

```
Administrator: Command Prompt

Intel(R) MEInfo Version: 11.8.81.3781
Copyright(C) 2005 - 2020, Intel Corporation. All rights reserved.

Windows OS Version : 10.0

FW Status Register1: 0x90000245
FW Status Register2: 0x00F60506
FW Status Register3: 0x00000030
FW Status Register4: 0x00684000
FW Status Register5: 0x00001F01
FW Status Register6: 0xC7C00BC9

CurrentState: Normal
ManufacturingMode: Disabled
FlashPartition: Valid
OperationalState: CM0 with UMA
InitComplete: Complete
BUPLoadState: Success
ErrorCode: No Error
ModeOfOperation: Normal
SPI Flash Log: Not Present
FPF HW Source value: Original FPF HW Fuse Bank
ME FPF Fusing Patch Status: ME FPF Fusing patch NOT required
Phase: ROM/Preboot
ICC: Valid OEM data, ICC programmed
ME File System Corrupted: No
PhaseStatus: AFTER_SRAM_INIT
FPF and ME Config Status: No match

FW Capabilities value is 0x7930124C
Feature enablement is 0x5930124C
Platform type is 0x41135421
No Intel Wireless device was found
Intel(R) Manageability and Security Application code versions:

Table Type 85 ( 0x 55 ) found, size of 0 (0x 00 ) bytes
BIOS Version 1.21.0
Table Type 85 ( 0x 55 ) found, size of 0 (0x 00 ) bytes
Table Type 0 ( 0x 00 ) found, size of 53 (0x 35 ) bytes
Table Type 1 ( 0x 01 ) found, size of 74 (0x 4A ) bytes
Table Type 2 ( 0x 02 ) found, size of 62 (0x 3E ) bytes
Table Type 3 ( 0x 03 ) found, size of 53 (0x 35 ) bytes
```

```
Administrator: Command Prompt
Feature enablement is 0x5930124C
Platform type is 0x41135421
No Intel Wireless device was found
Intel(R) Manageability and Security Application code versions:

Table Type 85 ( 0x 55 ) found, size of 0 (0x 00 ) bytes
BIOS Version 1.21.0
Table Type 85 ( 0x 55 ) found, size of 0 (0x 00 ) bytes
Table Type 0 ( 0x 00 ) found, size of 53 (0x 35 ) bytes
Table Type 1 ( 0x 01 ) found, size of 74 (0x 4A ) bytes
Table Type 2 ( 0x 02 ) found, size of 62 (0x 3E ) bytes
Table Type 3 ( 0x 03 ) found, size of 53 (0x 35 ) bytes
Table Type 8 ( 0x 08 ) found, size of 30 (0x 1E ) bytes
