



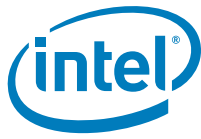
Comet Lake Platform Intel® Converged Security and Management Engine (Intel® CSME) 14.0 and Intel® Sensor Solution Corporate Firmware

Compliance and Testing Guide

Revision 1.1

April 2020

Intel Confidential



You may not use or facilitate the use of this document in connection with any infringement or other legal analysis concerning Intel products described herein. You agree to grant Intel a non-exclusive, royalty-free license to any patent claim thereafter drafted which includes subject matter disclosed herein.

No license (express or implied, by estoppel or otherwise) to any intellectual property rights is granted by this document.

Intel technologies' features and benefits depend on system configuration and may require enabled hardware, software or service activation. Learn more at Intel.com, or from the OEM or retailer.

No computer system can be absolutely secure. Intel does not assume any liability for lost or stolen data or systems or any damages resulting from such losses.

The products described may contain design defects or errors known as errata which may cause the product to deviate from published specifications. Current characterized errata are available on request.

Intel disclaims all express and implied warranties, including without limitation, the implied warranties of merchantability, fitness for a particular purpose, and non-infringement, as well as any warranty arising from course of performance, course of dealing, or usage in trade.

Intel technologies' features and benefits depend on system configuration and may require enabled hardware, software or service activation. Learn more at intel.com, or from the OEM or retailer.

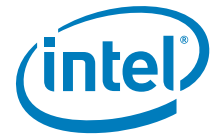
All information provided here is subject to change without notice. Contact your Intel representative to obtain the latest Intel product specifications and roadmaps.

Copies of documents which have an order number and are referenced in this document may be obtained by calling 1-800-548-4725 or visit www.intel.com/design/literature.htm.

Intel, and the Intel logo are trademarks or registered trademarks of Intel Corporation or its subsidiaries in the United States and other countries.

*Other names and brands may be claimed as the property of others.

© 2019-2020, Intel Corporation. All rights reserved.

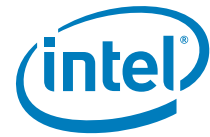


Contents

1	Introduction	15
1.1	Purpose and Scope of this Document	15
1.2	Features	15
1.3	Intel® CSME Firmware	16
1.3.1	WoWLAN or WOL Driver Feature	16
1.3.2	Windows* 8.1/10 Fast Startup (Partial Hibernate)	16
1.3.3	Environment Networking Recommendations	16
1.4	Terminology	17
1.5	Acronyms, Terminology, and Definitions	17
1.5.1	General	17
1.5.2	Intel® AMT Acronyms, Terminology, and Definitions	17
1.5.3	System States and Power Management	19
1.5.4	Wireless and Mobile	19
1.6	Reference Documents	20
1.7	External References	21
1.8	Testing Guidelines	21
1.9	Boot Guard Discrete TPM Intel® PTT	22
2	Intel® Trace Hub (Intel® TH)	23
2.1	Tools for testing:	23
2.2	Test Coverage Summary	23
2.3	Intel® CSME FW - DCI Enable (MEEN)	24
2.4	BIOS DCI Enable (HEEN)	24
2.5	BIOS DCI Enable Post EOM	25
2.6	Capture ITH BIOS/ME Tracing Via CCA	26
3	Signing, Manifesting, and Secure Tokens	28
3.1	Introduction	28
3.2	Test Environment Setup	28
3.3	Tools for Testing	28
3.4	Coverage Summary	28
3.5	Image Creation with OEM Signed Components	29
3.6	Debug Token	29
4	Intel® CSME Manufacturing Mode Compliancy — Corporate	31
4.1	Tools for Testing	31
4.2	Test Coverage Summary	31
4.3	CF9GR Locking/Unlocking	32
5	Intel® CSME BIOS Compliancy	33
5.1	Tools for Testing	33
5.2	Test Coverage Summary	33
5.3	End of Power-On Self-Test (POST)	34
5.4	CF9GR Locking/Unlocking	34
5.5	DRAM INIT Done	35
5.6	PCI SID and SVID Programming	36
5.7	Intel® MEBX Binary UI	36
5.8	Intel® CSME Temporary Disable	37
5.9	Intel® MEBX BIOS Extension Password Reset Security Mechanism	37
6	Common Services	39
6.1	Test System Configuration	39



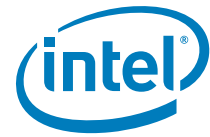
6.2	Test Coverage Summary.....	39
6.2.1	Test Environment Setup	41
6.3	Intel® AMT Wireless Network	41
6.3.1	Test Environment	41
6.3.2	Special Terminology	41
6.3.3	Intel® AMT Wireless Interface Setup	42
6.3.4	Host Control Mode Operation.....	44
6.3.5	Host Control Mode Operation without Intel® AMT Wireless Network Enabled ...	45
6.3.6	Intel® ME Control Mode Operation with Host OS	46
6.3.7	Intel® ME Control Mode Operation with BIOS.....	47
6.3.8	Intel® ME Control Mode Operation with Access Point Profile Switching.....	47
6.3.9	Intel® ME Control Mode Operation after Host Profile Synchronization	48
6.3.10	Intel® ME Control and Host Control Mode Toggle.....	49
6.3.11	Software Radio Frequency Kill (RF-Kill)	50
6.3.12	Hardware Radio Frequency Kill (RF-Kill)	51
6.3.13	Software and Hardware Radio Frequency Kill (RF-Kill)	52
6.4	Intel® ME Firmware Update and Partial Firmware Update	52
6.4.1	Tools for Testing.....	52
6.4.2	Intel® ME Firmware Update.....	53
6.4.3	Intel® ME Firmware Partition Update for Secure Output Locale.....	53
6.4.4	Intel® ME Firmware Partition Update for WLAN µCode	54
6.5	USB Key Based Configuration	55
6.5.1	Test Environment	55
6.5.2	USB Key File Version 2.1 with Consumable Record	55
6.5.3	USB Key File Version 2.1 with Non-Consumable Record.....	56
6.5.4	USB Key File Version 3 with Consumable Record	58
6.5.5	USB Key File Version 4 with Consumable Record	59
6.5.6	USB Key File with Multiple Consumable Records	61
6.5.7	USB Key File Configuration Process Cancellation.....	62
6.5.8	USB Key Drive Compliancy.....	63
6.5.9	USB Key File Configuration Disabled at Factory Default	65
6.6	Remote and Host Based Configuration	66
6.6.1	Test Environment	66
6.6.2	Remote Configuration Support.....	66
6.6.3	Hosted Based Configuration Support	67
6.6.4	Embedded Host Based Configuration Support	67
7	SPI Flash Interface	69
7.1	Overview	69
7.2	Tools for Testing	69
7.3	Test Environment.....	69
7.4	Test Coverage Summary.....	70
7.5	Descriptor Mode Test	70
7.6	Serial Flash Discoverable Parameter Test	70
7.7	4 Kbytes Erasable Blocks Test	71
7.8	SPI Flash Size Test	72
7.9	SPI Flash Vendor Specific Capabilities (VSCC) Test	73
7.10	Flash Descriptor Security Override Test.....	74
7.11	Serial Flash Single Input, Dual, or Quad Output Fast Read Test.....	74
8	Intel® CSME Resiliency Compliancy	76
8.1	Layout Overview with Boot Critical Redundancy	76
8.1.1	Layout Pointers	77
8.1.2	BPDT	77
8.1.3	High-Level Flow	79
8.1.4	Firmware Status (FWSTS1) Register Indication Scenarios	79



8.2	Test Environment	80
8.3	Test Coverage Summary	80
8.4	Boot Critical Redundancy Enabled	80
8.5	Critical Code Corruption - BPDT1	81
8.6	Critical Code Corruption - BUP	82
8.7	Critical Code Corruption - PMC	83
8.8	Critical Code Corruption - TypeC	84
8.9 Recovery of Corrupted Primary Boot Critical (BC1) Partition	85
9	Enhanced Serial Peripheral Interface (eSPI)	86
9.1	Introduction	86
9.2	Test Environment Setup	86
9.3	Tools for Testing	86
9.4	Test Coverage Summary	86
9.5	Bootting with MAF Configurations (Straps Set to MAF Defaults)	87
9.6	Platform Boots with EC Region	87
9.7	Platform Boots with EC Region in Different Place	88
9.8	Platform Boots without EC Region	88
9.9	IFWI with Empty EC Region	88
9.10	IFWI with Empty EC Binary	89
9.11	Platform Boots with Default EC Region Permissions	89
9.12	Platform Boots with EC Read-Only Permission to BIOS Region	90
9.13	Platform Boots with EC Read-Only Permission to BIOS Region and BIOS with RW Permissions to EC	90
9.14	Perform FWUpdate with MAF Configurations	91
10	Intel® CSME Power Management for Corporate Designs—Stress Testing	92
10.1	System Power States	92
10.2	Test Environment and System Configuration	92
10.2.1	Test Parameters	92
10.2.2	Tools for Testing	93
10.2.3	Test Environment Setup	94
10.2.4	Test Step Execution and Verification	94
10.2.5	Setup Environment Tests	95
10.3	Test Coverage Summary	95
10.4	PM_ST_1 - S5/CM3 to G3 to S5/CM3 via Power Cycle (DOS/UEFI)	97
10.5	PM_ST_2 - Remote Power Cycle S0/CM0 (DOS/UEFI)	97
10.6	PM_ST_3 - Remote Reset S0/CM0 (DOS/UEFI)	98
10.7	PM_ST_4 - S3/CM3 to S3/CM-Off to S3/CM3 via AC-detach/Attach	99
10.8	PM_ST_5 - S0/CM0 to S3/CM-Off to S0/CM0 via Suspend/Resume	101
10.9	PM_ST_6 - S0/CM0 to S3/CM3 to S0/CM0 via Suspend/Resume	102
10.10	PM_ST_7 - S0/CM0 to S5/CM3 to S0/CM0 via Power Button Override (DOS/UEFI)	103
10.11	PM_ST_8 - S0/CM0 to S4/CM-Off to S0/CM0 via Hibernate and WoL/WoWLAN	103
10.12	PM_ST_9 - S0/CM0 to S4/CM3 to S0/CM0 via Hibernate and Remote Power-Up	105
10.13	PM_ST_10 - S0/CM0 to S5/CM-Off to S0/CM0 via Shutdown and Power Button Press	106
10.14	PM_ST_11 - S0/CM0 to S5/CM3 to S0/CM0 via Shutdown and Remote Power-Up	108
10.15	PM_ST_12 - S3/CM3 to S3/CM-Off to S3/CM3 via Intel® AMT Idle Timeout and Intel® AMT Network Access	110
10.16	PM_ST_13 - S0/CM0 to S3/CM3 to S0/CM0 via Suspend and Remote Power-Up	111
10.17	PM_ST_14 - S0/CM0 to S3/CM-Off to S0/CM0 via Suspend and Power Button Press	112
10.18	PM_ST_16 - Remote Power Cycle S0/CM0 (DOS/UEFI)	114
10.19	PM_ST_17 - Remote Reset S0/CM0 (DOS/UEFI)	114
10.20	PM_ST_18 - S5/CM3 to S5/CM-Off to S5/CM3 via AC-detach/Attach	116
10.21	PM_ST_19 - S5/CM3 to S5/CM-Off to S5/CM3 via Intel® AMT Idle Timeout and Intel® AMT Network Access	117
10.22	PM_ST_20 - S0/CM0 to S3/CM3 to S0/CM0 via AC Attach	118



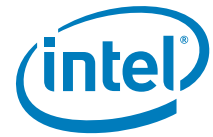
10.23	PM_ST_21 - S0/CM0 to S4/CM3 to S0/CM0 via AC-Attach	119
10.24	PM_ST_22 - S0/CM0 to S5/CM3 to S0/CM0 via AC Attach.....	120
10.25	PM_ST_23 - S0/CM0 to S3/CM-Off to S0/CM0 via AC Attach	121
10.26	PM_ST_24 - S0/CM0 to S4/CM-Off to S0/CM0 via AC Attach	122
10.27	PM_ST_25 - S0/CM0 to S5/CM-Off to S0/CM0 via AC Attach	123
10.28	PM_ST_26 - S0/CM0 to S3/CM-Off to S0/CM0 via AC Attach	124
10.29	PM_ST_27 - S0/CM0 to S4/CM-Off to S0/CM0 via AC Attach	125
10.30	PM_ST_28 - S0/CM0 to S5/CM-Off to S0/CM0 via AC Attach	126
10.31	PM_ST_29 - S0/CM0 to S3/CM-Off to S0/CM0 via AC Detach	127
10.32	PM_ST_30 - S0/CM0 to S4/CM-Off to S0/CM0 via AC Detach	128
10.33	PM_ST_31 - S0/CM0 to S5/CM-Off to S0/CM0 via AC Detach	129
10.34	PM_ST_32 - S0/CM0 to S3/CM-Off to S0/CM0 via AC Detach	130
10.35	PM_ST_33 - S0/CM0 to S4/CM-Off to S0/CM0 via AC Detach	131
10.36	PM_ST_34 - S0/CM0 to S5/CM-Off to S0/CM0 via AC Detach	132
11	Intel® AMT Tests.....	133
11.1	AMT Over Different LAN Solutions	133
11.2	Test System Power Model	134
11.3	Test Coverage Summary.....	135
11.3.1	Test Environment Setup	138
11.3.2	Setup Environment Tests	139
11.4	BIOS Tables.....	141
11.4.1	Test Environment	141
11.4.2	SMBIOS Table Generation	141
11.4.3	ASF Table Generation	143
11.5	Boot Options, Platform Event Traps, Hardware Assets, and Boot Audit Entry	144
11.5.1	Test Environment	144
11.5.2	BIOS Boot Option Read and Clear	145
11.5.3	PET Boot Progress Event Support	146
11.5.4	BIOS Hardware Asset Table Update.....	147
11.5.5	BAE PET Support	148
11.5.6	BAE PET Support with Alternate Boot Device	149
11.6	Remote Power Control.....	150
11.6.1	Test Environment	150
11.6.2	Remote Power Control via Intel® AMT LAN Network Interface for Mobile Systems 151	
11.6.3	Remote Power Control via Intel® AMT WLAN Network Interface for Mobile Systems	153
11.6.4	Remote Power Control via Intel® AMT LAN Network Interface for Non-Mobile Systems	155
11.6.5	Remote Power Control via Intel® AMT WLAN Network Interface for Non-Mobile Systems	157
11.6.6	Remote Power Control in S0 Low Power Idle State via Intel® AMT LAN Network Interface	159
11.6.7	Remote Power Control with S0 Low Power Idle via Intel® AMT WLAN Network Interface	160
11.6.8	Remote Power Control via Intel® AMT WLAN Network Interface for Mobile Systems Supporting Wake On Wireless LAN	161
11.6.9	Remote Power Control via Intel® AMT WLAN Network Interface for Non-Mobile Systems Supporting Wake On Wireless LAN	163
11.6.10	Remote Power Control with Host OS Interaction via Intel® AMT LAN Network Interface	165
11.6.11	Remote Power Control with Host OS Interaction via Intel® AMT WLAN Network Interface	167
11.7	Serial-Over-LAN and Storage Redirection	169
11.7.1	Test Environment	169



11.7.2	SOL Redirection and BIOS Setup Boot Option over Intel® AMT LAN	170
11.7.3	SOL Redirection and BIOS Setup Boot Option over Intel® AMT WLAN Network Interface	171
11.7.4	SOL and Storage Redirection over Intel® AMT LAN Network Interface	172
11.7.5	SOL and Storage Redirection over Intel® AMT WLAN Network Interface	174
11.7.6	SOL and Storage Redirection over Intel® AMT LAN Network Interface with User Consent Enabled	175
11.7.7	SOL and Storage Redirection over Intel® AMT WLAN Network Interface with User Consent Enabled	176
11.7.8	SOL and Storage Redirection with Secure Boot	178
11.7.9	SOL Character Interpretation	180
11.7.10	SOL Redirection during System Restart	181
11.8	Keyboard, Video, and Mouse (KVM) Redirection	182
11.8.1	Test Environment	182
11.8.2	KVM Redirection and BIOS Setup Boot Option over Intel® AMT LAN Network Interface	183
11.8.3	KVM Redirection and BIOS Setup Boot Option over Intel® AMT WLAN Network Interface	184
11.8.4	KVM Redirection over Intel® AMT LAN Network Interface	186
11.8.5	KVM Redirection over Intel® AMT WLAN Network Interface	188
11.8.6	KVM Redirection over Intel® AMT LAN Network Interface with User Consent Enabled	191
11.8.7	KVM Redirection over Intel® AMT WLAN Network Interface with User Consent Enabled	193
11.8.8	KVM Redirection during Warm Reset over Intel® AMT LAN Network Interface	196
11.8.9	KVM Redirection during Warm Reset over Intel® AMT WLAN Network Interface	198
11.8.10	KVM Redirection with S0 Low Power Idle via Intel® AMT LAN Network Interface	199
11.8.11	KVM Redirection with S0 Low Power Idle via Intel® AMT WLAN Network Interface	200
11.8.12	KVM Redirection in Discrete Graphics Mode	201
11.8.13	KVM Redirection and Switchable Graphics	202
11.8.14	KVM with SOL and Storage Redirection	203
11.8.15	KVM Redirection and USB Port Availability Check	204
11.8.16	KVM Redirection with Remote Screen Blank (RSB) Support	206
11.8.17	KVM Redirection with S0 Low Power Idle and Intel® ME Power Gating	207
11.8.18	KVM Redirection over Intel® AMT WLAN Network Interface for Systems Supporting Wake On Wireless LAN	208
11.8.19	KVM Redirection on Headless Configurations	209
11.9	Remote Access (Fast Call for Help)	212
11.9.1	Test Environment	212
11.9.2	Fast Call for Help During System Boot	212
11.9.3	Fast Call for Help During System Boot (End-to-End)	213
11.10	Settings, Storage, and Security Configuration	230
11.10.1	Test Environment	230
11.10.2	General Settings Information	230
11.10.3	Security Administration Realm Interface	231
11.10.4	Transport Layer Security (TLS) Authentication	231
11.10.5	Wake By Means of an Alarm Clock	233
11.11	Remote Secure Erase	235
11.11.1	Test Environment	236
11.11.2	Clear Secure Erase Boot Option	238
11.11.3	Remote Secure Erase without Drive Authentication	239
11.11.4	Remote Secure Erase with Drive Authentication via SOL Redirection	241
11.11.5	Remote Secure Erase with Drive Authentication via KVM Redirection	243



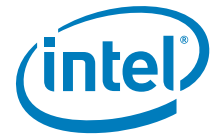
11.11.6	Remote Secure Erase with Drive Authentication via Direct Password Input....	246
11.11.7	Remote Secure Erase with Drive Authentication Failure via SOL Redirection ..	248
11.11.8	Remote Secure Erase with Drive Authentication Failure via Direct Password Input	249
12	Intel® CSME Power Management for Corporate Designs.....	252
12.1	System Power States	252
12.1.1	Deep S4/S5 Support	252
12.1.2	Intel® ME Power Gating	253
12.1.3	Intel® RMT	253
12.2	Test Environment and System Configuration.....	254
12.2.1	Test Parameters	254
12.2.2	Tools for Testing.....	255
12.2.3	Test Environment Setup	255
12.2.4	Test Step Execution and Verification	256
12.2.5	Setup Environment Tests	260
12.3	Test Coverage Summary.....	265
12.4	ME_PM_1: S0/CM0 to S3/CM-Off	267
12.5	ME_PM_2: S3/CM-Off to S0/CM0	269
12.6	ME_PM_3: S0/CM0 to S3/CM3	276
12.7	ME_PM_4: S3/CM3 to S0/CM0	278
12.8	ME_PM_5: S3/CM3 to S3/CM-Off (Without Intel® ME Wake)	282
12.9	ME_PM_6: S3/CM3 to S3/CM-Off (with Intel® ME Wake)	285
12.10	ME_PM_7: S3/CM-Off to S3/CM3	287
12.11	ME_PM_8: S0/CM0 to S4/CM-Off or S5/CM-Off	291
12.12	ME_PM_9: G3 or S4/CM-Off or S5/CM-Off (Suspend Well Off) to S0/CM0	295
12.13	ME_PM_10: S4/CM-Off or S5/CM-Off (Suspend Well On) to S0/CM0	303
12.14	ME_PM_11: S0/CM0 to S4, S5/CM3.....	314
12.15	ME_PM_12: S4-S5/CM3 to S0/CM0.....	317
12.16	ME_PM_13: S4-S5/CM3 to S4-S5/CM-Off (Without Intel® CSME Wake).....	325
12.17	ME_PM_14: S4-S5/CM3 to S4-S5/CM-Off (with Intel® CSME Wake).....	331
12.18	ME_PM_15: G3 or S4-S5/CM-Off (Suspend Well Off) to S4-S5/CM3	334
12.19	ME_PM_16: S4-S5/CM-Off (Suspend Well On) to S4-S5/CM3	339
12.20	ME_PM_17: Cold Reset.....	343
12.21	ME_PM_18: Global Reset	344
12.22	ME_PM_19: Straight-to-S5, Intel® ME Power Policy is S0 Only	348
12.23	ME_PM_20: Straight-to-S5 via Power Button Override	355
12.24	ME_PM_21: S3/CM-Off (with/Intel® ME Wake) to S3/CM-Off (Without Intel® ME Wake) .	372
12.25	ME_PM_22: S3/CM3-PG (with/ Intel® ME Wake) to S3/CM-Off (Without Intel® ME Wake)	373
12.26	ME_PM_23: G3 or S4-S5/CM-Off (Without Intel® ME Wake) to S4-S5/CM-Off (with Intel® ME Wake)	374
12.27	ME_PM_24: S4-S5/CM-Off (with Intel® ME Wake) to S4-S5/CM-Off (Without Intel® ME Wake)	377
12.28	ME_PM_25: S4-S5/CM-Off (Suspend Well Off) to S4-S5/CM-Off (with Host WoL) to S0/CM0 via Host WoL/WoWLAN	378
12.29	ME_PM_26: Warm Reset.....	382
12.30	ME_PM_27: S0/CM0 or Sx/Mx to G3.....	389
12.31	ME_PM_44: S0/CM0-PG, CM0 to S4-S5/CM-Off	391
12.32	ME_PM_45: G3 or S4-S5/CM-Off to S0/CM0-PG, CM0.....	395
12.33	ME_PM_46: S0/CM0-PG, CM0 to S0/CM0-PG, CM0	399
12.34	ME_PM_50: S0/CM0 to Sx/(CM3 or CM-Off) to S0/CM0 via AC Attach	405
12.35	ME_PM_51: S0/CM0 to Sx/CM-Off to S0/CM0 via AC Detach in Sx State.....	414
13	Intel® Trusted Execution Technology (Intel® TXT).....	420



