboard Device

USB Input Device

- HID-compliant consumer control device
- HID-compliant mouse
- HID-compliant system controller
- HID-compliant vendor-defined device

USB Input Device

- HID-compliant vendor-defined device
- HID-compliant vendor-defined device
- HID-compliant vendor-defined device

PCI Express Root Port

Broadcom 802.11ac Wireless PCIE Full Dongle Adapter #2

- Microsoft Wi-Fi Direct Virtual Adapter #2

PCI standard ISA bridge

- Communications Port (COM1)
- Legacy device
- Motherboard resources
- Programmable interrupt controller
- System timer

Intel SD Host Controller

SD Storage Class Controller

- Samsung AGND3R

Intel(R) Serial IO UART Controller

Broadcom Serial Bus Driver over UART Bus Enumerator

- Bluetooth Radio

Intel(R) Serial IO I2C ES Controller

BQMG0890 Charger Controller
LP8556 Backlight Controller
Realtek I2S Audio Codec

Intel(R) Serial IO I2C ES Controller

Camera Sensor OV5693
Camera Sensor T4KA3

Intel(R) Serial IO I2C ES Controller

HID for FocalTech Touch

HID Keyboard Device
HID-compliant touch screen
Microsoft Input Configuration Device

Intel(R) Serial IO I2C ES Controller

Intel Power Management IC Device
Microsoft ACPI-Compliant Control Method Battery

Intel SST Audio Device (WDM)

Microphone (Intel SST Audio Device (WDM))
Speakers (Intel SST Audio Device (WDM))

Intel(R) HID Event Filter

HID Keyboard Device
HID-compliant consumer control device
HID-compliant consumer control device
HID-compliant consumer control device
HID-compliant consumer control device
HID-compliant consumer control device
HID-compliant consumer control device
HID-compliant consumer control device
HID-compliant consumer control device
HID-compliant consumer control device
HID-compliant system controller
HID-compliant system controller
HID-compliant system controller
HID-compliant vendor-defined device
HID-compliant vendor-defined device
HID-compliant vendor-defined device
HID-compliant wireless radio controls

HID Button over Interrupt Driver

Portable Device Control device

Converted Portable Device Control device

HID Keyboard Device
HID-compliant consumer control device
HID-compliant system controller

Microsoft UEFI-Compliant System

Device Firmware
Device Firmware
System Firmware

CPU

Intel Atom x5 Z8500

Cores 4

Threads 4
Name Intel Atom x5 Z8500
Code Name Cherry Trail
Package Socket 1380 BGA
Technology 14nm
Specification Intel Atom x5-Z8500 CPU @ 1.44GHz
Family 6
Extended Family 6
Model C
Extended Model 4C
Stepping 3
Revision C0
Instructions MMX, SSE, SSE2, SSE3, SSSE3, SSE4.1, SSE4.2, Intel 64, NX, VMX, AES
Virtualization Supported, Enabled
Hyperthreading Supported, Disabled
Stock Core Speed 1440 MHz
Stock Bus Speed 80 MHz
Average Temperature 58 °C

Caches

L1 Data Cache Size 4 x 24 KBytes
L1 Instructions Cache Size 4 x 32 KBytes
L2 Unified Cache Size 2 x 1024 KBytes

Cores

Core 0

Core Speed 479.8 MHz
Multiplier x 6.0
Bus Speed 80.0 MHz
Temperature 56 °C
Threads APIC ID: 0

Core 1

Core Speed 2239.1 MHz
Multiplier x 28.0
Bus Speed 80.0 MHz
Temperature 63 °C
Threads APIC ID: 2

Core 2

Core Speed 479.8 MHz
Multiplier x 6.0
Bus Speed 80.0 MHz
Temperature 56 °C
Threads APIC ID: 4

Core 3

Core Speed 479.8 MHz
Multiplier x 6.0
Bus Speed 80.0 MHz
Temperature 56 °C
Threads APIC ID: 6

RAM

Memory

Type	DDR3
Size	1978 MBytes
DRAM Frequency	799.7 MHz
CAS# Latency (CL)	12 clocks
RAS# to CAS# Delay (tRCD)	15 clocks
RAS# Precharge (tRP)	20 clocks
Cycle Time (tRAS)	34 clocks
Command Rate (CR)	1T

Physical Memory

Memory Usage	81 %
Total Physical	1.93 GB
Available Physical	362 MB
Total Virtual	3.37 GB
Available Virtual	704 MB