Table Type 9 ( 0x 09 ) found, size of 23 (0x 17 ) bytes
Table Type 10 ( 0x 0A ) found, size of 27 (0x 1B ) bytes
Table Type 11 ( 0x 0B ) found, size of 78 (0x 4E ) bytes
Table Type 12 ( 0x 0C ) found, size of 21 (0x 15 ) bytes
Table Type 15 ( 0x 0F ) found, size of 37 (0x 25 ) bytes
Table Type 21 ( 0x 15 ) found, size of 9 (0x 09 ) bytes
Table Type 25 ( 0x 19 ) found, size of 11 (0x 0B ) bytes
Table Type 32 ( 0x 20 ) found, size of 22 (0x 16 ) bytes
Table Type 34 ( 0x 22 ) found, size of 19 (0x 13 ) bytes
Table Type 36 ( 0x 24 ) found, size of 18 (0x 12 ) bytes
Table Type 41 ( 0x 29 ) found, size of 26 (0x 1A ) bytes
Table Type 255 ( 0x FF ) found, size of 53 (0x 35 ) bytes
Table Type 16 ( 0x 10 ) found, size of 25 (0x 19 ) bytes
Table Type 17 ( 0x 11 ) found, size of 76 (0x 4C ) bytes
Table Type 19 ( 0x 13 ) found, size of 33 (0x 21 ) bytes
Table Type 7 ( 0x 07 ) found, size of 29 (0x 1D ) bytes
Table Type 4 ( 0x 04 ) found, size of 185 (0x B9 ) bytes
Table Type 20 ( 0x 14 ) found, size of 37 (0x 25 ) bytes
Table Type 126 ( 0x 7E ) found, size of 57 (0x 39 ) bytes
Table Type 22 ( 0x 16 ) found, size of 121 (0x 79 ) bytes
Table Type 27 ( 0x 1B ) found, size of 24 (0x 18 ) bytes
Table Type 28 ( 0x 1C ) found, size of 35 (0x 23 ) bytes
Table Type 177 ( 0x B1 ) found, size of 14 (0x 0E ) bytes
Table Type 178 ( 0x B2 ) found, size of 126 (0x 7E ) bytes
Table Type 208 ( 0x D0 ) found, size of 18 (0x 12 ) bytes
Table Type 216 ( 0x D8 ) found, size of 31 (0x 1F ) bytes
Table Type 217 ( 0x D9 ) found, size of 28 (0x 1C ) bytes
Table Type 218 ( 0x DA ) found, size of 253 (0x FD ) bytes
Table Type 218 ( 0x DA ) found, size of 109 (0x 6D ) bytes
Table Type 218 ( 0x DA ) found, size of 79 (0x 4F ) bytes
Table Type 220 ( 0x DC ) found, size of 24 (0x 18 ) bytes
Table Type 221 ( 0x DD ) found, size of 21 (0x 15 ) bytes
```



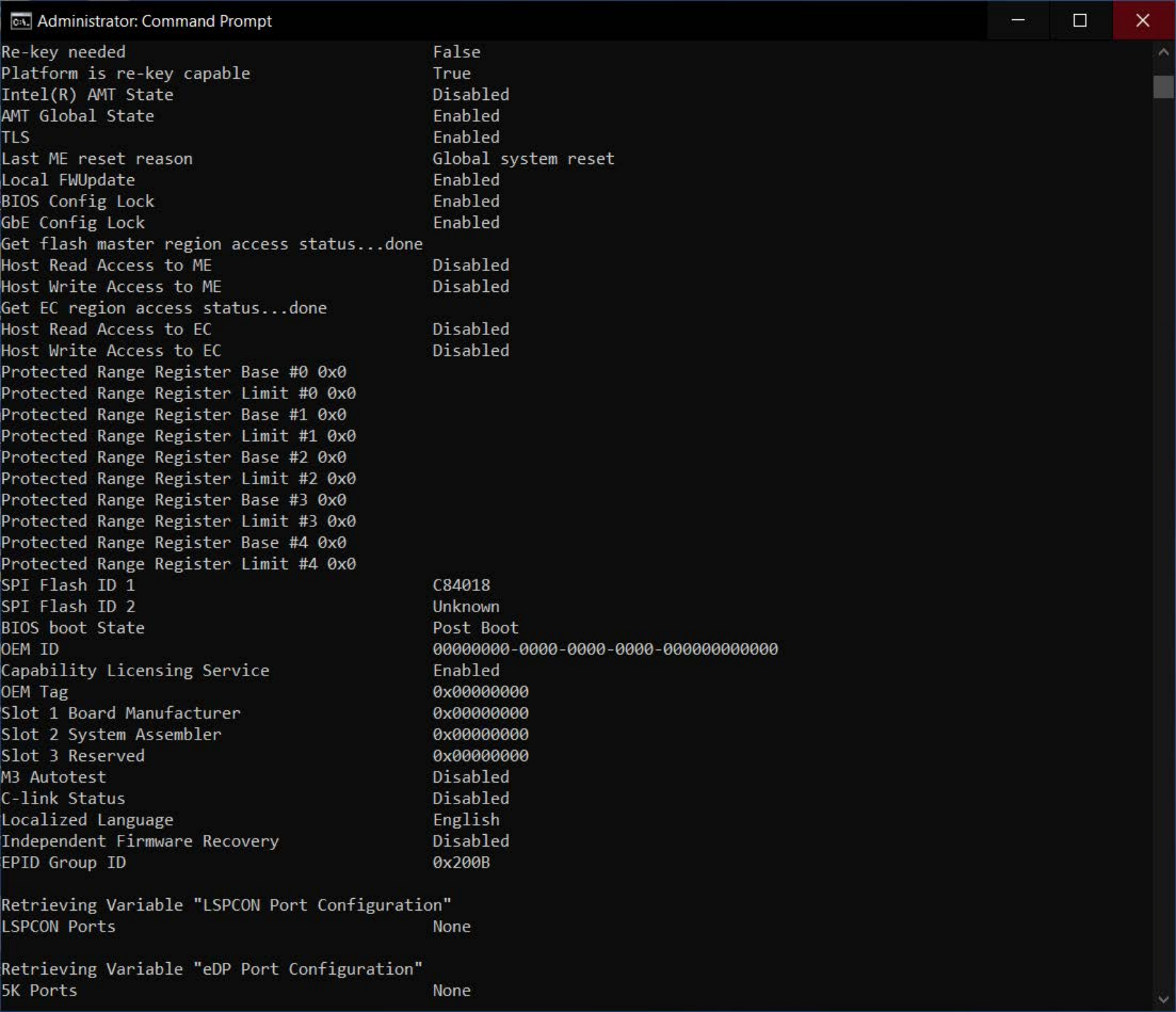
```
Administrator: Command Prompt

Table Type 218 ( 0x DA ) found, size of 79 (0x 4F ) bytes