13.1	Introduction	420
13.1.1	Validation Flow	420
13.2	Pre-requisite	421
13.2.1	TPM 1.2 NV Indices Defined and Locked	421
13.2.2	TPM 2.0 Indices Defined and Hierarchies	421
13.2.3	BIOS Setting	422
13.2.4	Unblocking Mechanism	423
13.2.5	SINIT ACM	423
13.3	Hardware and Software Components	423
13.3.1	Check Component Compliance	423
13.4	Tools	425
13.4.1	Validation Tools	425
13.4.2	TPM 1.2 Requirements	450
13.4.3	TPM 2.0 Requirements	450
13.5	BIOS-BIOS AC	452
13.5.1	Check BIOS-BIOS AC Integration	452
13.6	Measured Launch	453
13.6.1	Fundamental Measured Launching with getsec64.efi	453
13.6.2	Targeted Measured Launching	454
13.7	Verified Launch	454
13.8	Measured Launch Environment	454
13.8.1	Basic Stability	455
13.8.2	Functional Comprehensive	455
13.8.3	Platform Stability	455
13.8.4	BIOS/ACM Update Consideration	455
13.9	Secret Memory Protection Using SCLEAN	456
13.9.1	Set Secret Scenario	456
13.9.2	Secret Status Unknown Scenario	456
13.9.3	System Behavior with SLCEAN	457
13.10	Trusted Platform Module (TPM) Establishment Management	458
13.10.1	Checking TPM Establishment	458
13.10.2	Recommended TPM Establishment Behavior	459
13.10.3	Resetting Trusted Platform Module (TPM) Establishment	459
13.11	Summary	459
13.12	Intel® Trusted Execution Technology (Intel® TXT) Test Plan	459
13.12.1	Intel® TXT Testing Pre-requisite	461
13.12.2	Intel® TXT Baseline Coverage Summary	461
13.12.3	Intel® TXT Test Plan	462
14	Intel® Integrated Clock Control Compliance	478
14.1	Test Coverage Summary for CML-LP and CML-H	479
14.2	Test cases	479
14.2.1	Test Default Settings for Standard Configuration	479
14.2.2	Test Default Settings for Adaptive Configuration	480
14.2.3	GET and SET MPHY Settings	482
15	Media Playback	483
15.1	Test Coverage—Summary and Details	483
16	Intel® Dynamic Application Loader (Intel® DAL)	488
16.1	Introduction	488
16.2	Test Environment	488
16.2.1	Tools for Testing	488
16.2.2	Prerequisites	488
16.3	Test Coverage Summary and Details	489
17	Intel® Platform Trust Technology (Intel® PTT) Compliance	491



17.1	Test Coverage Summary.....	492
17.2	Verification of BIOS and Intel® PTT Communication Over CRB Interface	493
17.3	Intel® PTT Basic Functionality Under Windows* 10	494
17.4	Trusted Platform Module (TPM) Clear and Physical Presence	495
17.5	Windows* 10 BitLocker Integration	496
17.6	BitLocker TPM Protection	497
17.7	Virtual Smart Card Tests.....	498
17.8	Microsoft* Windows* Hardware Lab Kit (HLK) TPM Testing	499
17.9	Intel® PTT Disable/Enable from BIOS	499
17.10	Intel® PTT and Power Flows	500
17.11	Dictionary Attack Lockout After Coin Battery Removal with EOM Commit.....	500
18	Intel® Virtualization Technology (Intel® VT).....	502
18.1	Introduction	502
18.1.1	Purpose and Scope	502
18.1.2	Platforms Applicable.....	502
18.1.3	Terminology.....	502
18.1.4	Prerequisites	503
18.2	Test Plan and Details.....	503
18.2.1	Tests in EFI Shell	504
18.2.2	Intel® VT-x Tests with Microsoft* Client Hyper-V* on Windows* 8/8.1	506
18.2.3	Intel® VT Tests in Xen*/Linux* Environment	517
18.2.4	Platform Setup Requirements	521
18.2.5	Using openSUSE* 12.2 (64-Bit)	521
18.2.6	Using Fedora*17 (64-Bit).....	525
19	Intel® Device Protection Technology with Boot Guard.....	530
19.1	Overview	530
19.2	Scope	530
19.3	Prerequisites.....	530
19.4	Boot Guard Test Coverage Summary	531
20	Manufacturing Flow Simulation Test	537
20.1	Manufacturing Flow Simulation Test	537
21	Platform Controller Hub (PCH) SoftStrap Configuration	540
21.1	Test Coverage Summary.....	541
21.2	Intel Integrated Wired LAN Test.....	541
21.3	Wake On Wireless LAN (WoWLAN) Test.....	543
21.4	Flexible I/O Test	544
21.5	BIOS Boot-Block Size Test	557
21.6	Intel® CSME SMBus Alert Sending Device (ASD) Address Test	558
21.7	Power State Deep Sx Test.....	559
21.8	Trusted Platform Module (TPM) on SPI Test.....	560
22	Intel® ISH FW Compliance.....	561
22.1	Test Coverage Summary.....	561
22.2	Sensor Communication Test	562
22.3	Sensor Data Check	562
22.4	Loading and Execution.....	563
22.5	Sensor Diagnostic Test	563
22.6	Test System Sensors.....	564
22.6.1	Sensor Noise and Error Levels	564
22.6.2	Test System Sensor Noise and Effects on Sensor Algorithms.....	565
22.6.3	Test Worst Case System Interference and Effect on Sensor Algorithms	566
22.7	Test System Performance and Effective Calibration Under a Specific Range of Movements	567



22.8	Barometer (Pressure) Sensor Sanity Test	568
22.9	Light Sensor (ALS) Accuracy Test	568
22.10	Light Sensor (ALS) Angular Response Test.....	569
22.11	360 Hinge and Swivel Accuracy Test with 2nd Accelerometer	570
22.12	PLM Functionality Verification	571
22.13	Heading Sensor Accuracy and Drift Test	572
22.14	Intel Integrated Sensor Solution Power States.....	572
22.15	Sensor Activity Contexts	573
22.16	Sensor Terminal Contexts.....	574
22.17	Sensor Gesture Contexts	574
22.18	Wake On Shake Test.....	575
22.19	Step Counting Test.....	575
23	Intel® Software Guard Extension (Intel® SGX)	577
23.1	Introduction	577
23.2	Test Coverage Summary	577
24	Intel® System Security Report (Nifty Rock) Compliance	588
24.1	Introduction	588
24.1.1	Platforms Applicable	588
24.1.2	Terminology	589
24.1.3	Nifty Rock Prerequisites	589
24.1.4	Reference Documents	590
24.1.5	Validation Tools.....	590
24.2	Nifty Rock Test	591
24.3	NR_TC01.....	592
24.4	NR_TC02.....	592
24.5	NR_TC03.....	593
24.6	NR_TC04.....	593
24.7	NR_TC05.....	594
24.8	NR_TC06.....	595
24.9	NR_TC07.....	595
25	Intel® Trusted Device Setup	597
25.1	Introduction	597
25.2	Solution Prerequisites	597
25.3	Terminology	597
25.4	Tools for Testing	598
25.5	Process Prerequisites	598
25.6	Intel® TDS Solution Compliance Test Coverage Summary.....	599
25.7	Intel® TDS Tests.....	600
25.7.1	TDS_01	600
25.7.2	TDS_02	601
25.7.3	TDS_03	602
25.7.4	TDS_04	603
25.7.5	TDS_05	604
25.7.6	TDS_06	605
25.7.7	TDS_07	606
25.7.8	TDS_08	607
25.7.9	TDS_09	608
25.8	Backup	609
25.8.1	Full E2E Sealing	609



Figures

13-1 Intel® TXT Verified Launch/Validation Flow	421
18-1 Boot Loader Settings.....	523
18-2 Example Warning Allocating Space for Windows* 7/Virtual Machine.....	528
23-1 Intel® SGX Functional Validation Tool Pass Result Example	580
23-2 Functional Validation Tool Provisioning Pass Result Example	581

Tables

1-1 Boot Guard Discrete Intel® TPM and Intel® PTT	22
6-1 Intel® AMT Test Coverage Summary	40
8-1 BPDT Layout in Intel® CSME Region	78
11-1 Intel® AMT Test Coverage Summary	135
12-1 Supported Deep S4/S5 Policy Configurations.....	252
18-1 Applicable Platforms	502
18-2 Virtualization Testing Prerequisites.....	503
18-3 Intel® Virtualization Technology (Intel® VT) Test Overview	503
19-1 Boot Guard Tools for Testing	530
24-1 List of Applicable Platforms	589



Revision History

Document Number	Revision Number	Description	Revision Date
	0.7	<ul style="list-style-type: none">Initial release	July 2019
	0.8	<ul style="list-style-type: none">Common Services<ul style="list-style-type: none">Updated tests CS_030-037 since USB switching using Intel® APS is no longer required.Intel® AMT Chapter<ul style="list-style-type: none">Removed test AMT_072Updated Tests AMT_ (032-036) to no longer use the ISO Image that displays "Hello From PETS"Intel® Trusted Device Setup<ul style="list-style-type: none">Updated TDS_02	July 2019
	0.9	<ul style="list-style-type: none">Intel® AMT Chapter<ul style="list-style-type: none">Removed tests AMT_057 and AMT_058 and AMT_105Updated Test AMT_024Common Services<ul style="list-style-type: none">Updated CS test methodBoot Guard compliance chapter<ul style="list-style-type: none">Changed from BtgInfoTool to TxtBtgInfo.efiPower Management<ul style="list-style-type: none">Updated ME_PM_27 xmlCommon Services<ul style="list-style-type: none">Updated Test CS_006SGX Compliance<ul style="list-style-type: none">Updated Test SGX_03 description	September 2019



Document Number	Revision Number	Description	Revision Date
	1.0	<ul style="list-style-type: none"> • Intel CSME BIOS Compliance <ul style="list-style-type: none"> — Updated procedure of test BIOS _08 — Updated RSA readiness procedure • Intel® AMT Chapter <ul style="list-style-type: none"> — Intel® AMT_012 test was removed — Intel® AMT_10x TBT dock tests were removed — Updated Intel® AMT_024/_025/_048/_049/_055 • Intel® CSME Power Management for Corporate Design-Stress testing Updated the following tests: <ul style="list-style-type: none"> — PM_ST_2,3,7,16,17 — PM_ST_1,4,12,18,19 Updated last step that check flash log existence • Intel® Software Guard Extension (SGX) <ul style="list-style-type: none"> — Updated SW Controlled test — Updated Stress Test • Integrated Clock control Compliance <ul style="list-style-type: none"> — Removed OC Feature • B Appendix <ul style="list-style-type: none"> — Removed test cases that has Intel® WoWLAN coexistence mode which should be removed from SKL • C Appendix <ul style="list-style-type: none"> — Added to check SPI flash log at the end of procedure 	December 2019
	1.1	<ul style="list-style-type: none"> • Intel® Active Management Technology Tests (Intel® AMT) Tests <ul style="list-style-type: none"> — Removed 'Setup of AMT over TBT dock or WLAN section — Removed AMT_90-96 from main test table and all other internal tests — Removed "Setup of AMT Over Discrete LAN or WLAN" — Removed "WSMAN Commands Definition" — Removed setup environment tets — Updated LAN type in main table and all relevant tests to Integrate LAN only — Updated Test AMT_036 • Intel Trusted Technology Execution Technology <ul style="list-style-type: none"> — Removed TXT_TC0005B • Added Chapter 8 • Intel® Software Guard Extension (SGX) <ul style="list-style-type: none"> — Removed PETS support for SGX tests • Intel® CSME Power Management for Corporate Designs <ul style="list-style-type: none"> — Decreased PG check time from 3 minutes to 1 minute — Modified ME_PM 5,21,22 test to remove support of non-mobile (AC) systems 	April 2020

§ §



1 Introduction

1.1 Purpose and Scope of this Document

The Intel® Converged Security and Management Engine (Intel® CSME) and Intel® Sensor Solution Corporate Compliance Guide for the Comet Lake Platform is designed to provide Original Equipment Manufacturers (OEMs) and Original Design Manufacturers (ODMs) with the compliancy requirements for the 2016–2017 platform implementation and the methodology and tools to verify compliance for different Intel® Manageability firmware, core components and technologies.

This document contains the compliance requirements that reduces the number of issues seen in the implementation of consumer technologies. It also provides the test environment setup information, the procedure for each test, and the expected results for the purpose of validating compliancy. Requirements contained in this document target the system BIOS, Intel® CSME and other aspects of overall platform implementation.

Note: This document supports the following **network form factors**:

- LAN
- LAN + WLAN
- WLAN only

Note: This document supports Desktop, AIO, Workstation, Mobile, and Ultrabook™ **form factors** only.

Note: This document supports the following Operating Systems:

- Windows* 10

1.2 Features

The corporate Intel® CSME firmware binary is developed to meet the demands of Intel Mobile and Ultrabook™ platforms and Microsoft* Windows* 8.1/10 InstantGo (IG) requirements. Power consumption in idle state, coupled with enhanced security features are the key deliverable for this product.

The corporate Intel® CSME firmware binary implements a power-gating feature that can reduce the Intel® CSME idle power consumption within the PCH to near-zero milliwatt. Intel® CSME enters power-gated mode when the firmware becomes idle and the platform is in either S0 or S0ix states. This power-gated state of the Intel® CSME is represented as CM0-PG. Intel® CSME firmware exits CM0-PG state when Intel® CSME activity is requested, or host activity requires firmware execution, such as when power transition events occur.



1.3 Intel® CSME Firmware

1.3.1 WoWLAN or WOL Driver Feature

Intel® PETS tests that need to “Wake on LAN” may use either “Wake on LAN” (WoL) or “Wake on Wireless LAN” (WoWLAN). On platforms which are “WLAN only” (platform that has no LAN), customers should use the WoWLAN. Refer the WLAN driver release notes to verify that the WoWLAN feature is supported and enabled in the WLAN driver used, as the availability of the WoWLAN feature in the WLAN driver is not fully guaranteed, when this document was published.

Caution: In case that the WoWLAN feature is not available in the WLAN driver used, do not run WoL related test.

1.3.2 Windows* 8.1/10 Fast Startup (Partial Hibernate)

The ‘Windows* 8.1/10 Fast Startup’ feature should be disabled during Intel® PETS runs, as when enabled, platform would not go into S5 state. If this feature is enabled, S5-related tests fails.

1.3.3 Environment Networking Recommendations

In order to reduce environment impact on tests, the following steps are proposed.

1.3.3.1 General

1. Disable or shutdown non-essential applications or services on the Management Console (MC) which are not needed for testing. Applications which periodically interact with the network to scan it may inadvertently influence the test results.
2. Turn off the Microsoft* Windows* ‘Auto Discovery’ feature on the System Under Test (SUT) if enabled.
3. Turn off the Microsoft* Windows* ‘Network Discovery’ feature on the MC if enabled. Refer the following links for more information on this feature:
 - a. Microsoft* Windows* 7/8.1/10: <http://windows.microsoft.com/en-us/windows/enable-disable-network-discovery#1TC=windows-7>

1.3.3.2 Wireless

1. Isolate the Wireless AP so that only the SUT and MC are connected to it—to avoid outside interference with the test.
2. Configure the Wireless AP to a frequency and channel not used by other Access Points in the area, to avoid wireless crosstalk and frequency spectrum overcrowding.

Example: If surrounding APs are set to operate on 2.4 GHz frequency channel 13, change testing AP to use the 5 GHz frequency channel 44 which is unused by other local APs.



1.4 Terminology

The keywords “MUST”, “MUST NOT”, “REQUIRED”, “SHALL”, “SHALL NOT”, “SHOULD”, “SHOULD NOT”, “RECOMMENDED”, “MAY”, “MANDATORY”, and “OPTIONAL” in this document are to be interpreted as described in RFC 2119.

1.5 Acronyms, Terminology, and Definitions

1.5.1 General

Acronym or Terminology	Definition
CS	Connected Standby
FPF	Field Programmable Fuses
DHCP	Dynamic Host Configuration Protocol
DMA	Direct Memory Access
DN	Domain Name
DNS	Domain Name System
EC	Embedded Controller. Equivalent to KBC (Keyboard Controller)
EHBC	Embedded Host Based Configuration
USB-R	Integrated Device Electronics-Redirect
Intel® MEI	Intel® Management Engine Interface
Intel® TXT	Intel® Trusted Execution Technology.
ISV	Independent Software Vendor
MAC	Media Access Control
MC	Management Console
PET	Platform Event Trap
PID	Provisioning ID
PPS	Provisioning Pass Phrase
PSK	Pre-Shared Key
SOAP	Simple Object Access Protocol
SOL	Serial Over LAN
SPI	Serial Peripheral Interface
SUT	System Under Test

1.5.2 Intel® AMT Acronyms, Terminology, and Definitions

Acronym or Terminology	Definition
Agent	Software that runs on a client PC operating system.
Alert	An alert occurs when the firmware notifies the remote console that an event has occurred in the system. Examples of events are a fan failure or a virus attack.
ASF	Alert Standard Format
Asset Management	Intel® AMT stores hardware and software asset information in flash memory that can be read anytime; even when the PC is turned off



Acronym or Terminology	Definition
Closed configuration network	A closed configuration network is a special network that is used for configuration purposes only. It has no connection to the enterprise/business network.
Configuration server	A software application that runs at the user configuration station. This application is responsible for connecting to the Intel® AMT firmware and automatically configuring it with pre-defined parameters.
End User	The person who uses the computer system. In a corporate setting, the end user may not have an administrator privileges on the machine.
Host interface	A communication channel between the Intel firmware and applications running on the host. For Intel® AMT 1.0 this was implemented as KCS interface. In Intel® AMT 2.0 and onwards it is implemented as Intel® MEI interface
Host or Host Processor	The processor that is running the operating system. This is different than the management processor running the Intel® AMT firmware
Host Service/Application	An application that is running on the host Processor
Intel® Management Engine Interface (Intel® MEI) driver	Intel® MEI driver—Intel® AMT host driver that runs on the host and interfaces between ISV Agent and the Intel® AMT Hardware. Intel® MEI 1 - Used for BIOS and OS interface. Intel® MEI 2 - Optional, may be used for SMI. BIOS can either enable/disable second Intel® MEI and conceal it from the host software.
IT User	Information Technology user. Typically very technical and uses console to ensure multiple PCs on a network function.
Intel® Converged Security and Management Engine (Intel® CSME) firmware	The Intel® ME firmware running on the embedded processor. Cannot use "FW" generically in this PDG as there is Fan firmware too.
OS not functional	The Host OS is considered not functional in any one of the following cases: <ul style="list-style-type: none"> • System is in Sx power state. • System is in S0 power state and: • OS is hung • After PCI reset • OS watch dog expires • OS is not present • OS has crashed (BSOD Blue Screen of Death)
PET	Platform Event Trap is the ASF protocol.