SPD

Number Of SPD Modules	0
-----------------------	---

Motherboard

Manufacturer	Xiaomi Inc
Model	Mipad (CHV)
Version	4
Chipset Vendor	Intel
Chipset Model	Braswell Host Bridge
Chipset Revision	20
Southbridge Vendor	Intel
Southbridge Model	Braswell LPC Bridge
Southbridge Revision	20
System Temperature	38 °C

BIOS

Brand	Byosoft Corporation
Version	MIPad-P4.X64.0043.R03.1603071414
Date	3/7/2016

PCI Data

Graphics

Monitor

Name	LFP_Sharp on Intel HD Graphics
Current Resolution	1024x768 pixels
Work Resolution	1024x728 pixels
State	Enabled, Primary
Monitor Width	2048
Monitor Height	1536
Monitor BPP	32 bits per pixel
Monitor Frequency	60 Hz
Device	\\.\DISPLAY1\Monitor0

Intel HD Graphics

Manufacturer	Intel
Model	HD Graphics

Device ID 8086-22B0
Revision 21
Subvendor Unknown (1D72)
Current Performance Level Level 0
Driver version 20.19.15.4331

Count of performance levels : 1
Level 1 - "Perf Level 0"

Storage

Hard drives

Samsung AGND3R

Manufacturer SAMSUNG
Interface SD
Capacity 14.6 GB
Real size 15,634,268,160 bytes
RAID Type None

S.M.A.R.T

S.M.A.R.T not supported

Partition 0

Partition ID Disk #0, Partition #0
Size 100 MB

Partition 1

Partition ID Disk #0, Partition #1
Disk Letter C:
File System NTFS
Volume Serial Number 6805BEC7
Size 14 GB
Used Space 10.6 GB (76%)
Free Space 3.35 GB (24%)

Partition 2

Partition ID Disk #0, Partition #2
File System NTFS
Volume Serial Number D0067B45
Size 499 MB
Used Space 441 MB (88%)
Free Space 58 MB (12%)

Flash drives

UFD 2.0 Silicon-Power16G USB Device

Interface USB
Capacity 14.9 GB
Real size 16,013,852,672 bytes
RAID Type None

S.M.A.R.T

S.M.A.R.T not supported

Partition 0

Partition ID Disk #1, Partition #0
Disk Letter D:
File System NTFS
Volume Serial Number 8029CA72
Size 14.9 GB

Used Space	11.2 GB (75%)
Free Space	3.71 GB (25%)

Optical Drives

No optical disk drives detected

Audio

Sound Card

Intel SST Audio Device (WDM)

Playback Device

Speakers (Intel SST Audio Device (WDM))

Recording Device

Microphone (Intel SST Audio Device (WDM))

Peripherals

HID Keyboard Device

Device Kind Keyboard

Device Name HID Keyboard Device

Vendor Microsoft

Location Converted Portable Device Control device

Driver

Date 6-21-2006

Version 10.0.10586.0

File C:\Windows\system32\DRIVERS\kbdhid.sys

File C:\Windows\system32\DRIVERS\kbdclass.sys

HID Keyboard Device

Device Kind Keyboard

Device Name HID Keyboard Device

Vendor Unknown

Location Intel HID Event Filter

Driver

Date 6-21-2006

Version 10.0.10586.0

File C:\Windows\system32\DRIVERS\kbdhid.sys

File C:\Windows\system32\DRIVERS\kbdclass.sys

HID Keyboard Device

Device Kind Keyboard

Device Name HID Keyboard Device

Vendor FTSC

Location HID for FocalTech Touch

Driver

Date 6-21-2006

Version 10.0.10586.0

File C:\Windows\system32\DRIVERS\kbdhid.sys

File C:\Windows\system32\DRIVERS\kbdclass.sys

HID Keyboard Device

Device Kind Keyboard

Device Name HID Keyboard Device

Vendor Logitech

Location Logitech USB Input Device

Driver

Date 6-21-2006
Version 10.0.10586.0
File C:\Windows\system32\DRIVERS\kbdhid.sys
File C:\Windows\system32\DRIVERS\kbdclass.sys

HID-compliant mouse

Device Kind Mouse
Device Name HID-compliant mouse
Vendor Logitech
Location USB Input Device

Driver

Date 6-21-2006
Version 10.0.10586.0
File C:\Windows\system32\DRIVERS\mouhid.sys
File C:\Windows\system32\DRIVERS\mouclass.sys