Table Type 220 ( 0x DC ) found, size of 24 (0x 18 ) bytes
Table Type 221 ( 0x DD ) found, size of 21 (0x 15 ) bytes
Table Type 222 ( 0x DE ) found, size of 18 (0x 12 ) bytes
Table Type 130 ( 0x 82 ) found, size of 22 (0x 16 ) bytes
MEBx Version 11.0.0.0010
GbE Version Unknown
Vendor ID 8086
PCH Version 21
FW Version 11.8.81.3781 LP
Security Version (SVN) 3
LMS Version 2026.14.0.1682
MEI Driver Version 2040.100.0.1029

FW Capabilities 0x7930124C

Intel(R) Small Business Technology - PRESENT/ENABLED
Intel(R) Capability Licensing Service - PRESENT/ENABLED
Protect Audio Video Path - PRESENT/ENABLED
Intel(R) Dynamic Application Loader - PRESENT/ENABLED
Service Advertisement & Discovery - PRESENT/ENABLED
Intel(R) NFC Capabilities - NOT PRESENT
Intel(R) Platform Trust Technology - PRESENT/DISABLED

Re-key needed False
Platform is re-key capable True
Intel(R) AMT State Disabled
AMT Global State Enabled
TLS Enabled
Last ME reset reason Global system reset
Local FWUpdate Enabled
BIOS Config Lock Enabled
GbE Config Lock Enabled
Get flash master region access status...done
Host Read Access to ME Disabled
Host Write Access to ME Disabled
Get EC region access status...done
Host Read Access to EC Disabled
Host Write Access to EC Disabled
Protected Range Register Base #0 0x0
Protected Range Register Limit #0 0x0
Protected Range Register Base #1 0x0
Protected Range Register Limit #1 0x0
Protected Range Register Base #2 0x0
Protected Range Register Limit #2 0x0
```



```
Re-key needed                False
Platform is re-key capable   True
Intel(R) AMT State           Disabled
AMT Global State             Enabled
TLS                           Enabled
Last ME reset reason         Global system reset
Local FWUpdate               Enabled
BIOS Config Lock             Enabled
GbE Config Lock              Enabled
Get flash master region access status...done
Host Read Access to ME       Disabled
Host Write Access to ME      Disabled
Get EC region access status...done
Host Read Access to EC       Disabled