1.5.3 System States and Power Management

Acronym or Terminology	Definition
S0	A system state where power is applied to all Hardware devices and system is running normally (refer latest industry ACPI specification).
S0-S0ix	Core Well Powered; Intel® ME Well Powered; (Intel® ME core not consuming power) DRAM available.
S3	A system state where the host Processor is not running and power is still connected to the memory subsystem (refer latest industry ACPI specification). Also known as standby, where the OS state is saved to memory and resumed from memory when mouse, keyboard or other activity occurs that is configured as a wake event
S4	A system state where both the host Processor and memory are inactive (refer latest industry ACPI specification). Also known as hibernate, where the OS state is saved to the hard disk.
S5	A system state where all power to the host system is off and the power cord is still connected (refer latest industry ACPI specification).
Sx	Any power state that is not S0
OS hibernate	When the OS saves state information to the hard disk
Standby	When the OS state is saved to memory and resumed from the memory when mouse, keyboard or other activity occurs that is configured as a wake event.
Shut Down	A state where the system power is off and the power cord is still connected.
CM0	An Intel® ME firmware power state where all Hardware power planes are activated and the host power state is S0.
CM3	An Intel® ME firmware power state when the host is in Sx. The Processor DRAM Controller is turned off and DRAM power stays in off/self refresh mode. There is no UMA usage in M3 state. Less than 1MB of SRAM used for code and data. Code is executed off of flash takes ~1mS.
CM0-PG	Core Well Powered; Intel® ME Well Powered; (Intel® ME core not consuming power) DRAM available.
CM3-PG	An Intel® ME firmware power state where no power is applied to the Management Engine subsystem. (Intel® ME firmware is shut down).
Deep S4/S5	To minimize power consumption while in S4/S5, the PCH supports a lower power version of these power states known as Deep S4/S5. In these Deep S4 and Deep S5 states, the Suspend wells are powered off, while the new Deep S4/S5 Well (DSW) remains powered. A limited set of wake events are supported by the logic located in the DSW.
Global reset	A full platform reset that includes the Intel® ME sub system and host sub system
PG	Power Gating
Intel® ME Wake On LAN (WOL)	A feature where the Intel® ME sub system is powered off but automatically resume operation if it receives a packet from the network through the wired LAN connection.

1.5.4 Wireless and Mobile

Acronym or Terminology	Definition
AP	Access Point—a device that provides a bridge between the wired LAN and the wireless LAN.
BSS	Basic Service Set—A basic configuration of a wireless LAN network comprising an Access Point. All communications to and from the wireless nodes flow through the Access Point.
CCK	Complementary Code Keying
CCX	Cisco Certified Extensions



Acronym or Terminology	Definition
DCF	Distributed Coordination Function
EAP	Extended Authentication Protocol
ESS	Extended Service Set
IEEE	Institute of Electrical and Electronics Engineers
MAC	Media Access Control hardware
MIB	Management Information Base
Network Detection feature	Network Detection is a feature designed for mobile platforms. This feature consists of an externally-exposed button on the mobile chassis that can be pressed when the laptop lid is closed to activate a visual LED indicating to the user the presence of available wireless networks that are in range.
OFDM	Orthogonal Frequency Division Multiplexing
PCF	Point Coordination Function
RSSI	Receive Signal Strength Indicator
Supplicant	An 802.1x entity that is being authenticated by the Authenticator.
WEP	Wired Equivalent Privacy
Wi-Fi	Wireless Fidelity
WLAN	Wireless LAN
WoWLAN	Wake on WLAN

1.6 Reference Documents

Document	Document Number/Location
Intel® PCH Family SPI Flash Programming Guide	Latest on CDI or in VIP kit
Intel® Virtualization Technology for Directed I/O Architecture Specification	http://www.intel.com/technology/virtualization/index.htm
Intel® 64 and IA-32 Architectures Software Developer's Manual, Volume 3B (For Intel Virtualization, VT-x Specifications)	http://www.intel.com/products/processor/manuals/index.htm
Reference material and white papers on Intel® VT	http://www.intel.com/technology/virtualization
Intel® Virtualization Software Community	http://www.intel.com/software/virtualization
Intel® TXT-enabled Xen*	http://xenbits.xensource.com/xen-unstable.hg and http://xen.org/download/index.html
Intel® TXT – Trusted Boot Checkout Kit	VIP Kit number - 52849
EFI shell (DUET – FAT32)	http://developer.intel.com/technology/efi/agreesource.htm
Comet Lake Platform Controller Hub (PCH) LP External Design Specification (EDS)	606576
Comet Lake Platform Power Sequence Specification	TBD
Comet Lake Platform Design Guide Comet Lake H Platform Design Guide Comet Lake S PCH H Platform Design Guide Comet Lake S Platform with CML PCH V Design Guide	607109 611586 610244 612166



Document	Document Number/Location
Intel® Trusted Execution Technology (Intel® TXT) - Trusted Platform Module (TPM) Nonvolatile (NV) Storage Interface Usage - Application Note	420735
Intel® Converged Security and Management Engine (Intel® CSME) 14 Firmware PRD	605549
Intel® TXT Measured Launched Environment Developer's Guide	http://www.intel.com/technology/security
Intel® APS Setup and Configuration Guide for OEMs	Available in the Intel® ME Compliance Kit
Intel® Converged Security and Management Engine (Intel® ME 12) Tools - Product Requirements Document	TBD
Intel® Platform Enablement Test Suite User Guide	Located in Intel® Compliancy Kit
Intel® APS Setup and Configuration Guide for OEMs	Located in Intel® Compliancy Kit
Intel® Automated Power and System State Test Device (Intel® APS) User's Guide for OEMs	Located in Intel® Compliancy Kit
Intel® AMT Tools User Guide	Located in Intel® Compliancy Kit

1.7 External References

Document	Location
IEEE 802.11a Specification	http://standards.ieee.org/wireless
IEEE 802.11b Specification	http://standards.ieee.org/wireless
IEEE 802.11g Specification	http://standards.ieee.org/wireless
IEEE 802.11d Specification	http://standards.ieee.org/wireless
IEEE 802.11e Specification	http://standards.ieee.org/wireless
IEEE 802.11h Specification	http://standards.ieee.org/wireless
IEEE 802.11i Specification	http://standards.ieee.org/wireless
WPA Specification documentation	http://www.weca.net/OpenSection/protected_access.asp
ASF 2.0 Revision	http://www.dmtf.org/standards/asf/
ACPI Specification	http://www.acpi.info/spec20c.htm

1.8 Testing Guidelines

Intel recommends customers to run Intel® PETS testing whenever there are any changes in:

- BIOS
- Intel® Converged Security and Management Engine (Intel® CSME) firmware
- EC firmware
- Board/Silicon stepping changes

The following tests should be executed in the specified order:

1. Run Intel® PETS Setup Environment Test
2. Run Integrated Clock Control test Package
3. Run SPI test package
4. Run BIOS test package
5. Run Power Test packages
6. Run Feature tests (Intel® AMT, WLAN, and so forth) depending on the SKU



Note: The SKU matrix table is updated in future releases of this document.

Note: To enable WOL, go to Control Panel -> System -> Hardware -> Device Manager -> (select network adaptor) -> Properties -> Advanced. Change **Enable PME** to **enabled**

1.9 Boot Guard Discrete TPM Intel® PTT

Table below shows the configuration information for the Boot Guard—Discrete TPM and Intel® Platform Trust Technology (Intel® PTT) with respect to how they work with different operating systems and firmware (Consumer/Corporate) combinations.

Refer Boot Guard and Intel® PTT chapter for actual compliancy tests.

Definitions:

- Supported—Intel validates this combination
- Not Supported—Intel would not validate this combination
- N/A—Not a valid combination from a validation standpoint

Table 1-1. Boot Guard Discrete Intel® TPM and Intel® PTT

Platform 2015 ¹	Intel® ACM	Intel® ME Firmware	Intel® PTT	TPM 1.2	TPM 2.0
CNL Based (1-Chip and 2-chip)	Intel® ACM 3.x	Consumer	Yes	Yes	Yes
		Corporate Intel® vPro™	Yes ²	Yes	Yes

Notes:

1. Refer platform dashboard for POR configurations.
2. Refer Intel® PTT documentations for vPro™ compatibility.

§ §



2 Intel® Trace Hub (Intel® TH)

The Intel® Trace Hub Compliance section serves as a checklist for the environment setup of Trace Hub and the SUT.

2.1 Tools for testing:

- System Trace tool from Intel® System Debugger (part of Intel® System Studio NDA product) installed on the host computer, where the tests are run. The latest version of Intel® System Studio NDA can be downloaded from <https://registrationcenter.intel.com/en/forms/?productid=2336&SupportCode=ENA&pass=yes>. For setup and usage refer the System Trace User Guide located at "C:\IntelSWTools\system_studio_2018_nda\documentation_2018\en\debugger\system_studio_2018_nda\system_debugger\system_trace".
- Intel® SVT Closed Chassis Adapter.
- Enable DCI by setting Direct Connect Interface (DCI) Enabled under the debug tab of Intel® FIT to 'Yes'. Click Build Image and generate the full SPI image. Refer the Bringup Guide for more details on image creation.

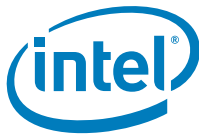
2.2 Test Coverage Summary

Form Factor:

D = Desktop, M = Mobile, A = All in one, W = Workstation

Test ID	Test Case Title	PETS/Manual	Form Factor
ITH_001	Intel® CSME FW - DCI Enable (MEEN)	Manual	D M A W
ITH_002	BIOS - DCI Enable (HEEN)	Manual	D M A W
ITH_003	BIOS - DCI Enable Post EOM	Manual	D M A W
ITH_004	Capture ITH BIOS/ME Tracing Via CCA	Manual	D M A W

Note: ITH_003 requires the SUT to be out of manufacturing mode, refer ITH_003 for more information.



2.3 Intel® CSME FW - DCI Enable (MEEN)

Test ID	ITH_001
Test Case Title	Intel® CSME FW - DCI enable
Mandatory/Optional	Mandatory
Description	When Intel® CSME is in manufacturing mode, DCI interface can be enabled through Intel® CSME FW (MEEN).
Objective	To enable DCI through Intel® CSME
Procedure	<ol style="list-style-type: none">1. Install Intel® System Debugger which supports platform on console.2. Flash the <u>full DCI enabled</u> image on to the platform.3. Perform RTC clear to make MEEN take effective.4. Boot to BIOS and ensure that Host DCI Enable (HEEN) is set to Disabled5. Connect the target end of the CCA to a USB3 port on the target and connect the host end of the CCA to a host with Intel® System Studio NDA software installed.6. Go to C:\Intel\OpenIPC\Config\CML and look for the xml files that reflects the silicon and probe (example: "CML_CMP_DCI_OOB").7. Open OpenIpcConfig.xml from C:\Intel\OpenIPC\Config and copy the file name in above step to name the field in this xml file (example: <DefaultIpcConfig Name="CML_CMP_DCI_OOB" />). Then, save and close the xml file.8. Open Intel® System Debugger and select the Target Connection Configuration.9. Select "Attempt to configure" which points to OpenIPC folder.10. Click connect button and ensure that DCI is connected without errors.
Test Pass/Fail Criteria	<p>Test passes if we are able to connect to the target over DCI and we are able to refer the following message in the console:</p> <p>18:54:45 [INFO] [npk_config_api] Successfully created target connection. 18:54:45 [INFO] [npk_config_api] Querying NPK hardware...</p> <ol style="list-style-type: none">1. NPK PCI access (0x0,0x1f,0x7): false2. NPK CSR access: true3. NPK hardware ready: true <p>18:54:45 [INFO] [npk_config_api] Detected Intel(R) Trace Hub hardware</p>

2.4 BIOS DCI Enable (HEEN)

Test ID	ITH_002
Test Case Title	BIOS—CI Enable
Mandatory/Optional	Mandatory
Description	Check that DCI interface can be enabled through BIOS (HEEN)



Test ID	ITH_002
Objective	To enable DCI through BIOS.
Procedure	<ol style="list-style-type: none"> 1. Install Intel® System Debugger which supports the platform on console. 2. Flash the <u>full DCI disabled</u> image on to the platform. 3. Boot to BIOS and ensure that Host DCI Enable (HEEN) is set to Enabled, refer Document# 558380 for BIOS implementation details. 4. Connect the target end of the CCA to a USB3 port on the target and connect the host end of the CCA to a host with Intel® System Studio NDA software installed. 5. Go to C:\Intel\OpenIPC\Config\CML and look for the xml files that reflects the silicon and probe (example: "CML_CMP_DCI_OOB") 6. Open OpenIpcConfig.xml from C:\Intel\OpenIPC\Config and copy the file name in above step to name the field in this xml file (example: <DefaultIpcConfig Name="CML_CMP_DCI_OOB" />). Then, save and close the xml file. 7. Open Intel® System Debugger and select the Target Connection Configuration 8. Select "Attempt to configure" which points to OpenIPC folder 9. Click connect button and ensure that DCI is connected without errors
Test Pass/Fail Criteria	<p>Test passes if we are able to connect to the target over DCI and we are able to refer the following message in the console:</p> <pre>18:54:45 [INFO] [npk_config_api] Successfully created target connection. 18:54:45 [INFO] [npk_config_api] Querying NPK hardware... 1. NPK PCI access (0x0,0x1f,0x7): false 2. NPK CSR access: true 3. NPK hardware ready: true 18:54:45 [INFO] [npk_config_api] Detected Intel(R) Trace Hub hardware</pre>

2.5 BIOS DCI Enable Post EOM

Test ID	ITH_003
Test Case Title	BIOS - DCI enable post EOM
Mandatory/Optional	Mandatory
Description	When platform is out of manufacturing mode, Intel(R) CSME would not be capable of enabling DCI on the platform. DCI interface can be enabled only through BIOS



Test ID	ITH_003
Objective	To enable DCI through BIOS
Procedure	<ol style="list-style-type: none">1. Install Intel® System Debugger which supports the platform on console.2. Execute fpt -closemnmf so that the platform is out of manufacturing mode. Check FWSTS to confirm that the platform is out of manufacturing (HECI1_CSE_FS - Host PCI 0:22:0 offset 0x40, BIT 4 Manufacture mode is cleared).3. Boot to BIOS and set Host DCI Enable (HEEN) to Enabled. Refer Document# 558380 for BIOS implementation details.4. Connect the target end of the CCA to a USB3 port on the target and connect the host end of the CCA to a host with OpenIPC software installed.5. Go to C:\Intel\OpenIPC\Config\CML and look for the xml files that reflects the silicon and probe (example: "CML_CMP_DCI_OOB")6. Open OpenIpcConfig.xml from C:\Intel\OpenIPC\Config and copy the file name in above step to name the field in this xml file (example: <DefaultIpcConfig Name="CML_CMP_DCI_OOB" />). Then, save and close the xml file.7. Open Intel® System Debugger and select the Target Connection Configuration.8. Click connect button and ensure that DCI is connected without errors.
Test Pass/Fail Criteria	<p>Test passes if we are able to connect to the target over DCI and we are able to refer the following message in the console:</p> <p>18:54:45 [INFO] [npk_config_api] Successfully created target connection. 18:54:45 [INFO] [npk_config_api] Querying NPK hardware...</p> <ol style="list-style-type: none">1. NPK PCI access (0x0,0x1f,0x7): false2. NPK CSR access: true3. NPK hardware ready: true <p>18:54:45 [INFO] [npk_config_api] Detected Intel(R) Trace Hub hardware</p>

2.6 Capture ITH BIOS/ME Tracing Via CCA

Test ID	ITH_004
Test Case Title	Capture ITH BIOS/ME tracing via CCA
Mandatory/Optional	Optional
Description	Collect Intel® CSME and BIOS logs using the STT tool



Objective	Collect Intel® Trace Hub logs using CCA
Procedure	<ol style="list-style-type: none"> Flash image that has DCI and Intel® CSME trace enabled. Connect the target end of the CCA to a USB3 port on the target and connect the host end of the CCA to a host with OpenIPC software installed. Open the System Trace Tool (STT). Use a fresh workspace and use the setup project menu to configure the trace project. Refer System Trace chapter of System Debugger Getting started Guide for more details. Check CSME and BIOS for the trace source. <p>Note: Selecting BIOS is optional, if the BIOS does not support trace messages over Intel® Trace Hub</p> <ol style="list-style-type: none"> Click the green button to connect to the target on the Target Connection tab. Click the play button to start the trace in the Trace Capture tab. Restart the target with the restart option from windows* menu. check if we are able to collect BIOS and Intel® CSME logs in the STT and the messages are time correlated. Shut down target by selecting shutdown option from windows* menu Power on the target to boot from S5 to S0 state check if we are able to collect BIOS and Intel® CSME logs in the STT and the messages are time correlated. Put the target to standby mode (S3) Resume the target to boot from standby by pressing the Power Button check if we are able to collect BIOS and Intel® CSME logs in the STT and the messages are time correlated. Execute a cold reset by writing 0xE to CF9 register (mm CF9 0xE -Io) check if we are able to collect BIOS and Intel® CSME logs in the STT and the messages are time correlated. Execute a warm reset by writing 0x6 to CF9 register (mm CF9 0x6 -Io) check if we are able to collect BIOS and Intel® CSME logs in the STT and the messages are time correlated.
Test Pass/Fail Criteria	The test passes, if user is able to collect BIOS and Intel® CSME logs in the STT and the messages are time correlated.

§ §



3 Signing, Manifesting, and Secure Tokens

3.1 Introduction

This chapter includes tests to verify that OEMs are able to add OEM signed components to the platform image, create Secure Tokens for Debug, and successfully inject them into the platform. It also verifies that OEM unlock token works on the platform.

Secure Tokens are only supported on platforms with a other OEM signed components.

The tests in this chapter are only relevant for OEMs who wish to sign OEM components in the platform image.

3.2 Test Environment Setup

Signing and manifesting documentation can be found in ME FW kit that details usage of signing the tokens.

3.3 Tools for Testing

- PFT (Platform Flash Tool): Tool used for DnX mode, and token creation/injection. Tool can be found in latest ME FW kit.
- OpenSSL: Freeware, can be found in Open source community.
- FIT (Flash Image Tool): Tool used to stitch FW image, can be found in ME FW kit.
- FPT (Flash Programming Tool): Tool used to burn images on SPI platforms, and set EOM state.

3.4 Coverage Summary

Platform, Operating System Support, How? Column describes the test methodology.

OS Support: W = Microsoft* Windows*, WI = Microsoft* Windows* InstantGo

How?: A = Fully Automated using Intel® PETS, I = Interactive using Intel® PETS and M = Manual

Test ID	Test Case Title	PETS Package Name	OS Support	How?
SIGN_01	Image creation with OEM signed component	N/A	W WI	M
SECTOK 02	Debug Token	N/A	W WI	M



3.5 Image Creation with OEM Signed Components

Test ID:	SIGN_01
Test Case Title:	Image Creation with OEM signed components
Objective:	This test verifies that OEMs are able to create a platform image with signed OEM components, and components have loaded correctly.
Test Pass Criteria	Platform boots and signed OEM components load correctly.
Description:	OEM sign OEM-provided binaries and add them to the image. The public key hashes of all the OEM-provided binaries signatures is entered into the OEM Key Manifest, which is itself signed and included in the image.
Windows* Procedure:	<p>Manual Procedure:</p> <ol style="list-style-type: none"> 1. Create pairs of keys for signing OEM-provided binaries, using OpenSSL. Details of procedure are in the LKF Signing and Manifesting Guide. A minimum of one pair of keys must be created that can be used for all signing, but a separate pair is ideally used for each OEM-provided binary and the OEM Key Manifest. The OEM-provided binaries include ISH, iUnit, aDSP, if the OEM plans to replace the Intel provided binaries with his own. 2. Enter the public key hashes of all the keys into the OEM Key Manifest's respective fields. If multiple key hashes are entered, separate nodes need to be created in the OEM Key Manifest xml, one for each different hash. Details of procedure for creating hashes are in the LKF Signing and Manifesting Guide. 3. Use MEU to manifest and sign the OEM Key Manifest. Details of procedure are in the LKF Signing and Manifesting Guide. 4. Use MEU to sign (or resign) each OEM-provided binary whose hash has been entered into the OEM Key Manifest. 5. Enter the hash of the OEM Key Manifest key and the OEM Key Manifest binary into FIT, and then use FIT to build an IFWI image including the OEM Key Manifest. Details of procedure are in the LKF Signing and Manifesting Guide. 6. Burn the IFWI image to the platform. 7. Verify that the platform boots to the OS and all OEM signed components are loaded correctly.