Intel(R) AVStream Camera

Device Kind Camera/scanner
Device Name Intel AVStream Camera
Vendor Intel
Location Intel HD Graphics

Driver

Date 10-29-2015
Version 21.10154.6044.496
File C:\Windows\system32\DRIVERS\iacamera64.sys
File C:\Windows\system32\DRIVERS\isp_firmware.bin
File C:\Windows\system32\DRIVERS\mute.bmp
File C:\Windows\system32\IntelCameraPlugin64.dll
File C:\Windows\system32\IntelSocYuvCopy64.dll
File C:\Windows\system32\pvl64.dll
File C:\Windows\system32\libia_cp64.dll
File C:\Windows\system32\cilkrts20_64.dll
File C:\Windows\SysWOW64\IntelCameraPlugin.dll
File C:\Windows\SysWOW64\IntelSocYuvCopy.dll
File C:\Windows\SysWOW64\pvl.dll
File C:\Windows\SysWOW64\libia_cp.dll
File C:\Windows\SysWOW64\cilkrts20_32.dll

Silicon-Power16G

Device Kind Portable Device
Device Name Silicon-Power16G
Vendor UFD_2.0
Comment SiliconPower 16GB
Location Generic volume

Driver

Date 6-21-2006
Version 10.0.10586.0
File C:\Windows\system32\DRIVERS\WUDFRd.sys

Printers**Fax**

Printer Port SHRFAX:
Print Processor winprint

Availability Always
Priority 1
Duplex None
Print Quality 200 * 200 dpi Monochrome
Status Unknown

Driver

Driver Name Microsoft Shared Fax Driver (v4.00)
Driver Path C:\Windows\system32\spool\DRIVERS\x64\3\FXSDRV.DLL

Microsoft Print to PDF (Default Printer)

Printer Port PORTPROMPT:
Print Processor winprint
Availability Always
Priority 1
Duplex None
Print Quality 600 * 600 dpi Color
Status Unknown

Driver

Driver Name Microsoft Print To PDF (v6.03)
Driver Path C:\Windows\System32\DriverStore\FileRepository\ntprint.inf_amd64_f9853ae82ff0dda6\Amd64\mxdwdrv.dll

Microsoft XPS Document Writer

Printer Port PORTPROMPT:
Print Processor winprint
Availability Always
Priority 1
Duplex None
Print Quality 600 * 600 dpi Color
Status Unknown

Driver

Driver Name Microsoft XPS Document Writer v4 (v6.03)
Driver Path C:\Windows\System32\DriverStore\FileRepository\ntprint.inf_amd64_f9853ae82ff0dda6\Amd64\mxdwdrv.dll

Network

You are connected to the internet

Connected through Broadcom 802.11ac Wireless PCIE Full Dongle Adapter #2
IP Address 192.168.1.41
Subnet mask 255.255.255.0
Gateway server 192.168.1.1
Preferred DNS server 192.168.1.1
DHCP Enabled
DHCP server 192.168.1.1
External IP Address 95.24.93.244
Adapter Type IEEE 802.11 wireless
NetBIOS over TCP/IP Enabled via DHCP
NETBIOS Node Type Hybrid node
Link Speed 0 Bps

Computer Name

NetBIOS Name MIPAD2
DNS Name MiPad2
Membership Part of workgroup
Workgroup WORKGROUP

Remote Desktop

Disabled

Console

State Active
Domain MIPAD2

Winlnet Info

LAN Connection
Local system uses a local area network to connect to the Internet
Local system has RAS to connect to the Internet

Wi-Fi Info

Using native Wi-Fi API version 2
Available access points count 11

Wi-Fi (Bobnet)

SSID	Bobnet
Frequency	2417000 kHz
Channel Number	2
Name	Bobnet
Signal Strength/Quality	18
Security	Enabled
State	The interface is connected to a network
Dot11 Type	Infrastructure BSS network
Network	Connectible
Network Flags	There is a profile for this network
Cipher Algorithm to be used when joining this network	AES-CCMP algorithm
Default Auth used to join this network for the first time	802.11i RSNA algorithm that uses PSK

Wi-Fi (Dom)

SSID	Dom
Frequency	2412000 kHz
Channel Number	1
Name	Dom
Signal Strength/Quality	72
Security	Enabled
State	The interface is connected to a network
Dot11 Type	Infrastructure BSS network
Network	Connectible
Network Flags	There is a profile for this network
Cipher Algorithm to be used when joining this network	AES-CCMP algorithm
Default Auth used to join this network for the first time	802.11i RSNA algorithm that uses PSK