Host Write Access to EC      Disabled
Protected Range Register Base #0 0x0
Protected Range Register Limit #0 0x0
Protected Range Register Base #1 0x0
Protected Range Register Limit #1 0x0
Protected Range Register Base #2 0x0
Protected Range Register Limit #2 0x0
Protected Range Register Base #3 0x0
Protected Range Register Limit #3 0x0
Protected Range Register Base #4 0x0
Protected Range Register Limit #4 0x0
SPI Flash ID 1               C84018
SPI Flash ID 2               Unknown
BIOS boot State              Post Boot
OEM ID                       00000000-0000-0000-0000-000000000000
Capability Licensing Service  Enabled
OEM Tag                      0x00000000
Slot 1 Board Manufacturer    0x00000000
Slot 2 System Assembler      0x00000000
Slot 3 Reserved              0x00000000
M3 Autotest                  Disabled
C-link Status                Disabled
Localized Language            English
Independent Firmware Recovery Disabled
EPID Group ID                0x200B

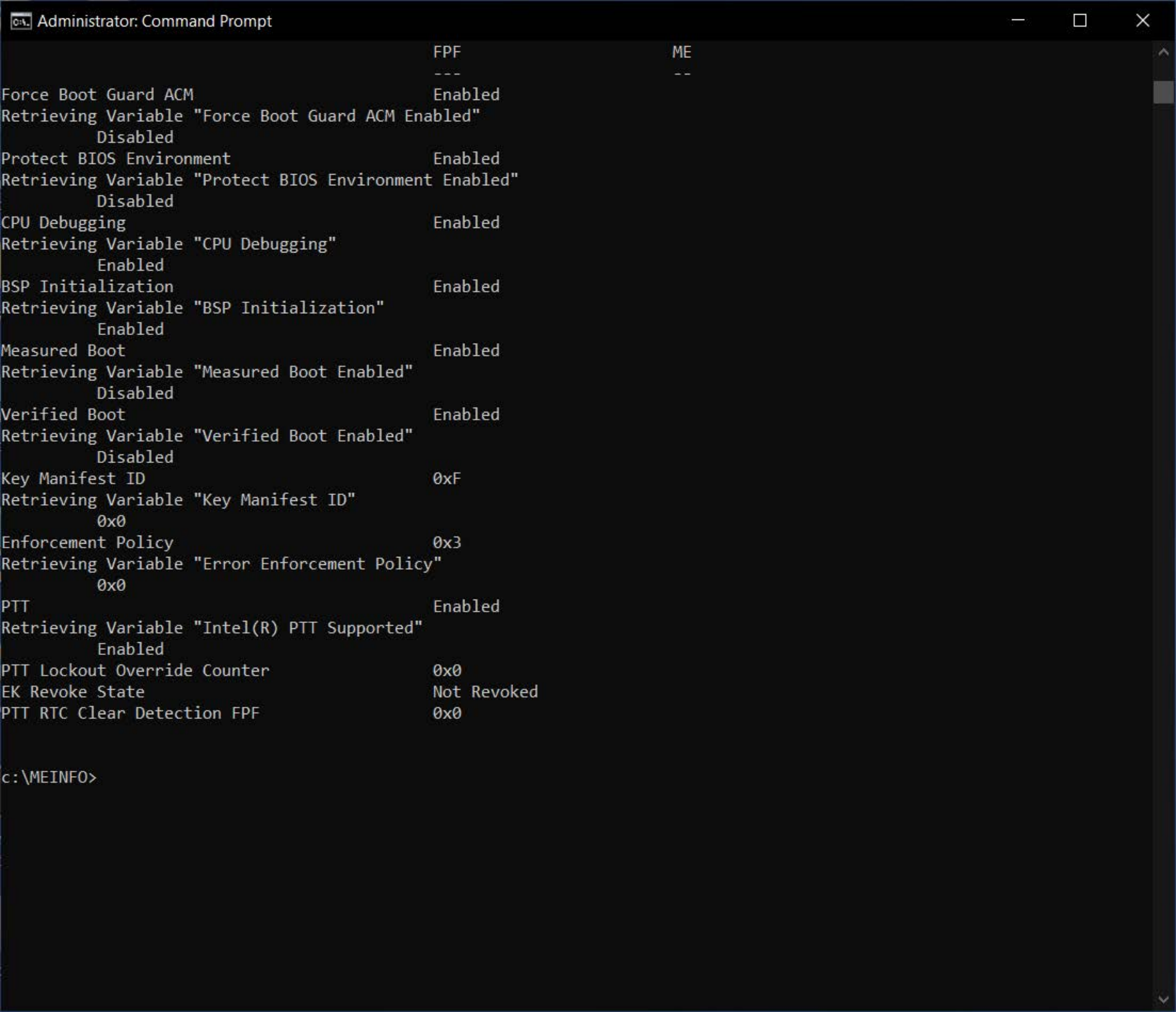
Retrieving Variable "LSPCON Port Configuration"
LSPCON Ports                  None

Retrieving Variable "eDP Port Configuration"
5K Ports                      None
```



1

10



	FPF	ME
	---	--
Force Boot Guard ACM	Enabled	
Retrieving Variable "Force Boot Guard ACM Enabled"	Disabled	
Protect BIOS Environment	Enabled	
Retrieving Variable "Protect BIOS Environment Enabled"	Disabled	
CPU Debugging	Enabled	
Retrieving Variable "CPU Debugging"	Enabled	
BSP Initialization	Enabled	
Retrieving Variable "BSP Initialization"	Enabled	
Measured Boot	Enabled	
Retrieving Variable "Measured Boot Enabled"	Disabled	
Verified Boot	Enabled	
Retrieving Variable "Verified Boot Enabled"	Disabled	
Key Manifest ID	0xF	
Retrieving Variable "Key Manifest ID"	0x0	
Enforcement Policy	0x3	
Retrieving Variable "Error Enforcement Policy"	0x0	
PTT	Enabled	
Retrieving Variable "Intel(R) PTT Supported"	Enabled	
PTT Lockout Override Counter	0x0	
EK Revoke State	Not Revoked	
PTT RTC Clear Detection FPF	0x0	

c:\MEINFO>