3.6 Debug Token

Test ID:	SIGN_02
Test Case Title:	Debug Tokens
Objective:	This test verifies that OEMs are able to create Secure Tokens for Debug, and successfully inject them into the platform. It also verifies that OEMs are able to enter the hash of the token public key into the OEM Key Manifest, and build an image with this manifest, such that the platform recognizes the injected token.



Test ID:	SIGN_02
Test Pass Criteria	Platform is in OEM Unlock State
Description:	OEM creates a token. The public key hash is entered into the OEM Key Manifest, which is included in the IFWI image. The token is injected into the platform using DnX. Platform moves to OEM Unlock Status
Windows* Procedure:	Manual Procedure: <ol style="list-style-type: none">1. Create a pair of keys for the Debug Token, for example, using OpenSSL. Details of procedure are in the LKF Secure Tokens guide found in latest ME FW kit. In order to use the Intel® Platform Flash tool to create tokens, the Private key and the password used to create this key should be entered in the Intel® Platform Flash tool under Security tab (on the top) -> General Settings as Certificate and password respectively.2. Enter the public key hash into the OEM Key Manifest's field for OEMUnlockTokens. Details of procedure for creating the hash are in the LKF Signing and Manifesting Guide, chapter 3, and details for entering the hash into the OEM Key Manifest are in chapter 5.3. Use MEU to manifest and sign the OEM Key Manifest. Details of procedure are in the LKF Signing and Manifesting Guide, chapter 5.4. Use FIT to build an IFWI image including the OEM Key Manifest. Details of procedure are in the LKF Signing and Manifesting Guide, chapter 5.<ol style="list-style-type: none">a. In order to create and sign an OEM Unlock token, use the Intel® Platform Flash Tool ensuring to set the OEMUnlockEnabled knob to OEMUnlockEnabled, and the ISH GDB Debug knob to "enabled" – follow instructions in the LKF Secure Token guide.b. To stitch token within the IFWI image,<ul style="list-style-type: none">·Use FIT also to add token in image.·Burn the IFWI image to the platform, and use FPT –EOM to close manufacturing state.c. If you choose NOT to stitch within IFWI, then continue to inject token via Intel® Flash Programming tool OR Intel® Platform Flash Tool if you are using DnX APIs (Refer LKF Secure Token Guide for instructions)5. Verify that platform functionality is (Orange) unlocked, and available for debugging. Ensure the following are done:<ol style="list-style-type: none">a. After injecting token via DnX or stitched in image by FIT, boot platform with DCI enabledb. Connect Lauterbach* to capture NPK messages (using NPK decoder released in compliance kit)c. Initiate warm reset6. Verify NPK log contains the following message: "Accept secure token".





4 Intel® CSME Manufacturing Mode Compliancey — Corporate

The Intel® Management Engine Manufacturing Mode compliancey chapter serves as a checklist for the environment setup for the host BIOS and Intel® CSME interface testing and validation when the Intel® CSME is in Manufacturing Mode.

The tests in this section verify that certain BIOS operations are *not* performed when the Intel® CSME is in Manufacturing Mode.

Test Environment for Intel® CSME BIOS Compliancey

The system under test is to be configured with the Intel® CSME in manufacturing mode and Deep S4/S5 disabled.

4.1 Tools for Testing

- Intel® Platform Enablement Test Suite—Latest version of the tool from the Intel® CSME Compliancey kit release. Refer the *Intel® Platform Enablement Test Suite User Guide* available in the Intel Compliancey kit for exact instructions on how to load and setup the Intel® Platform Enablement Test Suite software.
- Compliance_MeBios_ManufacturingMode.xml—Package should be loaded to Intel Platform Enablement Test Suite in order to complete this section.

4.2 Test Coverage Summary

Form Factor:

D = Desktop, M = Mobile, W = Workstation, A = All in one

Network:

LAN = systems with LAN interface and test is performed using LAN interface

WLAN = systems with WLAN interface and test is performed using the WLAN interface

WLAN** = systems with WLAN interface and test is performed using the WLAN interface, only if the WLAN card supports Host Wake on WLAN.

Test ID	Test Case Title	PETS/Manual	Form Factor	Network
BIOS_04	CF9GR locking/unlocking - Manufacturing Mode (Mandatory)	PETS	D M W A	LAN+WLAN; WLAN only



4.3 CF9GR Locking/Unlocking

Test ID:	BIOS_04
Test Case Title:	CF9GR locking/unlocking - Manufacturing Mode
Mandatory/Optional:	Mandatory
Description:	When the system is in the Intel® ME manufacturing mode, BIOS must set the CF9GR register (address space at PCH B0:D31:F2 register offset ACh [bit 20]) to '0' to allow host only resets before handing control to the OS. For the Intel® FPT tool to perform a global reset with parameter/GRESET, the BIOS must keep the CF9GR setting unlocked (by setting B0:D31:F2 register offset ACh [bit 31] of the same register to '0').
Objective:	For security reasons, the BIOS must ensure that CF9GR is cleared and locked before handing control to the OS in the shipping machine. But for the usage of Intel® FPT tool with /GRESET parameter in the manufacturing environment, the BIOS must ensure that CF9GR reset mode can be changed by the Intel® FPT tool.
Procedure:	<ol style="list-style-type: none">1. Boot the system under test to OS.2. Intel Platform Enablement Test Suite performs the following:<ol style="list-style-type: none">a. Manually read the PCI address space at PCH B0:D22:F0 register offset 40h [bit 4] to verify the Intel® ME Manufacturing Mode bit is equal to '1'.b. Manually read the PCI address space at PCH B0:D31:F2 register offset ACh [bit 20] to verify the bit is set to '0'.c. Manually read the PCI address space at PCH B0:D31:F2 register offset ACh [bit 31] to verify the bit is set to '0'.
Test Pass/Fail Criteria:	Test passes if the PCH B0:D31:F2 register offset ACh [bit 20] = '0' and [bit 31] of the same register is '0' when the system is in the Intel® ME manufacturing mode.





5 Intel® CSME BIOS Compliance

The Intel® CSME BIOS Compliance section serves as a checklist for the environment setup for the host BIOS and Intel® Management Engine interface testing and validation.

Test Environment for Intel® CSME BIOS Compliance section

The system under test is to be configured with the Intel® CSME **not** in manufacturing mode (fpt -closemnf) and Deep S4/S5 disabled.

5.1 Tools for Testing

- Intel® Platform Enablement Test Suite—Latest version of the tool from the Intel® CSME Compliance kit release. Refer the *Intel® Platform Enablement Test Suite User Guide* available in the Intel® CSME Compliance kit for exact instructions on how to load and setup the Intel® Platform Enablement Test Suite software.
- Compliance_MeBios.xml—Package should be loaded to Intel® Platform Enablement Test Suite (Intel® PETS) in order to complete this section.
- Intel System Trace Tool (STT)

5.2 Test Coverage Summary

Form Factor:

D = Desktop, M = Mobile, W = Workstation, A = All in one

Network:

LAN = systems with LAN interface and test is performed using LAN interface

WLAN = systems with WLAN interface and test is performed using the WLAN interface

WLAN* = systems with WLAN interface and test is performed using the WLAN interface, only if the WLAN card supports Host Wake on WLAN.

Test ID	Test Case Title	PETS/Manual	Form Factor	Network
BIOS_01	End of POST	PETS/Manual	D M W A	LAN+WLAN; WLAN only
BIOS_02	CF9GR locking/unlocking - non Manufacturing Mode	PETS/Manual	D M W A	LAN+WLAN; WLAN only
BIOS_03	DRAM INIT Done	PETS/Manual	D M W A	LAN+WLAN; WLAN only
BIOS_05	PCI SID and SVID programming (Not available in wireless only due to firmware implementation.)	PETS/Manual	D M W A	LAN+WLAN; WLAN only
BIOS_06	Intel® MEBX Binary UI	PETS/Manual	D M W A	LAN+WLAN; WLAN only
BIOS_07	Intel® CSME Software Temporary Disable	PETS/Manual	D M W A	LAN+WLAN; WLAN only
BIOS_08	Intel® CSME BIOS Extension Password reset security mechanism	PETS/Manual	D M W A	LAN+WLAN; WLAN only

**Notes:**

1. All tests in this section apply to LAN/WLAN platforms.
2. BIOS_04: belongs to "Intel® Management Engine
3. (Intel® ME) Manufacturing Mode Compliance—Corporate chapter, available at summary table.

5.3 End of Power-On Self-Test (POST)

Test ID:	BIOS_01
Test Case Title:	End of POST
Mandatory/Optional:	Mandatory
Description:	The system is not in the Intel® CSME manufacturing mode - when the system completes POST, BIOS is required to send an "END_OF_POST" message to the Intel® CSME by means of the Intel® MEI when the system is transitioning from S4/S5 to S0.
Objective:	<p>Verify that the BIOS sends the END_OF_POST message when the platform is transitioning from S4/S5 and before the BIOS boot process is done and the OS starts.</p> <p>If the system is in the Intel® CSME manufacturing mode, END_OF_POST message is optional.</p> <p>Note: Host Firmware Status Register (HFSTS) address space at PCH B0:D22:F0(HFSTS1) register offset 40h [bit 4] can determine if the Intel® CSME is in the 'Manufacturing Mode'. For shipping machine, HFSTS address space at PCH B0:D22:F0(HFSTS1) register offset 40h [bit 4] has to be '0'.</p>
Procedure:	<ol style="list-style-type: none">1. Boot the system under test to OS.2. Intel® Platform Enablement Test Suite performs the following:<ol style="list-style-type: none">a. For each of the following system transitions:<ol style="list-style-type: none">i. G3 -> S0 (CM-Off->CM0)ii. S5 -> S0 (CM3->CM0)iii. S4 -> S0 (CM3->CM0)b. Boot to OS and verify if END_OF_POST message was sent by BIOS or not.c. Read the PCI address space to verify the Intel® CSME Manufacturing mode bit is set as given below. Refer PCI address space at PCH B0:D22:F0(HFSTS1) register offset 40h [bit 4]. If [bit 4] is equal to '0', it means it's not in the Intel® CSME manufacturing mode. If [bit 4] is equal to '1', it means it's in the Intel® CSME manufacturing mode.
Test Pass/Fail Criteria:	Test passes if the BIOS Mode displays a status of POST Boot when the system is not in the Intel® CSME manufacturing mode. If the system is in the Intel® CSME manufacturing mode, the test fails with a status of system configuration error.

5.4 CF9GR Locking/Unlocking

Test ID:	BIOS_02
Test Case Title:	CF9GR(CF9h Global Reset) locking/unlocking—non Manufacturing Mode
Mandatory/Optional:	Mandatory
Description:	When the system is not in the Intel® CSME manufacturing mode, BIOS must ensure that CF9GR is cleared (PWRMBASE register offset 1048h [20] = '0') and locked (by means of setting PWRMBASE register offset 1048h [bit 31] of the same register to '1'), in order to prevent the host from issuing global resets and resetting Intel® CSME before handing control to the OS.



Test ID:	BIOS_02
Objective:	For security reasons, the BIOS must ensure that CF9GR is cleared and locked before handing control to the OS in the shipping machine (Intel® CSME not in manufacturing mode). Note. The recommended allocation of PWRMBASE is 0xFE000000 in PCH BIOS Specification.
Procedure:	<ol style="list-style-type: none"> 1. Manually read the PCI address space to verify the Intel® CSME Manufacturing Mode bit at PCH B0:D22:F0 register offset 40h [bit 4] is equal to '0'. 2. Manually read the memory-mapped address at PWRMBASE register offset 1048h [bit 20] to verify the bit is set to '0'. 3. Manually read the memory-mapped address at PWRMBASE register offset 1048h [bit 31] = '0' to verify the bit is set to '1'.
Test Pass/Fail Criteria:	Test passes if the PWRMBASE register offset 1048h [bit 20] = '0' and bit 31 of the same register is '1' when the system is not in the Intel® CSME Manufacturing Mode.

5.5 DRAM INIT Done

Test ID:	BIOS_03
Test Case Title:	DRAM INIT Done
Mandatory/Optional:	Mandatory
Description:	The BIOS is required to send the DRAM INIT Done message which belongs to MKHI_OSBUP_COMMON_GROUP. This message is sent by the BIOS prior to the End of Post (EOP) on the boot where host wants to indicate to Intel® CSME firmware that DRAM initialization is complete and CSME UMA is ready to use.
Objective:	Verify that the BIOS sends the DRAM INIT Done message and the Intel® CSME transitions to CM0 with UMA.
Procedure:	<ol style="list-style-type: none"> 1. For each of the following system transitions: <ol style="list-style-type: none"> a. G3 -> S0 (CM-Off->CM0) b. S5 -> S0 (CM3->CM0) c. S4 -> S0 (CM3->CM0) <p>Boot to OS and read the PCI address space B0:D22:F0 to verify the Intel® CSME HFSTS1 at offset 40h [bits 8:6]. If [bits 8:6] are equal to '001', it means Intel® CSME has transitioned to CM0 with UMA. If [bits 8:6] are equal to '000', it means the Intel® CSME is not using UMA and is not in a valid state.</p>
Test Pass/Fail Criteria:	Test passes if the Intel® CSME transitions to CM0 with UMA for the system transitions listed above ¹ .

Note: ¹Check for "CM0 with UMA" state once CSME exits from "CM0-PG" state.



5.6 PCI SID and SVID Programming

Test ID:	BIOS_05
Test Case Title:	PCI SID and SVID programming
Mandatory/Optional:	Mandatory
Description:	Verify that valid values are specified for the SID and SVID for PCI devices
Objective:	Verify that the BIOS programs the Subsystem ID (SID) and Subsystem Vendor ID (SVID) of the Intel® MEI and KT devices to be compliant with the PCI Specification requirement that SID and SVID must be non-zero and Read-Only. Intel® MEI device is in PCI B0:D22:F0 and Intel® CSME SOL(KT) device is in PCI B0:D22:F3.
Procedure:	<ol style="list-style-type: none">1. Configure the Intel® CSME platform.2. Enable the Intel® AMT and Intel® CSME SOL functionalities through the Intel® MEBX.3. Intel® Platform Enablement Test Suite analyzes and verify the Intel® Intel® MEI/ SOL SID and SVID fields are not zero.
Test Pass/Fail Criteria:	Test passes with the tool reports non-zero values for the SID and SVID fields.

5.7 Intel® MEBX Binary UI

Test ID:	BIOS_06
Test Case Title:	Intel® MEBX Binary UI
Mandatory/Optional:	Mandatory
Description:	OEM must provide a method to allow the user to invoke the Intel® MEBX UI when requested. OEMs are now using non-verbose or silent mode for Intel® MEBX invocation to reduce BIOS POST time, and the traditional method of CTRL+P has been replaced by many OEMs in favor of their own hot-key.
Objective:	This test is to verify that the BIOS provides a mechanism for the Intel® MEBX UI to be invoked.
Procedure:	In an Intel® CSME enabled system, following the OEM instructions to verify the Intel® MEBX UI can be entered on the system transitions.
Test Pass/Fail Criteria:	Test passes if the Intel® MEBX UI can be invoked in the following system transitions: <ol style="list-style-type: none">a. First System Boot - After flashing the system or performing clear CMOS.b. G3 -> S0 (CM-Off->CM0)c. S5 -> S0 (CM3->CM0)d. S4 -> S0 (CM3->CM0) Test fails if the Intel® MEBX UI can be invoked in the S3 -> S0 system transition.



5.8 Intel® CSME Temporary Disable

Test ID:	BIOS_07
Test Case Title:	Intel® CSME Software Temporary Disable
Mandatory/Optional:	Optional
Description:	BIOS should not send any Intel® MEI messages when the Intel® CSME firmware is in software temporary disable mode.
Objective:	If the SUT supports the ability to put the Intel® CSME in the software temporary disable mode, enable this feature using the option (typically a BIOS Setup option). The system BIOS must boot without any halt or long delays.
Procedure:	<ol style="list-style-type: none"> 1. Boot the machine. 2. Enable the Intel® CSME software temporary disable mode using the SUT provided method. A subsequent reboot occurs. 3. The Intel® CSME enters the software temporary disable mode. 4. The BIOS should not send any Intel® MEI message except for the DRAM INIT Done message and set the Intel® CSME enable message. BIOS should not prompt the Intel® MEBX hotkey entrance. No Intel® MEBX is allowed when the system runs in software temporary disable mode. 5. The system can boot to OS successfully. 6. Restore the Intel® CSME to normal mode by disabling the Intel® CSME software temporary disable mode by using the SUT provided method. A subsequent reboot occurs. 7. The Intel® CSME enters the normal mode. 8. The system can boot to OS successfully.
Test Pass/Fail Criteria:	Test passes if the BIOS can boot to OS successfully without noticeable delays (5 second delays for Intel® MEI message timeout) and no error messages are printed to the SUT console when the Intel® CSME is in software temporary disable mode.

5.9 Intel® MEBX BIOS Extension Password Reset Security Mechanism

Test ID:	BIOS_08
Test Case Title:	Intel® CSME BIOS Extension Password reset security mechanism
Mandatory/Optional:	Optional
Description:	<p>The initiation of the Intel® CSME BIOS Extension password reset process must be protected with one of the following:</p> <ul style="list-style-type: none"> • Hardware mechanism that is, user must open the computer chassis and change the Hardware settings • A CMOS clear • A BIOS setup option



Test ID:	BIOS_08
Objective:	Verify that the platform has a mechanism to un-provision without a strong password. for example Open the computer chassis to do a CMOS clear or a BIOS setup option.
Procedure:	This would depend on the platform implementation
Test Pass/Fail Criteria:	<p>Test passes, if there is a mechanism in such as using the NVRAM to un-provision the system and also restore back to factory default password (which has been set at closemfn process) without a strong password.</p> <p>Note:</p> <ol style="list-style-type: none">1. Due to the Password encryption with unique hash calculation on different platform, Default password hash differs irrespective to the password key value in different platforms.2. Change in the hashed password subjects to password update with in the platform.

§ §



6 Common Services

This chapter covers Intel® AMT and Intel® ME related features and technologies. Among those are the following features which require BIOS and/or system integration:

- Intel® AMT Wireless Network
- Intel® ME Firmware Update and Partial Firmware Update
- USB Key Based Configuration
- Remote and Host Based Configuration

6.1 Test System Configuration

Each test in this chapter contains a table describing the system configuration to which the test is applicable. Below is an example environment for a given test:

Form Factor	System Power Model	Intel® AMT Network Interface
<input checked="" type="checkbox"/> Desktop <input checked="" type="checkbox"/> Workstation <input checked="" type="checkbox"/> Mobile	<input checked="" type="checkbox"/> Standard <input checked="" type="checkbox"/> Modern Standby or InstantGo*	<input type="checkbox"/> LAN <input type="checkbox"/> Either Used <input type="checkbox"/> WLAN <input checked="" type="checkbox"/> Not Used

Form Factor: Describes the kind of system for which the test is applicable. These tests cover feature availability for associated platform. Note that for Workstation form factors, the term 'Intel® AMT Server' may be also used for systems which support Intel® AMT and run a server operating system.

System Power Model: Describes under which System Power Model the test is applicable under. A system with 'Standard' configuration follows traditional OS power model wherein sending the system to Sleep results in a S3 resting system state. Systems that support Modern Standby or Microsoft Windows* InstantGo* moves to S0 Low Power Idle state upon being sent to Sleep. This is usually defined by feature support relative to the operating system in conjunction with BIOS and system device support, but may also be due to the nature of the operating system itself relative to the goals of the test.

Intel® AMT Network Interface: Describes the Intel® AMT networking interface used by the test, if any. 'LAN' and 'WLAN' indicate that the test is explicitly using the respective LAN and/or wireless LAN (WLAN) interface. 'Either Used' indicates that an Intel® AMT network interface is used during the test, but the test itself is not specifically define which specific interface is to be used. 'Not Used' indicates that the test procedure does not rely on the Intel® AMT network interface; even though Intel® Platform Enablement Test Suite (Intel® PETS) or other test methodology may require general networking access to the SUT. Note that not all Workstation and Intel® AMT Server designs may have Intel® AMT wireless LAN interface support.

6.2 Test Coverage Summary

The following describes columns in the test coverage summary below. The **Test ID** is the reference identifier for the test in this document and any related tools which reference this document. The **Title** is the name of the test. The **Req.** (Requirement) column describes the requirement for test execution. The **Form Factor**, **OS** (Operating System), and **Net** (Intel® AMT Network Interface) indicate the applicable test system configuration (Refer [Section 6.1](#) for details). **How?** column describes the test methodology.



Req.: M = Mandatory, C = Conditional[†], and O = Optional

[†] Considered the same as Mandatory but with exemptions. Refer test for details.