Wi-Fi (Keenetic-8946)

SSID	Keenetic-8946
------	---------------

Frequency	2452000 kHz
Channel Number	9
Name	Keenetic-8946
Signal Strength/Quality	60
Security	Enabled
State	The interface is connected to a network
Dot11 Type	Infrastructure BSS network
Network	Connectible
Network Flags	There is a profile for this network
Cipher Algorithm to be used when joining this network	AES-CCMP algorithm
Default Auth used to join this network for the first time	802.11i RSNA algorithm that uses PSK
Wi-Fi (Keenetic-8946-5G)	
SSID	Keenetic-8946-5G
Frequency	5180000 kHz
Channel Number	36
Name	Keenetic-8946-5G
Signal Strength/Quality	4
Security	Enabled
State	The interface is connected to a network
Dot11 Type	Infrastructure BSS network
Network	Connectible
Network Flags	There is a profile for this network
Cipher Algorithm to be used when joining this network	AES-CCMP algorithm
Default Auth used to join this network for the first time	802.11i RSNA algorithm that uses PSK
Wi-Fi (Lazer)	
SSID	Lazer
Frequency	2442000 kHz
Channel Number	7
Name	Lazer
Signal Strength/Quality	72
Security	Enabled
State	The interface is connected to a network
Dot11 Type	Infrastructure BSS network
Network	Connectible
Network Flags	Currently Connected to this network
Cipher Algorithm to be used when joining this network	AES-CCMP algorithm
Default Auth used to join this network for the first time	802.11i RSNA algorithm that uses PSK
Wi-Fi (Maria)	
SSID	Maria
Frequency	2427000 kHz
Channel Number	4

Name	Maria
Signal Strength/Quality	68
Security	Enabled
State	The interface is connected to a network
Dot11 Type	Infrastructure BSS network
Network	Connectible
Network Flags	There is a profile for this network
Cipher Algorithm to be used when joining this network	AES-CCMP algorithm
Default Auth used to join this network for the first time	802.11i RSNA algorithm that uses PSK
Wi-Fi (MegaBoris78)	
SSID	MegaBoris78
Frequency	2437000 kHz
Channel Number	6
Name	MegaBoris78
Signal Strength/Quality	14
Security	Enabled
State	The interface is connected to a network
Dot11 Type	Infrastructure BSS network
Network	Connectible
Network Flags	There is a profile for this network
Cipher Algorithm to be used when joining this network	AES-CCMP algorithm
Default Auth used to join this network for the first time	802.11i RSNA algorithm that uses PSK
Wi-Fi (TheShowMustGoOn)	
SSID	TheShowMustGoOn
Frequency	2447000 kHz
Channel Number	8
Name	TheShowMustGoOn
Signal Strength/Quality	0
Security	Enabled
State	The interface is connected to a network
Dot11 Type	Infrastructure BSS network
Network	Connectible
Network Flags	There is a profile for this network
Cipher Algorithm to be used when joining this network	AES-CCMP algorithm
Default Auth used to join this network for the first time	802.11i RSNA algorithm that uses PSK
Wi-Fi (default)	
SSID	default
Frequency	2447000 kHz
Channel Number	8
Name	default
Signal Strength/Quality	14

Security State	Enabled
Dot11 Type Network	The interface is connected to a network
Network Flags	Infrastructure BSS network
Cipher Algorithm to be used when joining this network	Connectible
Default Auth used to join this network for the first time	There is a profile for this network
	AES-CCMP algorithm
	802.11i RSNA algorithm that uses PSK

Wi-Fi (interzet119)

SSID	interzet119
Frequency	2412000 kHz
Channel Number	1
Name	interzet119
Signal Strength/Quality	4
Security State	Enabled
Dot11 Type Network	The interface is connected to a network
Network Flags	Infrastructure BSS network
Cipher Algorithm to be used when joining this network	Connectible
Default Auth used to join this network for the first time	There is a profile for this network
	AES-CCMP algorithm
	802.11i RSNA algorithm that uses PSK

Wi-Fi (izhome127)

SSID	izhome127
Frequency	2462000 kHz
Channel Number	11
Name	izhome127
Signal Strength/Quality	4
Security State	Enabled
Dot11 Type Network	The interface is connected to a network
Network Flags	Infrastructure BSS network
Cipher Algorithm to be used when joining this network	Connectible
Default Auth used to join this network for the first time	There is a profile for this network
	AES-CCMP algorithm
	802.11i RSNA algorithm that uses PSK