Form Factor: D = Desktop, M = Mobile, and W = Workstation

Power Model: S = Standard, and M/I = Modern Standby or Microsoft Windows* InstantGo* (refer above for details)

Net: L = LAN, W = WLAN, E = Either Used, and N = Not Used

How?: A = Fully automated using Intel® PETS, I = Interactive using Intel® PETS automation, and M = Manual

Table 6-1. Intel® AMT Test Coverage Summary

Test ID	Title	Req.	Form Factor D M W	Power Model S M/I	Net	How?
Intel® AMT Wireless Network						
CS_001	Host Control Mode Operation	C	☑ ☑ ☑	☑ ☑	W	I
CS_002	Host Control Mode Operation with Intel® AMT Wireless Network Support Disabled	C	☑ ☑ ☑	☑ ☑	W	A
CS_003	Intel® ME Control Mode Operation with Host OS	C	☑ ☑ ☑	☑ ☑	W	A
CS_004	Intel® ME Control Mode Operation with BIOS	C	☑ ☑ ☑	☑ ☑	W	I
CS_005	Intel® ME Control Mode Operation with Access Point Profile Switching	C	☑ ☑ ☑	☑ ☑	W	I
CS_006	Intel® ME Control Mode Operation after Host Profile Synchronization	C	☑ ☑ ☑	☑ ☑	W	I
CS_007	Intel® ME Control and Host Control Mode Toggle	C	☑ ☑ ☑	☑ ☑	W	A
CS_008	Software Radio Frequency Kill (RF-Kill)	C	☑ ☑ ☑	☑ ☑	W	I
CS_009	Hardware Radio Frequency Kill (RF-Kill)	C	☑ ☑ ☑	☑ ☑	W	I
CS_010	Software and Hardware Radio Frequency Kill (RF-Kill)	C	☑ ☑ ☑	☑ ☑	W	I
Intel® ME Firmware Update and Partial Firmware Update						
CS_020	Intel® ME Firmware Update	C	☑ ☑ ☑	☑ ☑	N	I
CS_021	Intel® ME Firmware Partition Update for Secure Output Locale	M	☑ ☑ ☑	☑ ☑	N	I
CS_022	Intel® ME Firmware Partition Update for WLAN µCode	C	☑ ☑ ☑	☑ ☑	W	I
USB Key Based Configuration						
CS_030	USB Key File Version 2.1 with Consumable Record	M	☑ ☑ ☑	☑ ☑	E	I
CS_031	USB Key File Version 2.1 with Non-Consumable Record	M	☑ ☑ ☑	☑ ☑	E	I
CS_032	USB Key File Version 3 with Consumable Record	M	☑ ☑ ☑	☑ ☑	E	I
CS_033	USB Key File Version 4 with Consumable Record	M	☑ ☑ ☑	☑ ☑	E	I
CS_034	USB Key with Multiple Consumable Records	M	☑ ☑ ☑	☑ ☑	E	I
CS_035	USB Key File Configuration Process Cancellation	M	☑ ☑ ☑	☑ ☑	E	I
CS_036	USB Key Drive Compliancy	M	☑ ☑ ☑	☑ ☑	E	I
CS_037	USB Key File Configuration Disabled at Factory Default	M	☑ ☑ ☑	☑ ☑	E	I
Remote and Host Based Configuration						
CS_040	Remote Configuration Support	C	☑ ☑ ☑	☑ ☑	E	A
CS_041	Host Based Configuration Support	M	☑ ☑ ☑	☑ ☑	E	A

**Table 6-1. Intel® AMT Test Coverage Summary**

Test ID	Title	Req.	Form Factor D M W	Power Model S M/I	Net	How?
CS_042	Embedded Host Based Configuration Support	O	☑ ☑ ☑	☑ ☑	E	A

6.2.1 Test Environment Setup

When completing tests within this chapter, especially those which send the system to a specific S-state (S3, S4, S5, DeepSx, etc.), it is important to ensure that the network wake events are properly configured for each applicable device (LAN and/or WLAN).

If not properly configured, the system may wake from a given S-state unexpectedly during test execution as a result of various network traffic within the test environment, and cause the test to result in a *false failure*.

The following Host OS LAN/WLAN driver settings allow the network device to process specific network frames **without** waking the system where supported.

- ARP (Address Resolution Protocol) offload should be **enabled**
- NS (Neighbor Solicitation) offload should be **enabled**

The following Host OS LAN/WLAN driver settings allow the network device to wake the system, where supported, when specific network frames are received.

- Wake on Magic Packet should be **disabled**
- Wake on Pattern Match should be **disabled**
- Wake on Magic Packet from power off state should be **disabled**

Note: The wording used for the Host OS driver settings above may vary, and in some cases may not be available depending on driver support or system configuration.

Beyond the guidance in this section, refer individual test setup information for details on specifically when to enable relevant wake functionality in the network device, as applicable to the test. In all other cases, the above settings should be applied by default.

6.3 Intel® AMT Wireless Network

The section serves as a checklist for the environment setup and testing of Intel® AMT Wireless Network feature support.

6.3.1 Test Environment

The System Under Test (SUT) is to be configured with Intel® AMT set in manual provisioning mode with static IP address or DHCP. The management console may be a laptop or a desktop with a version of Windows* supported by Intel® PETS, and the SUT should have a version of Windows* supported by Intel® PETS as well. The test network is comprised of a hub/switch and network cables. The SUT should have only one HDD.

6.3.2 Special Terminology

Host Control: The Host WLAN driver has ownership over the WLAN NIC and ensures proper network support for both the Host OS and, if enabled, Intel® AMT.



Intel® ME Control: The Host WLAN driver disabled, or missing, or otherwise unavailable. In this mode, the Intel® ME takes ownership over the WLAN NIC to ensure OOB manageability when Intel® AMT Wireless Network support is enabled.

Web UI: The web-based interface on a system with Intel® AMT provisioned. While secure HTTP is available, the Web UI is also commonly accessible by means of HTTP as follows:

- Remotely: `http://<host_name>:16992/` or `http://<host_ip_address>:16992/`
- Locally: `http://127.0.0.1:16992/` or `http://localhost:16992/` after the Local Manageability Service (LMS) has started. Note: To force the LMS to start on the SUT, run the Intel® Management and Security Status (Intel® MSS), otherwise, wait 3-4 minutes after boot for the service to start automatically.

6.3.3 Intel® AMT Wireless Interface Setup

The Web UI may be used to enable the Intel® AMT wireless network interface via the *Wireless Settings* page. Under *Wireless Management* choose one of the following Link Policies:

Link Policy 2: Enabled in S0

Link Policy 3: Enabled in S0, Sx/AC

Note: **Link Policy 1** means Intel® AMT wireless network interface is **disabled**.

After setting the Link Policy, a wireless profile must be registered into Intel® AMT in order to enable WLAN connectivity when the system is in S3, S4, or S5 (or in S0 when the Host WLAN driver is not available). This can also be done via the *Wireless Settings* page. Under *Profile Management* click *New...* to create a new wireless profile with associated security settings and pass phrase. For details, refer the *Intel® AMT OEM Web User Interface Guide* included in the firmware kit.

In order to complete wireless connectivity support for Intel® AMT, the appropriate Host WLAN driver supporting manageability must also be installed on the Host OS.

Warning:

Unless specifically designated by the test configuration setup itself, the wireless LAN network security configuration settings used for testing wireless Intel® AMT must match in **both** the Intel® AMT and the Host OS driver configurations. This includes both:

- **Network Authentication** method (WPA-PSK known as *Wi-Fi Protected Access Pre-Shared Key*, or RSN-PSK known as *Robust Security Network Pre-Shared Key*)
- **Encryption** method (TKIP known as *Temporal Key Integrity Protocol*, or CCMP known as *Counter CBC-MAC Protocol* or AES)

Problems may occur in testing if both the Network Authentication and Encryption methods do not align. When testing on Microsoft Windows* environments, the Host OS may default to the highest Encryption level supported by the Access Point when connecting to it for the first time. If the Access Point supports multiple Encryption (TKIP and CCMP) protocols at the same time, there is the risk that the Host OS select CCMP (AES) automatically while the test operator selects TKIP. This is considered a wireless security configuration mismatch and should be fixed before starting testing.

With the Intel® AMT Link Policy is set to 2 or 3 (wireless manageability support enabled), the Host WLAN driver installed, and the Host OS connected to a wireless access point, the Web UI show the assigned Intel® AMT wireless network IP address on the *System Status* screen when the system is in S0.



With the Intel® AMT Link Policy is set to 1 (wireless manageability support disabled), the Web UI shows no wireless network IP address on the *System Status* screen. To clear any Intel® AMT wireless configuration previously entered, the Access Point profiles registered on the *Wireless Settings* page should be deleted. Note that it is only possible to delete an Access Point profile if it is not in use by Intel® AMT.

Note: To thoroughly clear and reset the Intel® AMT wireless network configuration, use either the Intel® Management Engine BIOS Extension (Intel® MEBX) full unprovision menu, the CMOS clear mechanism, or the BIOS unconfigure without password mechanism. Refer the *Intel® Management Engine BIOS Extension User's Guide* or *Intel® ME BIOS Writers Guide* documents for details.

When the system is in Sx, or the Host WLAN driver is not functional, the wireless profile registered to Intel® AMT, via the Web UI, is used for enabling wireless manageability support.

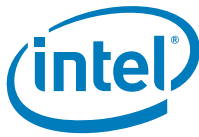
6.3.3.1 Common Issues and Troubleshooting

The following is a list of common issues that can occur during wireless Intel® AMT testing and associated recommendations on how to check test environment and system configuration. Before checking S3-related issues, review the *Intel® AMT and Wake On Wireless LAN Coexistence* feature overview.

1. Cannot connect to the Web UI locally from the SUT.
 - a. Verify that the LMS (Local Manageability Service) service is installed and running on the SUT. If necessary, restart the service to verify that connectivity can be restored.
 - b. Verify access using an alternate Web browser on the SUT.
2. There is no *Wireless Settings* menu in the Web UI, the data shown on the *Wireless Settings* page is incorrect, or the controls on the *Wireless Settings* page are not behaving as expected.
 - a. Verify that a wireless LAN card supporting Intel® vPro™ Technology is installed in the system.
 - b. Verify that the *WLAN Power Well* configuration is correctly set in the SPI image. Refer the firmware *Bring Up Guide* included with the firmware kit for details.
 - c. Verify that the correct wireless LAN uCode is installed in the firmware. Refer the *Intel® ME System Tools User Guide* for details on how to verify that there is no wireless LAN uCode mismatch and how to manually update the wireless LAN uCode.
 - d. Verify that the C-Link (Controller Link) hardware interface is properly connected to the WLAN NIC and that it is functional. Refer the *Platform Controller Hub External Design Specification* for details.
3. The *System Status* screen on the Web UI shows that there is no IP address for the wireless interface when the system is in S0, S0ix (Microsoft InstantGo* mode), or S3 with Wake On Wireless LAN Coexistence **enabled**.

Note that it may take a few seconds for the Host WLAN driver to synchronize IP and MAC address information with the Intel® ME firmware. As such, a few refreshes of the Web UI may be needed after the system completes transition to the destination S-state.

- a. Verify that the correct Intel® Wireless LAN Host OS driver is installed and that it supports Intel® vPro™ Technology with Intel® AMT.
- b. Verify that the Host OS is connected to an Access Point which supports either WPA-PSK or RSN-PSK network authentication, and either TKIP or CCMP (AES) encryption.



- c. Verify that the wireless Link Policy is **not** set to Link Policy 1 (disabled) in the Web UI.
4. The *System Status* screen on the Web UI shows that there is no IP address for the wireless interface when the system is in S4, S5, or S3 with Wake On Wireless LAN Coexistence **disabled**.
 - a. Verify that the wireless Link Policy is **not** set to Link Policy 1 (disabled) in the Web UI.
 - b. Verify that the an Access Point which supports either WPA-PSK or RSN-PSK network authentication, and either TKIP or CCMP (AES) encryption is registered with Intel® AMT. This can be done through the Web UI.
5. Cannot connect to the Web UI remotely or KVM/Storage/SoL redirection does not function while the system is in S0, S0ix (Microsoft InstantGo* mode), or S3 with Wake On Wireless LAN Coexistence **enabled**.
 - a. Verify that the Intel® AMT has received an IP address from the Host OS driver while in S0. This can be done through the Web UI.
 - b. If the system is booted to an OS which does not have an Intel® Wireless LAN Host OS driver which supports Intel® vPro™ Technology with Intel® AMT installed, wait 2 minutes. If the Intel® Wireless LAN driver does not take ownership of the WLAN NIC within 2 minutes after power-on, the Intel® ME attempt to take ownership and try to connect to the Access Points registered within Intel® AMT (via the Web UI).
6. Cannot connect to the Web UI remotely or KVM/Storage/SoL redirection does not function while the system is in S5, S4, or S3 (regardless of Wake On Wireless LAN Coexistence configuration).
 - a. Verify that the correct wireless LAN uCode is installed in the firmware. Refer the *Intel® ME System Tools User Guide* for details on how to verify that there is no wireless LAN uCode mismatch and how to manually update the wireless LAN uCode.
 - b. Verify that the WLAN NIC is powered by the EC/BIOS when SLP_WLAN# is de-asserted high. Refer the *Platform Controller Hub External Design Specification* for details.
 - c. Verify that the RF-Kill (W_DISABLE#) signal to the WLAN NIC is not asserted low by the EC/BIOS.
 - d. If the SUT is running Microsoft* Windows* 10, verify that the random hardware addresses (MAC address) Wi-Fi setting is **disabled**. Intel® AMT wireless feature coexistence is not available for this Host OS feature. For more information about this Host OS feature, refer the Windows* 10 Wi-Fi settings and documentation provided by Microsoft.
7. The KVM/Storage/SoL redirection is lost during system reboot or during transition from Sx to S0.
 - a. Verify that the Host OS wireless and Intel® AMT wireless network security configurations match.

6.3.4 Host Control Mode Operation

ID:	CS_001
Title:	Host Control Mode Operation
Requirement:	Mandatory - exempt for systems without Intel® AMT WLAN support



ID:	CS_001				
System:	Form Factor		System Power Model	Intel® AMT Network Interface	
	<input checked="" type="checkbox"/> Desktop <input checked="" type="checkbox"/> Mobile	<input checked="" type="checkbox"/> Workstation	<input checked="" type="checkbox"/> Standard <input checked="" type="checkbox"/> Modern Standby or InstantGo*	<input type="checkbox"/> LAN <input checked="" type="checkbox"/> WLAN	<input type="checkbox"/> Either Used <input type="checkbox"/> Not Used
Method:	Automated by Intel® PETS with test operator interaction				
Description:	Intel® AMT connects over wireless LAN in S0 when the Host WLAN driver has control over the WLAN NIC.				
Objective:	Verify that the Intel® AMT connection over wireless LAN in S0 occurs when the Host WLAN driver is operational and connected to an Access Point.				
Setup:	<p>The initial state of the SUT should be S0/MeOn with Host OS running. Intel® AMT should be provisioned via manual mode. Intel® AMT wireless should not be configured or operational.</p> <p>If the SUT has already been configured, either unprovision/re-provision the SUT to clear the wireless network configuration, or disable and completely clear the wireless network configuration via the Web UI (Refer Section 6.3.3 for details).</p>				
Procedure:	<ol style="list-style-type: none"> 1. Verify that the Host WLAN driver is enabled. 2. Configure the Host OS to connect to an Access Point which supports either WPA-PSK (Wi-Fi Protected Access Pre-Shared Key) or RSN-PSK (Robust Security Network Pre-Shared Key) authentication, and either TKIP (Temporal Key Integrity Protocol) or CCMP (Counter CBC-MAC Protocol) encryption. 3. Verify the Host OS receives an IP address on the Access Point. 4. Ping the SUT from the management console via the wireless network interface. Note, this may require disabling firewall, anti-virus, or other software, and/or performing other configuration on the Host OS of the SUT to enable ping receipt and response. 5. Open the Web UI from the SUT locally (refer Section 6.3.2 for details) and confirm Intel® AMT wireless does not have a network IP address on the <i>System Status</i> page. 6. Follow the instructions in section Section 6.3.3 for enabling wireless network connectivity via Link Policy 2 or 3 setting in the Web UI. 7. Open the Web UI on the SUT remotely from the management console via the wireless interface (refer Section 6.3.2 for details) and confirm the Intel® AMT wireless network IP address on the <i>System Status</i> page. 				
Pass Criteria:	The test passes if Intel® AMT responds over the wireless network when the Host WLAN driver controls the WLAN NIC in Host Control mode.				
References:	For details on Intel® AMT Web UI access or Wireless Setting configuration, refer the <i>Intel® AMT OEM Web User Interface Guide</i> .				

6.3.5 Host Control Mode Operation without Intel® AMT Wireless Network Enabled

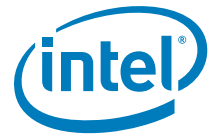
ID:	CS_002				
Title:	Host Control Mode Operation with Intel® AMT Wireless Network Support Disabled				
Requirement:	Mandatory - exempt for systems without Intel® AMT WLAN support				
System:	Form Factor		System Power Model	Intel® AMT Network Interface	
	<input checked="" type="checkbox"/> Desktop <input checked="" type="checkbox"/> Mobile	<input checked="" type="checkbox"/> Workstation	<input checked="" type="checkbox"/> Standard <input checked="" type="checkbox"/> Modern Standby or InstantGo*	<input type="checkbox"/> LAN <input checked="" type="checkbox"/> WLAN	<input type="checkbox"/> Either Used <input type="checkbox"/> Not Used
Method:	Automated by Intel® PETS				
Description:	Intel® AMT would not connect over wireless LAN in S0 when the Link Policy is set to 1 (Disabled).				
Objective:	Verify that there is no Intel® AMT connection over wireless LAN in S0 when the Host WLAN driver is operational and connected to an Access Point, but the Intel® AMT wireless network interface is disabled.				



ID:	CS_002
Setup:	The initial state of the SUT should be S0/MeOn with Host OS running. Intel® AMT should be provisioned via manual mode. Intel® AMT wireless should be configured and operational (refer Section 6.3.3 for details).
Procedure:	<ol style="list-style-type: none">1. Open the Web UI from the SUT locally (refer Section 6.3.2 for details) and confirm Intel® AMT wireless has a network IP address on the <i>System Status</i> page.2. Follow the instructions in section Section 6.3.3 to disable wireless network connectivity via Link Policy 1 (Disabled) setting in the Web UI.3. Confirm Intel® AMT wireless does not have a network IP address on the <i>System Status</i> page in the Web UI.4. Attempt to open the Web UI on the SUT remotely from the management console via the wireless interface (refer Section 6.3.2 for details). This test step should fail.5. Ping the SUT from the management console via the wireless network interface. Note, this may require disabling firewall, anti-virus, or other software, and/or performing other configuration on the Host OS of the SUT to enable ping receipt and response.
Pass Criteria:	The test passes if Intel® AMT access is no longer available over the wireless network when the Host WLAN driver controls the WLAN NIC in Host Control mode with Intel® AMT wireless network support disabled. In this configuration, the Host OS must still receive wireless network support via the Host WLAN driver.
References:	For details on Intel® AMT Web UI access or Wireless Setting configuration, refer the <i>Intel® AMT OEM Web User Interface Guide</i> .

6.3.6 Intel® ME Control Mode Operation with Host OS

ID:	CS_003																			
Title:	Intel® ME Control Mode Operation with Host OS																			
Requirement:	Mandatory - exempt for systems without Intel® AMT WLAN support																			
System:	<table><tr><th colspan="2">Form Factor</th><th>System Power Model</th><th colspan="2">Intel® AMT Network Interface</th></tr><tr><td><input checked="" type="checkbox"/> Desktop</td><td><input checked="" type="checkbox"/> Workstation</td><td><input checked="" type="checkbox"/> Standard</td><td><input type="checkbox"/> LAN</td><td><input type="checkbox"/> Either Used</td></tr><tr><td><input checked="" type="checkbox"/> Mobile</td><td></td><td><input checked="" type="checkbox"/> Modern Standby or InstantGo*</td><td><input checked="" type="checkbox"/> WLAN</td><td><input type="checkbox"/> Not Used</td></tr></table>					Form Factor		System Power Model	Intel® AMT Network Interface		<input checked="" type="checkbox"/> Desktop	<input checked="" type="checkbox"/> Workstation	<input checked="" type="checkbox"/> Standard	<input type="checkbox"/> LAN	<input type="checkbox"/> Either Used	<input checked="" type="checkbox"/> Mobile		<input checked="" type="checkbox"/> Modern Standby or InstantGo*	<input checked="" type="checkbox"/> WLAN	<input type="checkbox"/> Not Used
Form Factor		System Power Model	Intel® AMT Network Interface																	
<input checked="" type="checkbox"/> Desktop	<input checked="" type="checkbox"/> Workstation	<input checked="" type="checkbox"/> Standard	<input type="checkbox"/> LAN	<input type="checkbox"/> Either Used																
<input checked="" type="checkbox"/> Mobile		<input checked="" type="checkbox"/> Modern Standby or InstantGo*	<input checked="" type="checkbox"/> WLAN	<input type="checkbox"/> Not Used																
Method:	Automated by Intel® PETS																			
Description:	Intel® AMT connect over wireless LAN in S0 when the Host WLAN driver is disabled or not installed.																			
Objective:	Verify that the Intel® AMT connection over wireless LAN in S0 occurs when the Host WLAN driver is disabled or not installed.																			
Setup:	The initial state of the SUT should be S0/MeOn with Host OS running. Intel® AMT should be provisioned via manual mode. Intel® AMT wireless should be configured and operational (refer Section 6.3.3 for details).																			
Procedure:	<ol style="list-style-type: none">1. Wait 2 minutes before starting the test after the Host OS loads to allow entry into Host Control mode.2. Open the Web UI from the SUT locally (refer Section 6.3.2 for details) and confirm Intel® AMT wireless has a network IP address on the <i>System Status</i> page.3. Open the Host OS device manager on the SUT and disable the Host WLAN driver.4. Wait 1 minute as the SUT moves into Intel® ME Control mode.5. Open the Web UI on the SUT remotely from the management console via the wireless interface (refer Section 6.3.2 for details) and confirm the Intel® AMT wireless network IP address on the <i>System Status</i> page.6. In the Host OS device manager on the SUT, re-enable the Host WLAN driver.																			
Pass Criteria:	The test passes if Intel® AMT responds over the wireless network when the Host WLAN driver is disabled (or not installed).																			
References:	For details on Intel® AMT Web UI access or Wireless Setting configuration, refer the <i>Intel® AMT OEM Web User Interface Guide</i> .																			



6.3.7 Intel® ME Control Mode Operation with BIOS

ID:	CS_004				
Title:	Intel® ME Control Mode Operation with BIOS				
Requirement:	Mandatory - exempt for systems without Intel® AMT WLAN support				
System:	Form Factor		System Power Model	Intel® AMT Network Interface	
	<input checked="" type="checkbox"/> Desktop <input checked="" type="checkbox"/> Mobile	<input checked="" type="checkbox"/> Workstation	<input checked="" type="checkbox"/> Standard <input checked="" type="checkbox"/> Modern Standby or InstantGo*	<input type="checkbox"/> LAN <input checked="" type="checkbox"/> WLAN	<input type="checkbox"/> Either Used <input type="checkbox"/> Not Used
Method:	Automated by Intel® PETS with test operator interaction				
Description:	Intel® AMT connects over wireless LAN in S0 when there is no Host OS.				
Objective:	Verify that the Intel® AMT connection over wireless LAN in S0 occurs when there is no Host OS and WLAN device driver loaded 2 minutes after boot.				
Setup:	The initial state of the SUT should be S0/MeOn with Host OS running. Intel® AMT should be provisioned via manual mode. Intel® AMT wireless should be configured and operational (refer Section 6.3.3 for details).				
Procedure:	<ol style="list-style-type: none"> 1. Turn on the SUT to S0, and enter the BIOS menu. 2. Wait at least 2 minutes. 3. Open the Web UI on the SUT remotely from the management console via the wireless interface (refer Section 6.3.2 for details) and confirm the Intel® AMT wireless network IP address on the <i>System Status</i> page 4. Gracefully restart the system back to Host OS. 				
Pass Criteria:	The test passes if Intel® AMT responds over the wireless network when the BIOS is loaded after 2 minutes.				
References:	For details on Intel® AMT Web UI access or Wireless Setting configuration, refer the <i>Intel® AMT OEM Web User Interface Guide</i> .				

6.3.8 Intel® ME Control Mode Operation with Access Point Profile Switching

ID:	CS_005				
Title:	Intel® ME Control Mode Operation with Access Point Profile Switching				
Requirement:	Mandatory - exempt for systems without Intel® AMT WLAN support				
System:	Form Factor		System Power Model	Intel® AMT Network Interface	
	<input checked="" type="checkbox"/> Desktop <input checked="" type="checkbox"/> Mobile	<input checked="" type="checkbox"/> Workstation	<input checked="" type="checkbox"/> Standard <input checked="" type="checkbox"/> Modern Standby or InstantGo*	<input type="checkbox"/> LAN <input checked="" type="checkbox"/> WLAN	<input type="checkbox"/> Either Used <input type="checkbox"/> Not Used
Method:	Automated by Intel® PETS with test operator interaction				
Description:	Intel® AMT connects over wireless LAN in S0 when the Host WLAN driver is disabled or not installed. If there is a second Access Point profile registered with Intel® AMT, it is used when connectivity to the primary Access Point is lost.				
Objective:	Verify that the Intel® AMT connection over wireless LAN in S0 occurs when the wireless connectivity to the primary Access Point is lost in Intel® ME Control mode.				
Setup:	The initial state of the SUT should be S0/MeOn with Host OS running. Intel® AMT should be provisioned via manual mode. Intel® AMT wireless should be configured and operational (refer Section 6.3.3 for details) with at least one Access Point profile registered.				

ID:	CS_005
Procedure:	<ol style="list-style-type: none"> Wait 2 minutes before starting the test after the Host OS loads to allow entry into Host Control mode. Open the Web UI from the SUT locally (refer Section 6.3.2 for details) and confirm Intel® AMT wireless has a network IP address on the <i>System Status</i> page. Take note of the wireless IP address assigned by the current Access Point. If necessary, follow the instructions in section Section 6.3.3 to add a second Access Point profile. There should be at least two Access Point profiles, each with the following different configuration: <ul style="list-style-type: none"> One with WPA-PSK authentication and TKIP encryption. One with RSN-PSK authentication and CCMP encryption. Turn off the radios of the Access Points that the SUT is not connected to. Open the Host OS device manager on the SUT and disable the Host WLAN driver. Wait 1 minute as the SUT moves into Intel® ME Control mode. Open the Web UI from the SUT locally (refer Section 6.3.2 for details) and verify the SUT is connected to the first (and only available) Access Point by attempting to delete its profile via the Web UI. This should fail if Intel® AMT is connected to the associated Access Point. Open the Web UI on the SUT from the management console via the wireless interface (refer Section 6.3.2 for details) and confirm the Intel® AMT wireless network IP address on the <i>System Status</i> page. Turn on the radio of the second Access Point registered with Intel® AMT.
Procedure: (continued)	<ol style="list-style-type: none"> Wait 1 minute. Turn off the radio of the Access Point that the SUT is currently connected to. The Intel® AMT wireless network interface should shift to the second Access Point which was enabled in step 9. Wait 1 minute. Open the Web UI from the SUT locally (refer Section 6.3.2 for details) and confirm Intel® AMT wireless has a network IP address on the <i>System Status</i> page. Take note that the new wireless IP address assigned by the second Access Point may be different than the one assigned by the first Access Point. Open the Web UI on the SUT from the management console via the wireless interface (refer Section 6.3.2 for details) and confirm the Intel® AMT wireless network IP address on the <i>System Status</i> page. In the Host OS device manager on the SUT, re-enable the Host WLAN driver. Restore the radio states of the Access Points as they were before testing started.
Pass Criteria:	The test passes if Intel® AMT responds over the wireless network after the Access Point profile switch has occurred.
References:	For details on Intel® AMT Web UI access or Wireless Setting configuration, refer the <i>Intel® AMT OEM Web User Interface Guide</i> .

6.3.9 Intel® ME Control Mode Operation after Host Profile Synchronization

ID:	CS_006				
Title:	Intel® ME Control Mode Operation after Host Profile Synchronization				
Requirement:	Mandatory - exempt for systems without Intel® AMT WLAN support				
System:	Form Factor		System Power Model	Intel® AMT Network Interface	
	<input checked="" type="checkbox"/> Desktop <input checked="" type="checkbox"/> Mobile	<input checked="" type="checkbox"/> Workstation	<input checked="" type="checkbox"/> Standard <input checked="" type="checkbox"/> Modern Standby or InstantGo*	<input type="checkbox"/> LAN <input checked="" type="checkbox"/> WLAN	<input type="checkbox"/> Either Used <input type="checkbox"/> Not Used
Method:	Automated by Intel® PETS with test operator interaction				
Description:	Intel® AMT connects over wireless LAN in Sx when the Access Point profile has been synchronized from the Host OS via Intel® PROSet software.				
Objective:	Verify that the Intel® AMT connection over wireless LAN in Sx occurs when after the Host WLAN driver is operational and connected to an Access Point, and the Access Point profile has been synchronized via Intel® PROSet software.				



ID:	CS_006
Setup:	The initial state of the SUT should be S0/MeOn with Host OS running. Intel® AMT wireless should not be configured or operational. If the SUT has already been configured, unprovision the SUT to clear the wireless network configuration completely.
Procedure:	<ol style="list-style-type: none"> If Intel® AMT has already been provisioned: <ol style="list-style-type: none"> Restart the SUT, Enter Intel® MEBX and perform a full unprovision, and then Boot the SUT to S0/MeOn with Host OS running. Restart the SUT, and boot into Intel® MEBX: <ol style="list-style-type: none"> Provision Intel® AMT. Set the active power package to Power Package 2 (Intel® ME on in S0, Intel® ME wake in S3, S4-S5). Boot back to the Host OS, and then Run the Intel® MSS to allow fast access to the Web UI locally. Verify that the Host WLAN driver is enabled. Enable Profile sync by executing the WSMAN command on the SUT local host interface. Configure the Host OS to connect to an Access Point, which supports either Wi-Fi Protected Access Pre-Shared Key (WPA-PSK) or Robust Security Network Pre-Shared Key (RSN-PSK) authentication, and either Temporal Key Integrity Protocol (TKIP) or Counter CBC-MAC Protocol (CCMP) encryption. Open the Web UI from the SUT locally (refer Section 6.3.2 for details) and <ol style="list-style-type: none"> Open the Wireless Settings page, and under Wireless Management select 'Enabled in S0, Sx/AC' (Link Policy 3), and click Submit, and then Wait 1 minute for the changes to apply, then confirm Intel® AMT wireless has a network IP address on the System Status page. Shutdown the SUT to S5/MeOn via the Host OS. Open the Web UI on the SUT remotely from the management console via the wireless interface (refer Section 6.3.2 for details) and confirm the Intel® AMT wireless network IP address on the <i>System Status</i> page. Unprovision the system.
Pass Criteria:	The test passes if Intel® AMT responds over the wireless network when the Intel® ME controls the WLAN NIC in Intel® ME Control mode.
References:	For details on Intel® AMT Web UI access or Wireless Setting configuration, refer the <i>Intel® AMT OEM Web User Interface Guide</i> . For details on provisioning Intel® AMT via Intel® MEBX, refer the <i>Intel® Management Engine BIOS Extension User's Guide</i> .

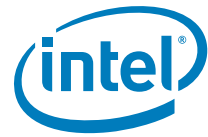
6.3.10 Intel® ME Control and Host Control Mode Toggle

ID:	CS_007				
Title:	Intel® ME Control and Host Control Mode Toggle				
Requirement:	Mandatory - exempt for systems without Intel® AMT WLAN support				
System:	Form Factor		System Power Model		Intel® AMT Network Interface
	<input checked="" type="checkbox"/> Desktop <input checked="" type="checkbox"/> Mobile	<input checked="" type="checkbox"/> Workstation	<input checked="" type="checkbox"/> Standard <input checked="" type="checkbox"/> Modern Standby or InstantGo*	<input type="checkbox"/> LAN <input checked="" type="checkbox"/> WLAN	<input type="checkbox"/> Either Used <input type="checkbox"/> Not Used
Method:	Automated by Intel® PETS				
Description:	Intel® AMT connects over wireless LAN in S0 when the Host WLAN driver is disabled or not installed.				
Objective:	Verify that the Intel® AMT connection over wireless LAN in S0 when moving from Intel® ME Control mode to Host Control mode and back.				
Setup:	The initial state of the SUT should be S0/MeOn with Host OS running. Intel® AMT should be provisioned via manual mode. Intel® AMT wireless should be configured and operational (refer Section 6.3.3 for details).				

ID:	CS_007
Procedure:	<ol style="list-style-type: none"> 1. Wait 2 minutes before starting the test after the Host OS loads to allow entry into Host Control mode. 2. Open the Web UI from the SUT locally (refer Section 6.3.2 for details) and confirm Intel® AMT wireless has a network IP address on the <i>System Status</i> page. 3. Open the Host OS device manager on the SUT and disable the Host WLAN driver. 4. Wait 1 minute as the SUT moves into Intel® ME Control mode. 5. Open the Web UI on the SUT remotely from the management console via the wireless interface (refer Section 6.3.2 for details) and locate the Intel® AMT wireless network IPv4 address on the <i>System Status</i> page. Note the IPv4 address assigned to Intel® AMT while in Intel® ME Control mode. 6. In the Host OS device manager on the SUT, re-enable the Host WLAN driver. 7. Wait 1 minute as the SUT moves into Host Control mode. 8. Again, open the Web UI on the SUT remotely from the management console via the wireless interface and confirm the Intel® AMT wireless network IPv4 address on the <i>System Status</i> page is the same in Host Control mode as it was in Intel® ME control mode. In the case of IPv6, the addresses may be different and should not be used for comparison. 9. In the Host OS device manager on the SUT, disable the Host WLAN driver again.
Procedure: (continued)	<ol style="list-style-type: none"> 10. Wait 1 minute as the SUT moves back into Intel® ME Control mode. 11. Finally, open the Web UI on the SUT remotely from the management console via the wireless interface and confirm the Intel® AMT wireless network IP address on the <i>System Status</i> page. 12. In the Host OS device manager on the SUT, re-enable the Host WLAN driver one final time.
Pass Criteria:	The test passes if Intel® AMT responds over the wireless network when the in both Intel® ME Control mode and Host Control mode.
References:	For details on Intel® AMT Web UI access or Wireless Setting configuration, refer the <i>Intel® AMT OEM Web User Interface Guide</i> .

6.3.11 Software Radio Frequency Kill (RF-Kill)

ID:	CS_008																			
Title:	Software Radio Frequency Kill (RF-Kill)																			
Requirement:	Mandatory - exempt for systems without Intel® AMT WLAN support or software RF-Kill																			
System:	<table><tr><th colspan="2">Form Factor</th><th>System Power Model</th><th colspan="2">Intel® AMT Network Interface</th></tr><tr><td><input checked="" type="checkbox"/> Desktop</td><td><input checked="" type="checkbox"/> Workstation</td><td><input checked="" type="checkbox"/> Standard</td><td><input type="checkbox"/> LAN</td><td><input type="checkbox"/> Either Used</td></tr><tr><td><input checked="" type="checkbox"/> Mobile</td><td></td><td><input checked="" type="checkbox"/> Modern Standby or InstantGo*</td><td><input checked="" type="checkbox"/> WLAN</td><td><input type="checkbox"/> Not Used</td></tr></table>					Form Factor		System Power Model	Intel® AMT Network Interface		<input checked="" type="checkbox"/> Desktop	<input checked="" type="checkbox"/> Workstation	<input checked="" type="checkbox"/> Standard	<input type="checkbox"/> LAN	<input type="checkbox"/> Either Used	<input checked="" type="checkbox"/> Mobile		<input checked="" type="checkbox"/> Modern Standby or InstantGo*	<input checked="" type="checkbox"/> WLAN	<input type="checkbox"/> Not Used
Form Factor		System Power Model	Intel® AMT Network Interface																	
<input checked="" type="checkbox"/> Desktop	<input checked="" type="checkbox"/> Workstation	<input checked="" type="checkbox"/> Standard	<input type="checkbox"/> LAN	<input type="checkbox"/> Either Used																
<input checked="" type="checkbox"/> Mobile		<input checked="" type="checkbox"/> Modern Standby or InstantGo*	<input checked="" type="checkbox"/> WLAN	<input type="checkbox"/> Not Used																
Method:	Automated by Intel® PETS with test operator interaction																			
Description:	Intel® AMT would not connect over wireless LAN in S0 when software RF-Kill is active, regardless of Host Control or Intel® ME Control mode SUT operation.																			
Objective:	Verify that the Intel® AMT does not connect over wireless LAN in S0 in either Host Control or Intel® ME Control mode when software RF-kill is active.																			
Setup:	The initial state of the SUT should be S0/MeOn with Host OS running. Intel® AMT should be provisioned via manual mode. Intel® AMT wireless should be configured and operational (refer Section 6.3.3 for details).																			



ID:	CS_008
Procedure:	<ol style="list-style-type: none"> 1. Wait 2 minutes before starting the test after the Host OS loads to allow entry into Host Control mode. 2. Open the Web UI on the SUT remotely from the management console via the wireless interface (refer Section 6.3.2 for details) and confirm the Intel® AMT wireless network IP address on the <i>System Status</i> page. 3. Disable wireless connectivity on the SUT by applying software RF-Kill. 4. Reload the Web UI from the SUT on the management console and confirm that Intel® AMT wireless network connectivity is not available. 5. Open the Host OS device manager on the SUT and disable the Host WLAN driver. 6. Wait 1 minute as the SUT moves into Intel® ME Control mode. 7. Reload the Web UI from the SUT on the management console and confirm that Intel® AMT wireless network connectivity is not available. 8. In the Host OS device manager on the SUT, re-enable the Host WLAN driver. 9. Enable wireless connectivity on the SUT by canceling software RF-Kill.
Pass Criteria:	The test passes if Intel® AMT does not respond over the wireless network when the SUT is in either Host Control or Intel® ME Control mode with software RF-kill applied
References:	For details on Intel® AMT Web UI access, refer the <i>Intel® AMT OEM Web User Interface Guide</i> .

6.3.12 Hardware Radio Frequency Kill (RF-Kill)

ID:	CS_009																						
Title:	Hardware Radio Frequency Kill (RF-Kill)																						
Requirement:	Mandatory - exempt for systems without Intel® AMT WLAN support or hardware RF-Kill																						
System:	<table border="1"> <thead> <tr> <th colspan="2">Form Factor</th><th colspan="2">System Power Model</th><th colspan="2">Intel® AMT Network Interface</th></tr> </thead> <tbody> <tr> <td><input checked="" type="checkbox"/> Desktop</td><td><input checked="" type="checkbox"/> Workstation</td><td><input checked="" type="checkbox"/> Standard</td><td><input checked="" type="checkbox"/> Modern Standby or InstantGo*</td><td><input type="checkbox"/> LAN</td><td><input type="checkbox"/> Either Used</td></tr> <tr> <td><input checked="" type="checkbox"/> Mobile</td><td></td><td><input checked="" type="checkbox"/> Modern Standby or InstantGo*</td><td></td><td><input checked="" type="checkbox"/> WLAN</td><td><input type="checkbox"/> Not Used</td></tr> </tbody> </table>					Form Factor		System Power Model		Intel® AMT Network Interface		<input checked="" type="checkbox"/> Desktop	<input checked="" type="checkbox"/> Workstation	<input checked="" type="checkbox"/> Standard	<input checked="" type="checkbox"/> Modern Standby or InstantGo*	<input type="checkbox"/> LAN	<input type="checkbox"/> Either Used	<input checked="" type="checkbox"/> Mobile		<input checked="" type="checkbox"/> Modern Standby or InstantGo*		<input checked="" type="checkbox"/> WLAN	<input type="checkbox"/> Not Used
Form Factor		System Power Model		Intel® AMT Network Interface																			
<input checked="" type="checkbox"/> Desktop	<input checked="" type="checkbox"/> Workstation	<input checked="" type="checkbox"/> Standard	<input checked="" type="checkbox"/> Modern Standby or InstantGo*	<input type="checkbox"/> LAN	<input type="checkbox"/> Either Used																		
<input checked="" type="checkbox"/> Mobile		<input checked="" type="checkbox"/> Modern Standby or InstantGo*		<input checked="" type="checkbox"/> WLAN	<input type="checkbox"/> Not Used																		
Method:	Automated by Intel® PETS with test operator interaction																						
Description:	Intel® AMT would not connect over wireless LAN in S0 when hardware RF-Kill is active, regardless of Host Control or Intel® ME Control mode SUT operation.																						
Objective:	Verify that the Intel® AMT does not connect over wireless LAN in S0 in either Host Control or Intel® ME Control mode when hardware RF-kill is active.																						
Setup:	The initial state of the SUT should be S0/MeOn with Host OS running. Intel® AMT should be provisioned via manual mode. Intel® AMT wireless should be configured and operational (refer Section 6.3.3 for details).																						
Procedure:	<ol style="list-style-type: none"> 1. Wait 2 minutes before starting the test after the Host OS loads to allow entry into Host Control mode. 2. Open the Web UI on the SUT remotely from the management console via the wireless interface (refer Section 6.3.2 for details) and confirm the Intel® AMT wireless network IP address on the <i>System Status</i> page. 3. Disable wireless connectivity on the SUT by applying hardware RF-Kill. 4. Reload the Web UI from the SUT on the management console and confirm that Intel® AMT wireless network connectivity is not available. 5. Open the Host OS device manager on the SUT and disable the Host WLAN driver. 6. Wait 1 minute as the SUT moves into Intel® ME Control mode. 7. Reload the Web UI from the SUT on the management console and confirm that Intel® AMT wireless network connectivity is not available. 8. In the Host OS device manager on the SUT, re-enable the Host WLAN driver. 9. Enable wireless connectivity on the SUT by canceling hardware RF-Kill. 																						
Pass Criteria:	The test passes if Intel® AMT does not respond over the wireless network when the SUT is in either Host Control or Intel® ME Control mode with hardware RF-kill applied.																						
References:	For details on Intel® AMT Web UI access, refer the <i>Intel® AMT OEM Web User Interface Guide</i> .																						