WinHTTPInfo

WinHTTPSessionProxyType	No proxy
Session Proxy	
Session Proxy Bypass	
Connect Retries	5
Connect Timeout (ms)	60,000
HTTP Version	HTTP 1.1
Max Connects Per 1.0 Servers	INFINITE

Max Connects Per Servers	INFINITE
Max HTTP automatic redirects	10
Max HTTP status continue	10
Send Timeout (ms)	30,000
IEProxy Auto Detect	Yes
IEProxy Auto Config	
IEProxy	
IEProxy Bypass	
Default Proxy Config Access Type	No proxy
Default Config Proxy	
Default Config Proxy Bypass	

Sharing and Discovery

Network Discovery	Disabled
File and Printer Sharing	Disabled
File and printer sharing service	Enabled
Simple File Sharing	Enabled
Administrative Shares	Enabled
Network access: Sharing and security model for local accounts	Classic - local users authenticate as themselves

Adapters List

Enabled

Broadcom 802.11ac Wireless PCIE Full Dongle Adapter #2

Connection Name	Wi-Fi 2
NetBIOS over TCPIP	Yes
DHCP enabled	Yes
MAC Address	64-CC-2E-29-DA-B0
IP Address	192.168.1.41
Subnet mask	255.255.255.0
Gateway server	192.168.1.1
DHCP	192.168.1.1
DNS Server	192.168.1.1

Network Shares

No network shares

Current TCP Connections

C:\Windows\explorer.exe (3972)

Local	ESTABLISHED Remote 111.221.29.113:443 (Querying...)
192.168.1.41:49410	(HTTPS)
Local	ESTABLISHED Remote 111.221.29.168:443 (Querying...)
192.168.1.41:49412	(HTTPS)

C:\Windows\SystemApps\Microsoft.MicrosoftEdge_8wekyb3d8bbwe\MicrosoftEdgeCP.exe (5300)

Local	CLOSE-WAIT Remote 74.125.232.247:443 (Querying...)
192.168.1.41:50718	(HTTPS)
Local	ESTABLISHED Remote 151.101.36.64:443 (Querying...)
192.168.1.41:50721	(HTTPS)
Local	CLOSE-WAIT Remote 64.233.164.95:443 (Querying...)
192.168.1.41:50727	(HTTPS)
Local	CLOSE-WAIT Remote 64.233.164.95:443 (Querying...)
192.168.1.41:50730	(HTTPS)

Local	CLOSE-WAIT Remote 198.232.125.83:443 (Querying...)
192.168.1.41:50734	(HTTPS)
Local	CLOSE-WAIT Remote 173.194.32.191:443 (Querying...)
192.168.1.41:50736	(HTTPS)
Local	CLOSE-WAIT Remote 173.194.32.191:443 (Querying...)
192.168.1.41:50737	(HTTPS)
Local	CLOSE-WAIT Remote 173.194.32.191:443 (Querying...)
192.168.1.41:50738	(HTTPS)
Local	CLOSE-WAIT Remote 173.194.32.142:443 (Querying...)
192.168.1.41:50739	(HTTPS)
Local	CLOSE-WAIT Remote 159.8.86.228:443 (Querying...)
192.168.1.41:50741	(HTTPS)
Local	CLOSE-WAIT Remote 159.8.86.228:443 (Querying...)
192.168.1.41:50742	(HTTPS)
Local	CLOSE-WAIT Remote 23.63.234.41:443 (Querying...)
192.168.1.41:50743	(HTTPS)
Local	CLOSE-WAIT Remote 23.63.234.41:443 (Querying...)
192.168.1.41:50744	(HTTPS)
Local	CLOSE-WAIT Remote 173.194.44.94:443 (Querying...)
192.168.1.41:50745	(HTTPS)
Local	CLOSE-WAIT Remote 173.194.44.94:443 (Querying...)
192.168.1.41:50746	(HTTPS)
Local	CLOSE-WAIT Remote 108.161.188.192:443 (Querying...)
192.168.1.41:50747	(HTTPS)
Local	CLOSE-WAIT Remote 108.161.188.192:443 (Querying...)
192.168.1.41:50748	(HTTPS)
Local	CLOSE-WAIT Remote 64.233.162.155:443 (Querying...)
192.168.1.41:50752	(HTTPS)
Local	CLOSE-WAIT Remote 64.233.162.155:443 (Querying...)
192.168.1.41:50753	(HTTPS)
Local	CLOSE-WAIT Remote 159.122.19.205:443 (Querying...)
192.168.1.41:50762	(HTTPS)
Local	CLOSE-WAIT Remote 159.122.19.205:443 (Querying...)
192.168.1.41:50763	(HTTPS)
Local	CLOSE-WAIT Remote 173.194.32.151:443 (Querying...)
192.168.1.41:50766	(HTTPS)
Local	CLOSE-WAIT Remote 173.194.32.151:443 (Querying...)
192.168.1.41:50767	(HTTPS)
Local	ESTABLISHED Remote 151.101.36.64:443 (Querying...)
192.168.1.41:50805	(HTTPS)
Local	ESTABLISHED Remote 151.101.36.64:443 (Querying...)
192.168.1.41:50806	(HTTPS)
Local	ESTABLISHED Remote 151.101.36.64:443 (Querying...)
192.168.1.41:50807	(HTTPS)
Local	ESTABLISHED Remote 151.101.36.64:443 (Querying...)
192.168.1.41:50808	(HTTPS)
Local	ESTABLISHED Remote 151.101.36.64:443 (Querying...)
192.168.1.41:50809	(HTTPS)
Local	CLOSE-WAIT Remote 173.194.122.244:443 (Querying...)
192.168.1.41:50810	(HTTPS)

Local 192.168.1.41:50811 CLOSE-WAIT Remote 173.194.122.244:443 (Querying...) (HTTPS)

Local 192.168.1.41:50812 CLOSE-WAIT Remote 31.13.92.14:443 (Querying...) (HTTPS)

Local 192.168.1.41:50813 CLOSE-WAIT Remote 31.13.92.14:443 (Querying...) (HTTPS)

Local 192.168.1.41:50814 CLOSE-WAIT Remote 93.184.220.66:443 (Querying...) (HTTPS)

Local 192.168.1.41:50815 CLOSE-WAIT Remote 93.184.220.66:443 (Querying...) (HTTPS)

Local 192.168.1.41:50818 CLOSE-WAIT Remote 31.13.91.36:443 (Querying...) (HTTPS)

Local 192.168.1.41:50819 CLOSE-WAIT Remote 31.13.91.36:443 (Querying...) (HTTPS)

Local 192.168.1.41:50821 CLOSE-WAIT Remote 178.162.208.180:443 (Querying...) (HTTPS)

Local 192.168.1.41:50822 CLOSE-WAIT Remote 104.244.43.209:443 (Querying...) (HTTPS)

Local 192.168.1.41:50823 CLOSE-WAIT Remote 104.244.43.209:443 (Querying...) (HTTPS)

Local 192.168.1.41:50824 CLOSE-WAIT Remote 54.240.184.59:80 (Querying...) (HTTP)

Local 192.168.1.41:50825 CLOSE-WAIT Remote 54.240.184.59:80 (Querying...) (HTTP)

Local 192.168.1.41:50827 CLOSE-WAIT Remote 104.244.42.136:443 (Querying...) (HTTPS)

Local 192.168.1.41:50828 ESTABLISHED Remote 104.244.42.136:443 (Querying...) (HTTPS)

Local 192.168.1.41:50717 CLOSE-WAIT Remote 74.125.232.247:443 (Querying...) (HTTPS)

C:\Windows\SystemApps\Microsoft.MicrosoftEdge_8wekyb3d8bbwe\MicrosoftEdgeCP.exe (6552)

Local 192.168.1.41:50863 CLOSE-WAIT Remote 74.201.198.77:443 (Querying...) (HTTPS)

lsass.exe (740)

Local 0.0.0.0:49670 LISTEN

services.exe (728)

Local 0.0.0.0:49668 LISTEN

spoolsv.exe (1616)

Local 0.0.0.0:49667 LISTEN

svchost.exe (584)

Local 0.0.0.0:7680 LISTEN

Local 0.0.0.0:49665 LISTEN

svchost.exe (724)

Local 0.0.0.0:49666 LISTEN

svchost.exe (984)

Local 0.0.0.0:135 (DCE) LISTEN

System Process

Local 192.168.1.41:50861 TIME-WAIT Remote 191.237.208.126:443 (Querying...) (HTTPS)

System Process

Local 0.0.0.0:445 (Windows shares) LISTEN

Local 192.168.1.41:139 (NetBIOS session service) LISTEN

wininit.exe (656)

Local 0.0.0.0:49664 LISTEN