6.3.13 Software and Hardware Radio Frequency Kill (RF-Kill)

ID:	CS_010																			
Title:	Software and Hardware Radio Frequency Kill (RF-Kill)																			
Requirement:	Mandatory - exempt for systems without Intel® AMT WLAN support, or both SW and HW RF-Kill																			
System:	<table><tr><th colspan="2">Form Factor</th><th>System Power Model</th><th colspan="2">Intel® AMT Network Interface</th></tr><tr><td><input checked="" type="checkbox"/> Desktop</td><td><input checked="" type="checkbox"/> Workstation</td><td><input checked="" type="checkbox"/> Standard</td><td><input type="checkbox"/> LAN</td><td><input type="checkbox"/> Either Used</td></tr><tr><td><input checked="" type="checkbox"/> Mobile</td><td></td><td><input checked="" type="checkbox"/> Modern Standby or InstantGo*</td><td><input checked="" type="checkbox"/> WLAN</td><td><input type="checkbox"/> Not Used</td></tr></table>					Form Factor		System Power Model	Intel® AMT Network Interface		<input checked="" type="checkbox"/> Desktop	<input checked="" type="checkbox"/> Workstation	<input checked="" type="checkbox"/> Standard	<input type="checkbox"/> LAN	<input type="checkbox"/> Either Used	<input checked="" type="checkbox"/> Mobile		<input checked="" type="checkbox"/> Modern Standby or InstantGo*	<input checked="" type="checkbox"/> WLAN	<input type="checkbox"/> Not Used
Form Factor		System Power Model	Intel® AMT Network Interface																	
<input checked="" type="checkbox"/> Desktop	<input checked="" type="checkbox"/> Workstation	<input checked="" type="checkbox"/> Standard	<input type="checkbox"/> LAN	<input type="checkbox"/> Either Used																
<input checked="" type="checkbox"/> Mobile		<input checked="" type="checkbox"/> Modern Standby or InstantGo*	<input checked="" type="checkbox"/> WLAN	<input type="checkbox"/> Not Used																
Method:	Automated by Intel® PETS with test operator interaction																			
Description:	Intel® AMT would not connect over wireless LAN in S0 when software and hardware RF-Kill are active, regardless of Host Control or Intel® ME Control mode SUT operation.																			
Objective:	Verify that the Intel® AMT does not connect over wireless LAN in S0 in either Host Control or Intel® ME Control mode when software and hardware RF-kill are active.																			
Setup:	The initial state of the SUT should be S0/MeOn with Host OS running. Intel® AMT should be provisioned via manual mode. Intel® AMT wireless should be configured and operational (refer Section 6.3.3 for details).																			
Procedure:	<ol style="list-style-type: none">1. Wait 2 minutes before starting the test after the Host OS loads to allow entry into Host Control mode.2. Open the Web UI on the SUT remotely from the management console via the wireless interface (refer Section 6.3.2 for details) and confirm the Intel® AMT wireless network IP address on the <i>System Status</i> page.3. Disable wireless connectivity on the SUT by applying both software and hardware RF-Kill.4. Open the Host OS device manager on the SUT and disable the Host WLAN driver.5. Wait 1 minute as the SUT moves into Intel® ME Control mode.6. Reload the Web UI from the SUT on the management console and confirm that Intel® AMT wireless network connectivity is not available.7. Cancel the hardware RF-Kill setting, leaving software RF-kill still applied.8. Reload the Web UI from the SUT on the management console and confirm that Intel® AMT wireless network connectivity remains unavailable.9. In the Host OS device manager on the SUT, re-enable the Host WLAN driver.10. Enable wireless connectivity on the SUT by canceling software RF-Kill.																			
Pass Criteria:	The test passes if Intel® AMT does not respond over the wireless network with both software and hardware RF-kill applied.																			
References:	For details on Intel® AMT Web UI access, refer the <i>Intel® AMT OEM Web User Interface Guide</i> .																			

6.4 Intel® ME Firmware Update and Partial Firmware Update

The section serves as a checklist for the environment setup and testing of Intel® ME firmware update and partial (partition) firmware update feature support.

6.4.1 Tools for Testing

A formatted USB Key, the Intel® FWUpdLcl and Intel® MEInfo tools from the Intel® ME firmware kit.



6.4.2 Intel® ME Firmware Update

ID:	CS_020																						
Title:	Intel® ME Firmware Update																						
Requirement:	Mandatory - exempt when upgrade/downgrade support is not yet available in firmware																						
System:	<table><tr><th colspan="2">Form Factor</th><th colspan="2">System Power Model</th><th colspan="2">Intel® AMT Network Interface</th></tr><tr><td><input checked="" type="checkbox"/> Desktop</td><td><input checked="" type="checkbox"/> Workstation</td><td><input checked="" type="checkbox"/> Standard</td><td></td><td><input type="checkbox"/> LAN</td><td><input type="checkbox"/> Either Used</td></tr><tr><td><input checked="" type="checkbox"/> Mobile</td><td></td><td><input checked="" type="checkbox"/> Modern Standby or InstantGo*</td><td></td><td><input type="checkbox"/> WLAN</td><td><input checked="" type="checkbox"/> Not Used</td></tr></table>					Form Factor		System Power Model		Intel® AMT Network Interface		<input checked="" type="checkbox"/> Desktop	<input checked="" type="checkbox"/> Workstation	<input checked="" type="checkbox"/> Standard		<input type="checkbox"/> LAN	<input type="checkbox"/> Either Used	<input checked="" type="checkbox"/> Mobile		<input checked="" type="checkbox"/> Modern Standby or InstantGo*		<input type="checkbox"/> WLAN	<input checked="" type="checkbox"/> Not Used
Form Factor		System Power Model		Intel® AMT Network Interface																			
<input checked="" type="checkbox"/> Desktop	<input checked="" type="checkbox"/> Workstation	<input checked="" type="checkbox"/> Standard		<input type="checkbox"/> LAN	<input type="checkbox"/> Either Used																		
<input checked="" type="checkbox"/> Mobile		<input checked="" type="checkbox"/> Modern Standby or InstantGo*		<input type="checkbox"/> WLAN	<input checked="" type="checkbox"/> Not Used																		
Method:	Automated by Intel® PETS with test operator interaction																						
Description:	Firmware Update settings, as set by the Intel® FIT tool, allow update to the firmware.																						
Objective:	Verify that the Intel® ME firmware can be updated.																						
Setup:	The initial state of the SUT should be S0/MeOn with Host OS running.																						
Procedure:	<div>1. Enter a formatted USB Key into the management console.</div> <div>2. Browse to an update firmware image on the management console. This may be the latest firmware released by Intel, or an earlier version of the firmware than the firmware currently loaded on the SUT.</div> <div>3. Place the selected update firmware image on the USB Key.</div> <div>4. Move the USB Key to the SUT.</div> <div>5. Run the Intel® FWUpdLcl tool on the SUT with the -save option, to save the current firmware image to the USB Key.</div> <div>6. Extract the current version of the Intel® ME firmware, using the Intel® MEInfo tool.</div> <div>7. Run the Intel® FWUpdLcl tool on the SUT to update the firmware to the image on the USB Key.</div> <div>8. Restart the SUT.</div> <div>9. Verify the SUT has booted to the Host OS.</div> <div>10. Extract the new version of the Intel® ME firmware using Intel® MEInfo and ensure that it has changed from the original firmware version.</div> <div>11. Verify that the new firmware version is correct.</div>																						
Procedure: (continued)	<div>12. Run the Intel® FWUpdLcl tool on the SUT to restore the firmware to the original image extracted earlier from the SUT.</div> <div>13. Restart the SUT.</div> <div>14. Verify the SUT has booted to the Host OS.</div> <div>15. Extract the new version of the Intel® ME firmware using Intel® MEInfo, and ensure that it has been restored to the original firmware version.</div>																						
Pass Criteria:	<div>The test passes if the firmware update is successful, and the original firmware can be restored for each of the following conditions:</div> <div><div><div>• Update to newer version of firmware than what is installed on the SUT.</div><div>• Downgrade to an older version of firmware than what is installed on the SUT. Noted, it is not allowed to downgrade to an older version of firmware with lower VCN.</div></div><div>Depending on the Intel® ME development milestone at which this test is being executed, it may not be possible to fully execute this test with available firmware due to upgrade / downgrade firmware compatibility limitations. In this case, the results for this test become 'Not Available' or 'NA' until such time at which suitable firmware images become available to allow full execution of this test.</div></div>																						
References:	For details on Intel® ME firmware tools, refer the Intel® ME System Tools User Guide.																						

6.4.3 Intel® ME Firmware Partition Update for Secure Output Locale

ID:	CS_021
Title:	Intel® ME Firmware Partition Update for Secure Output Locale



ID:	CS_021				
Requirement:	Mandatory				
System:	Form Factor		System Power Model	Intel® AMT Network Interface	
	<input checked="" type="checkbox"/> Desktop <input checked="" type="checkbox"/> Mobile	<input checked="" type="checkbox"/> Workstation	<input checked="" type="checkbox"/> Standard <input checked="" type="checkbox"/> Modern Standby or InstantGo*	<input type="checkbox"/> LAN <input type="checkbox"/> WLAN	<input type="checkbox"/> Either Used <input checked="" type="checkbox"/> Not Used
Method:	Automated by Intel® PETS with test operator interaction				
Description:	This is a test of the Secure Output sprite locale update performed by Local Manageability Service (LMS) on a Microsoft Windows* platform.				
Objective:	Verify that the Secure Output localization partition in Intel® ME firmware region is correctly updated with the locale resources matching those specified by the end user in Intel® MSS.				
Setup:	The initial state of the SUT should be S0/MeOn with Host OS running.				
Procedure:	<ol style="list-style-type: none">1. Open the Intel® MSS Application;<ol style="list-style-type: none">a. select the <i>Advanced</i> tab, andb. change the selected Secure Output message language.2. Trigger a Secure Output event (i.e., User Consent confirmation request via KVM, SOL, or Storage Redirection) and verify that the message appears in the selected language. Note: Intel® PETS in combination with one of the Intel® AMT Redirection tests with User Consent enabled can be used to facilitate this test step.3. Use the Intel® MSS to return the Secure Output message language to the setting selected before the test was run.				
Pass Criteria:	The test passes if the Secure Output message is displayed in the language chosen in the Intel® MSS.				
References:	For details on Intel® MSS settings, refer the <i>Intel® Management and Security Status User's Guide</i> .				

6.4.4 Intel® ME Firmware Partition Update for WLAN µCode

ID:	CS_022				
Title:	Intel® ME Firmware Partition Update for WLAN µCode				
Requirement:	Mandatory - exempt where only one kind of WLAN NIC is supported on the platform				
System:	Form Factor		System Power Model	Intel® AMT Network Interface	
	<input checked="" type="checkbox"/> Desktop <input checked="" type="checkbox"/> Mobile	<input checked="" type="checkbox"/> Workstation	<input checked="" type="checkbox"/> Standard <input checked="" type="checkbox"/> Modern Standby or InstantGo*	<input type="checkbox"/> LAN <input checked="" type="checkbox"/> WLAN	<input type="checkbox"/> Either Used <input type="checkbox"/> Not Used
Method:	Automated by Intel® PETS with test operator interaction				
Description:	This is a test of the WLAN uCode (microcode) update performed by Local Manageability Service (LMS) on a Microsoft Windows* platform.				
Objective:	Verify that the WLAN uCode partition in Intel® ME firmware region is correctly updated with the uCode resources matching those required for the installed WLAN NIC.				
Setup:	The initial state of the SUT should be S0/MeOn with Host OS running.				
Procedure:	<ol style="list-style-type: none">1. Shutdown the SUT to G3, and replace the WLAN NIC with a different WLAN NIC which also supports Intel® vPro™ Technology.2. Boot the SUT with the new WLAN card.3. Open the Intel® MSS and verify that an event was created indicating a partition update occurred.4. Ensure that basic Intel® AMT wireless connectivity is functional. Note: The Intel® AMT wireless network tests relying on Web UI access at the beginning of this chapter can be used to facilitate this test step.5. Shutdown the SUT to G3, and replace the WLAN NIC with the original WLAN NIC used at the start of this test.				



ID:	CS_022
Pass Criteria:	The test passes if the event indicating the WLAN uCode partition update occurred as seen with Intel® MSS, and Intel® AMT connectivity is confirmed using the alternate WLAN NIC.
References:	For details on WLAN uCode update, refer the <i>Intel® ME System Tools User Guide</i> .

6.5 USB Key Based Configuration

The section serves as a checklist for the environment setup and testing of Intel® ME firmware configuration via USB Key feature support.

6.5.1 Test Environment

The System Under Test (SUT) is to be configured with Intel® AMT set in manual provisioning mode with static IP address or DHCP. The management console may be a laptop or a desktop with a version of Windows* supported by Intel® PETS, and the SUT should have a version of Windows* supported by Intel® PETS as well. The test network is comprised of a hub/switch and network cables. The SUT should have only one HDD.

Tools for Testing:

- Intel® PETS: The latest version of the tool from the Intel® CSME Compliancy and Debug kit release. Refer the Intel® PETS User Guide for exact instructions on how to load and setup the Intel® PETS software.
- System Under Test (SUT): Should be connected to Intel® APS 3. In case an Intel® APS 3 is not available, select the Manual configuration in the Intel® PETS SUT profile configuration menu.
- Intel® PETS Local Agent: The local agent must be installed on the SUT.
- USB Keys formatted to FAT16. It is recommended to test also with a FAT32 USB Key but it is not mandatory.

The system under test is to be UN-configured at start of each test, unless otherwise stated.

6.5.2 USB Key File Version 2.1 with Consumable Record

ID:	CS_030				
Title:	USB Key File Version 2.1 with Consumable Record				
Requirement:	Mandatory				
System:	Form Factor		System Power Model	Intel® AMT Network Interface	
	<input checked="" type="checkbox"/> Desktop <input checked="" type="checkbox"/> Mobile	<input checked="" type="checkbox"/> Workstation	<input checked="" type="checkbox"/> Standard <input checked="" type="checkbox"/> Modern Standby or InstantGo*	<input type="checkbox"/> LAN <input type="checkbox"/> WLAN	<input checked="" type="checkbox"/> Either Used <input type="checkbox"/> Not Used
Method:	Automated by Intel® PETS with test operator interaction				
Description:	Validate that the BIOS can recognize USB Key file format version 2.1, and pass a record to the Intel® MEBX.				
Objective:	Verify that the BIOS is able to read the USB Key file format version 2.1, process it, and correctly mark it as read.				
Setup:	Insert a USB key formatted to FAT16 or FAT32 into the SUT.				



ID:	CS_030
Procedure:	<ol style="list-style-type: none">1. Bring the SUT to the base state of S0/MeOn. This is done to ensure that it can be safely shutdown from any prior test.2. For a provisioned SUT, set the active power package on the SUT to Power Package 1 (Intel® ME on in S0). This is done to ensure that the Intel® ME moves to the MeOff state after system shutdown.3. If the SUT is in an <i>In-Provisioning</i> state, return it to a <i>Pre-Provisioning</i> state.4. Shutdown the SUT, and confirm that Intel® ME is in the MeOff state.5. The following step(s) to perform Intel® ME un-configuration and verify the system BIOS is configured to enable USB Key provisioning are dependent on Intel® APS usage:<ul style="list-style-type: none">— If the Intel® APS is used, Intel® PETS check if the Intel® ME has been configured to perform un-configure operation on RTC clear:<ol style="list-style-type: none">i. In the case that Intel® ME is un-configured by RTC-clear, Intel® PETS ensures Intel® ME is not configured by clearing the CMOS, and then prompt the test operator to ensure the system BIOS is configured to enable USB Key provisioning, before booting the SUT to Host OS.ii. In the case that Intel® ME would not be un-configured by RTC-clear, the test operator is prompted to manually un-configure the Intel® ME by system-specific means, ensure that the system BIOS is configured to enable USB Key provisioning, and then boot the SUT to Host OS.— If the Intel® APS is not used, Intel® PETS prompts the test operator in one of the following two ways:<ol style="list-style-type: none">i. In the case that Intel® ME is un-configured by RTC-clear, the test operator is prompted to safely bring the system to G3 state, disconnect the CMOS battery, wait 15 seconds for all electricity to dissipate from the system, reattach the CMOS battery, reattach AC-power, ensure the system BIOS is configured to enable USB Key provisioning, and then boot the SUT to Host OS.ii. In the case that Intel® ME would not be un-configured by RTC-clear, the test operator is prompted to manually un-configure Intel® ME by system-specific means, ensure the system BIOS is configured to enable USB Key provisioning, and then boot the SUT to Host OS.
Procedure: (continued)	<ol style="list-style-type: none">6. The Intel® PETS will prompt the test operator to insert a formatted USB key into the SUT.7. The Intel® PETS will place a file called SetUp.bin on the USB Key, containing a single consumable record (USB file version 2.1) including the following configuration information:<ol style="list-style-type: none">a. Intel® MEBX password (both old and new) The password which was entered in the SUT configuration for the Intel® ME password is used as the new password.b. FQDN "provisionServer.compliance.com" (to update ConfigServerFQDN)c. CA (Certificate Authority) hash8. Request the test operator to acknowledge the provisioning prompt on the SUT during the next boot. The system should continue booting to Host OS.9. Restart the SUT to the base state of S0/MeOn. The test operator should acknowledge the provisioning prompt during the boot process and the system should continue booting to Host OS.
Procedure: (continued)	<ol style="list-style-type: none">10. Verify the SUT has booted to Host OS.11. On the SUT, confirm the FQDN and CA hash were passed correctly to Intel® ME firmware.12. Restart the SUT to the base state of S0/MeOn.13. Verify the SUT has booted to Host OS.14. Request the test operator to confirm that SUT has booted to Host OS with no provisioning prompts during the boot process.15. Read the Setup.bin from USB Key and verify that the file was updated correctly to erase the used configuration record.
Pass Criteria:	The test passes if the SUT is configured with USB Key file format version 2.1. The configuration record is erased from the USB Key, and SUT boots normally afterwards.
References:	For details on the USB Key processing, refer the <i>Intel® ME BIOS Writers Guide</i> . Additional details about USB Key contents are available in the <i>Intel® Management Engine USB Key Local Provisioning Architecture Specification EDS</i> .

6.5.3 USB Key File Version 2.1 with Non-Consumable Record

ID:	CS_031
Title:	USB Key File Version 2.1 with Non-Consumable Record
Requirement:	Mandatory



ID:	CS_031				
System:	Form Factor		System Power Model	Intel® AMT Network Interface	
	<input checked="" type="checkbox"/> Desktop <input checked="" type="checkbox"/> Mobile	<input checked="" type="checkbox"/> Workstation	<input checked="" type="checkbox"/> Standard <input checked="" type="checkbox"/> Modern Standby or InstantGo*	<input type="checkbox"/> LAN <input type="checkbox"/> WLAN	<input checked="" type="checkbox"/> Either Used <input type="checkbox"/> Not Used
Method:	Automated by Intel® PETS with test operator interaction				
Description:	Validate that the BIOS can recognize USB Key file format version 2.1, and pass a record to the Intel® MEBX.				
Objective:	Verify that the BIOS is able to read the USB Key file format version 2.1, process it, and correctly mark it as read if it is non-consumable.				
Setup:	Insert a USB key formatted to FAT16 or FAT32 into the SUT.				
Procedure:	<ol style="list-style-type: none">1. Bring the SUT to the base state of S0/MeOn. This is done to ensure that it can be safely shutdown from any prior test.2. For a provisioned SUT, set the active power package on the SUT to Power Package 1 (Intel® ME on in S0). This is done to ensure that the Intel® ME moves to the MeOff state after system shutdown.3. If the SUT is in an <i>In-Provisioning</i> state, return it to a <i>Pre-Provisioning</i> state.4. Shutdown the SUT, and confirm that Intel® ME is in the MeOff state.5. The following step(s) to perform Intel® ME un-configuration and verify the system BIOS is configured to enable USB Key provisioning are dependent on Intel® APS usage:<ul style="list-style-type: none">— If the Intel® APS is used, Intel® PETS check if the Intel® ME has been configured to perform un-configure operation on RTC clear:<ol style="list-style-type: none">i. In the case that Intel® ME is un-configured by RTC-clear, Intel® PETS ensures Intel® ME is not configured by clearing the CMOS, and then prompt the test operator to ensure the system BIOS is configured to enable USB Key provisioning, before booting the SUT to Host OS.ii. In the case that Intel® ME would not be un-configured by RTC-clear, the test operator is prompted to manually un-configure the Intel® ME by system-specific means, ensure that the system BIOS is configured to enable USB Key provisioning, and then boot the SUT to Host OS.— If the Intel® APS is not used, Intel® PETS prompts the test operator in one of the following two ways:<ol style="list-style-type: none">i. In the case that Intel® ME is un-configured by RTC-clear, the test operator is prompted to safely bring the system to G3 state, disconnect the CMOS battery, wait 15 seconds for all electricity to dissipate from the system, reattach the CMOS battery, reattach AC-power, ensure the system BIOS is configured to enable USB Key provisioning, and then boot the SUT to Host OS.ii. In the case that Intel® ME would not be un-configured by RTC-clear, the test operator is prompted to manually un-configure Intel® ME by system-specific means, ensure the system BIOS is configured to enable USB Key provisioning, and then boot the SUT to Host OS.				
Procedure: (continued)	<ol style="list-style-type: none">6. Request the test operator to to:<ol style="list-style-type: none">a. reboot the SUT and enter the Intel® MEBX, thenb. from the Intel® MEBX menu, change the default 'admin' password to 'Admin!98' (or if using Intel® PETS, the same Intel® ME password which was provided in the Intel® PETS SUT configuration), and thenc. exit the Intel® MEBX menu and allow the system to boot to Host OS.7. The Intel® PETS will prompt the test operator to insert a formatted USB key into the SUT.8. Intel® PETS will place a file called SetUp.bin on the USB Key, containing a single non-consumable record (USB file version 2.1) including the following configuration information:<ol style="list-style-type: none">a. Intel® MEBX password: "Admin!98" (same password for both old and new) The same password which was entered in the SUT configuration for the Intel® ME password is used for both the old and new passwords.b. FQDN "provisionServer.compliance.com" (to update ConfigServerFQDN)c. CA (Certificate Authority) hash				

ID:	CS_031
Procedure: (continued)	9. Request the test operator to acknowledge the provisioning prompt on the SUT during the next boot. The system should continue booting to Host OS. 10. Restart the SUT to the base state of S0/MeOn. The test operator should acknowledge the provisioning prompt during the boot process and the system should continue booting to Host OS. 11. Verify the SUT has booted to Host OS. 12. On the SUT, confirm the FQDN and CA hash were passed correctly to Intel® ME firmware. 13. Request the test operator to acknowledge the provisioning prompt on the SUT during the next boot. The system should continue booting to Host OS. 14. Restart the SUT to the base state of S0/MeOn. The test operator should acknowledge the provisioning prompt during the boot process and the system should continue booting to Host OS. 15. Verify the SUT has booted to Host OS. 16. Request the test operator to confirm that a provisioning prompt was presented on the SUT.
Procedure: (continued)	17. Read the Setup.bin from USB Key and verify that the file was updated correctly to allow re-use of the configuration record, and the file was not changed by comparing the file content and header before and after the configuration.
Pass Criteria:	The test passes if the SUT is configured with USB Key file format version 2.1, and correctly handles non-consumable records.
References:	For details on the USB Key processing, refer the <i>Intel® ME BIOS Writers Guide</i> . Additional details about USB Key contents are available in the <i>Intel® Management Engine USB Key Local Provisioning Architecture Specification EDS</i> .

6.5.4 USB Key File Version 3 with Consumable Record

ID:	CS_032				
Title:	USB Key File Version 3 with Consumable Record				
Requirement:	Mandatory				
System:	Form Factor		System Power Model		Intel® AMT Network Interface
	<input checked="" type="checkbox"/> Desktop <input checked="" type="checkbox"/> Mobile	<input checked="" type="checkbox"/> Workstation	<input checked="" type="checkbox"/> Standard <input checked="" type="checkbox"/> Modern Standby or InstantGo*		<input type="checkbox"/> LAN <input type="checkbox"/> WLAN <input checked="" type="checkbox"/> Either Used <input type="checkbox"/> Not Used
Method:	Automated by Intel® PETS with test operator interaction				
Description:	<p>Validate that the BIOS can recognize USB file format version 3, and pass a record to the Intel® MEBX.</p> <p>The term “Version 3” does not refer USB 3.0. It refers to the 3rd revision USB configuration file format introduced in with Intel® ME 6 platforms.</p>				
Objective:	Verify that the BIOS is able to read the USB Key file format version 3, process it, and correctly mark it as read.				
Setup:	Insert a USB key formatted to FAT16 or FAT32 into the SUT.				



ID:	CS_032
Procedure:	<ol style="list-style-type: none"> 1. Bring the SUT to the base state of S0/MeOn. This is done to ensure that it can be safely shutdown from any prior test. 2. For a provisioned SUT, set the active power package on the SUT to Power Package 1 (Intel® ME on in S0). This is done to ensure that the Intel® ME moves to the MeOff state after system shutdown. 3. If the SUT is in an <i>In-Provisioning</i> state, return it to a <i>Pre-Provisioning</i> state. 4. Shutdown the SUT, and confirm that Intel® ME is in the MeOff state. 5. The following step(s) to perform Intel® ME un-configuration and verify the system BIOS is configured to enable USB Key provisioning are dependent on Intel® APS usage: <ol style="list-style-type: none"> a. If the Intel® APS is used, Intel® PETS check if the Intel® ME has been configured to perform un-configure operation on RTC clear: <ol style="list-style-type: none"> i. In the case that Intel® ME is un-configured by RTC-clear, Intel® PETS ensures Intel® ME is not configured by clearing the CMOS, and then prompt the test operator to ensure the system BIOS is configured to enable USB Key provisioning, before booting the SUT to Host OS. ii. In the case that Intel® ME would not be un-configured by RTC-clear, the test operator is prompted to manually un-configure the Intel® ME by system-specific means, ensure that the system BIOS is configured to enable USB Key provisioning, and then boot the SUT to Host OS. b. If the Intel® APS is not used, Intel® PETS prompts the test operator in one of the following two ways: <ol style="list-style-type: none"> i. In the case that Intel® ME is un-configured by RTC-clear, the test operator is prompted to safely bring the system to G3 state, disconnect the CMOS battery, wait 15 seconds for all electricity to dissipate from the system, reattach the CMOS battery, reattach AC-power, ensure the system BIOS is configured to enable USB Key provisioning, and then boot the SUT to Host OS. ii. In the case that Intel® ME would not be un-configured by RTC-clear, the test operator is prompted to manually un-configure Intel® ME by system-specific means, ensure the system BIOS is configured to enable USB Key provisioning, and then boot the SUT to Host OS.
Procedure: (continued)	<ol style="list-style-type: none"> 6. The Intel® PETS will prompt the test operator to insert a formatted USB key into the SUT. 7. The Intel® PETS will place a file called SetUp.bin on the USB Key, containing a single consumable record (USB file version 3) including the following configuration information: <ol style="list-style-type: none"> a. Intel® MEBX password (both old and new) The password which was entered in the SUT configuration for the Intel® ME password is used as the new password. b. FQDN "provisionServer.compliance.com" (to update ConfigServerFQDN) c. CA (Certificate Authority) hash 8. Request the test operator to acknowledge the provisioning prompt on the SUT during the next boot. The system should continue booting to Host OS. 9. Restart the SUT to the base state of S0/MeOn. The test operator should acknowledge the provisioning prompt during the boot process and the system should continue booting to Host OS.
Procedure: (continued)	<ol style="list-style-type: none"> 10. Verify the SUT has booted to Host OS. 11. On the SUT, confirm the FQDN and CA hash were passed correctly to Intel® ME firmware. 12. Restart the SUT to the base state of S0/MeOn. 13. Verify the SUT has booted to Host OS. 14. Request the test operator to confirm that SUT has booted to Host OS with no provisioning prompts during the boot process. 15. Read the Setup.bin from USB Key and verify that the file was updated correctly to erase the used configuration record.
Pass Criteria:	The test passes if the SUT is configured with USB Key file format version 3. The configuration record is erased from the USB Key, and SUT boots normally afterwards.
References:	For details on the USB Key processing, refer the <i>Intel® ME BIOS Writers Guide</i> . Additional details about USB Key contents are available in the <i>Intel® Management Engine USB Key Local Provisioning Architecture Specification EDS</i> .

6.5.5 USB Key File Version 4 with Consumable Record

ID:	CS_033
Title:	USB Key File Version 4 with Consumable Record
Requirement:	Mandatory



ID:	CS_033				
System:	Form Factor		System Power Model	Intel® AMT Network Interface	
	<input checked="" type="checkbox"/> Desktop <input checked="" type="checkbox"/> Mobile	<input checked="" type="checkbox"/> Workstation	<input checked="" type="checkbox"/> Standard <input checked="" type="checkbox"/> Modern Standby or InstantGo*	<input type="checkbox"/> LAN <input type="checkbox"/> WLAN	<input checked="" type="checkbox"/> Either Used <input type="checkbox"/> Not Used
Method:	Automated by Intel® PETS with test operator interaction				
Description:	Validate that the BIOS can recognize USB file format version 4, and pass a record to the Intel® MEBX.				
Objective:	Verify that the BIOS is able to read the USB Key file format version 4, process it, and correctly mark it as read.				
Setup:	Insert a USB key formatted to FAT16 or FAT32 into the SUT.				
Procedure:	<div>1. Bring the SUT to the base state of S0/MeOn. This is done to ensure that it can be safely shutdown from any prior test.</div> <div>2. For a provisioned SUT, set the active power package on the SUT to Power Package 1 (Intel® ME on in S0). This is done to ensure that the Intel® ME moves to the MeOff state after system shutdown.</div> <div>3. If the SUT is in an <i>In-Provisioning</i> state, return it to a <i>Pre-Provisioning</i> state.</div> <div>4. Shutdown the SUT, and confirm that Intel® ME is in the MeOff state.</div> <div>5. The following step(s) to perform Intel® ME un-configuration and verify the system BIOS is configured to enable USB Key provisioning are dependent on Intel® APS usage:<div><div>– If the Intel® APS is used, Intel® PETS check if the Intel® ME has been configured to perform un-configure operation on RTC clear:<div><div>i. In the case that Intel® ME is un-configured by RTC-clear, Intel® PETS ensures Intel® ME is not configured by clearing the CMOS, and then prompt the test operator to ensure the system BIOS is configured to enable USB Key provisioning, before booting the SUT to Host OS.</div><div>ii. In the case that Intel® ME would not be un-configured by RTC-clear, the test operator is prompted to manually un-configure the Intel® ME by system-specific means, ensure that the system BIOS is configured to enable USB Key provisioning, and then boot the SUT to Host OS.</div></div></div><div>– If the Intel® APS is not used, Intel® PETS prompts the test operator in one of the following two ways:<div><div>i. In the case that Intel® ME is un-configured by RTC-clear, the test operator is prompted to safely bring the system to G3 state, disconnect the CMOS battery, wait 15 seconds for all electricity to dissipate from the system, reattach the CMOS battery, reattach AC-power, ensure the system BIOS is configured to enable USB Key provisioning, and then boot the SUT to Host OS.</div><div>ii. In the case that Intel® ME would not be un-configured by RTC-clear, the test operator is prompted to manually un-configure Intel® ME by system-specific means, ensure the system BIOS is configured to enable USB Key provisioning, and then boot the SUT to Host OS.</div></div></div></div></div>				
Procedure: (continued)	<div>6. The Intel® PETS will prompt the test operator to insert a formatted USB key into the SUT.</div> <div>7. The Intel® PETS will place a file called Setup.bin on the USB Key, containing a single consumable record (USB file version 4) including the following configuration information:<div><div>a. Intel® MEBX password (both old and new) The password which was entered in the SUT configuration for the Intel® ME password is used as the new password.</div><div>b. FQDN "provisionServer.compliance.com" (to update ConfigServerFQDN)</div><div>c. CA (Certificate Authority) hash</div></div></div> <div>8. Request the test operator to acknowledge the provisioning prompt on the SUT during the next boot. The system should continue booting to Host OS.</div> <div>9. Restart the SUT to the base state of S0/MeOn. The test operator should acknowledge the provisioning prompt during the boot process and the system should continue booting to Host OS.</div>				
Procedure: (continued)	<div>10. Verify the SUT has booted to Host OS.</div> <div>11. On the SUT, confirm the FQDN and CA hash were passed correctly to Intel® ME firmware.</div> <div>12. Restart the SUT to the base state of S0/MeOn.</div> <div>13. Verify the SUT has booted to Host OS.</div> <div>14. Request the test operator to confirm that SUT has booted to Host OS with no provisioning prompts during the boot process.</div> <div>15. Read the Setup.bin from USB Key and verify that the file was updated correctly to erase the used configuration record.</div>				
Pass Criteria:	The test passes if the SUT is configured with USB Key file format version 4. The configuration record is erased from the USB Key, and SUT boots normally afterwards.				



ID:	CS_033
References:	For details on the USB Key processing, refer the <i>Intel® ME BIOS Writers Guide</i> . Additional details about USB Key contents are available in the <i>Intel® Management Engine USB Key Local Provisioning Architecture Specification EDS</i> .

6.5.6 USB Key File with Multiple Consumable Records

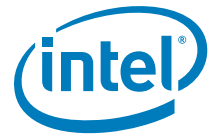
ID:	CS_034																			
Title:	USB Key with Multiple Consumable Records																			
Requirement:	Mandatory																			
System:	<table><tr><td colspan="2">Form Factor</td><td>System Power Model</td><td colspan="2">Intel® AMT Network Interface</td></tr><tr><td><input checked="" type="checkbox"/> Desktop</td><td><input checked="" type="checkbox"/> Workstation</td><td><input checked="" type="checkbox"/> Standard</td><td><input type="checkbox"/> LAN</td><td><input checked="" type="checkbox"/> Either Used</td></tr><tr><td><input checked="" type="checkbox"/> Mobile</td><td></td><td><input checked="" type="checkbox"/> Modern Standby or InstantGo*</td><td><input type="checkbox"/> WLAN</td><td><input type="checkbox"/> Not Used</td></tr></table>					Form Factor		System Power Model	Intel® AMT Network Interface		<input checked="" type="checkbox"/> Desktop	<input checked="" type="checkbox"/> Workstation	<input checked="" type="checkbox"/> Standard	<input type="checkbox"/> LAN	<input checked="" type="checkbox"/> Either Used	<input checked="" type="checkbox"/> Mobile		<input checked="" type="checkbox"/> Modern Standby or InstantGo*	<input type="checkbox"/> WLAN	<input type="checkbox"/> Not Used
Form Factor		System Power Model	Intel® AMT Network Interface																	
<input checked="" type="checkbox"/> Desktop	<input checked="" type="checkbox"/> Workstation	<input checked="" type="checkbox"/> Standard	<input type="checkbox"/> LAN	<input checked="" type="checkbox"/> Either Used																
<input checked="" type="checkbox"/> Mobile		<input checked="" type="checkbox"/> Modern Standby or InstantGo*	<input type="checkbox"/> WLAN	<input type="checkbox"/> Not Used																
Method:	Automated by Intel® PETS with test operator interaction																			
Description:	Verify that multiple machines can be provisioned using one USB Key. This tests the ability of the BIOS to mark records on the USB Key as used and to process USB file that contains consumed records.																			
Objective:	Verify that the BIOS to mark records on the USB Key as used, and also for the BIOS to recover gracefully when there are no unmarked records on the USB Key.																			
Setup:	Insert a USB key formatted to FAT16 or FAT32 into the SUT.																			
Procedure:	<ol style="list-style-type: none">1. Bring the SUT to the base state of S0/MeOn. This is done to ensure that it can be safely shutdown from any prior test.2. For a provisioned SUT, set the active power package on the SUT to Power Package 1 (Intel® ME on in S0). This is done to ensure that the Intel® ME moves to the MeOff state after system shutdown.3. If the SUT is in an <i>In-Provisioning</i> state, return it to a <i>Pre-Provisioning</i> state.4. Shutdown the SUT, and confirm that Intel® ME is in the MeOff state.5. The following step(s) to perform Intel® ME un-configuration and verify the system BIOS is configured to enable USB Key provisioning are dependent on Intel® APS usage:<ul style="list-style-type: none">— If the Intel® APS is used, Intel® PETS check if the Intel® ME has been configured to perform un-configure operation on RTC clear:<ol style="list-style-type: none">i. In the case that Intel® ME is un-configured by RTC-clear, Intel® PETS ensures Intel® ME is not configured by clearing the CMOS, and then prompt the test operator to ensure the system BIOS is configured to enable USB Key provisioning, before booting the SUT to Host OS.ii. In the case that Intel® ME would not be un-configured by RTC-clear, the test operator is prompted to manually un-configure the Intel® ME by system-specific means, ensure that the system BIOS is configured to enable USB Key provisioning, and then boot the SUT to Host OS.— If the Intel® APS is not used, Intel® PETS prompts the test operator in one of the following two ways:<ol style="list-style-type: none">i. In the case that Intel® ME is un-configured by RTC-clear, the test operator is prompted to safely bring the system to G3 state, disconnect the CMOS battery, wait 15 seconds for all electricity to dissipate from the system, reattach the CMOS battery, reattach AC-power, ensure the system BIOS is configured to enable USB Key provisioning, and then boot the SUT to Host OS.ii. In the case that Intel® ME would not be un-configured by RTC-clear, the test operator is prompted to manually un-configure Intel® ME by system-specific means, ensure the system BIOS is configured to enable USB Key provisioning, and then boot the SUT to Host OS.																			



ID:	CS_034
Procedure: (continued)	<p>6. Request the test operator to:</p> <ol style="list-style-type: none">reboot the SUT and enter the Intel® MEBX, thenfrom the Intel® MEBX menu, change the default 'admin' password to 'Admin!98' (or if using Intel® PETS, the same Intel® ME password which was provided in the Intel® PETS SUT configuration), and thenexit the Intel® MEBX menu and allow the system to boot to Host OS. <p>7. The Intel® PETS will prompt the test operator to insert a formatted USB key into the SUT.</p> <p>8. The Intel® PETS will place a file called Setup.bin on the USB Key, containing a two consumable records including the following configuration information:</p> <ol style="list-style-type: none">Intel® MEBX password: "Admin!98" (same password for both old and new) The same password which was entered in the SUT configuration for the Intel® ME password is used for both the old and new passwords.FQDN "provisionServer.compliance.com" (to update ConfigServerFQDN)CA (Certificate Authority) hash
Procedure: (continued)	<p>9. Request the test operator to acknowledge the provisioning prompt on the SUT during the next boot. The system should continue booting to Host OS.</p> <p>10. Restart the SUT to the base state of S0/MeOn. The test operator should acknowledge the provisioning prompt during the boot process and the system should continue booting to Host OS.</p> <p>11. Verify the SUT has booted to Host OS.</p> <p>12. On the SUT, confirm the FQDN and CA hash were passed correctly to Intel® ME firmware.</p> <p>13. Repeat steps 10 through 14.</p> <p>14. Restart the SUT for the third time to the base state of S0/MeOn.</p> <p>15. Verify the SUT has booted to Host OS.</p> <p>16. Request the test operator to confirm that SUT has booted to Host OS with no provisioning prompts during the boot process. There should no longer be any unmarked provisioning records in the USB Key. However, the BIOS should continue gracefully when all records in the USB Key are marked as used, and the boot should continue to the OS.</p>
Procedure: (continued)	<p>17. Read the Setup.bin from USB Key and verify that the file was updated correctly to erase the used configuration records.</p>
Pass Criteria:	The test passes if the first two (2) configuration attempts succeed, and the final iteration fails. The final iteration should continue to boot to the OS, without configuring the system.
References:	For details on the USB Key processing, refer the <i>Intel® ME BIOS Writers Guide</i> . Additional details about USB Key contents are available in the <i>Intel® Management Engine USB Key Local Provisioning Architecture Specification EDS</i> .

6.5.7 USB Key File Configuration Process Cancellation

ID:	CS_035				
Title:	USB Key File Configuration Process Cancellation				
Requirement:	Mandatory				
System:	Form Factor		System Power Model		Intel® AMT Network Interface
	<input checked="" type="checkbox"/> Desktop <input checked="" type="checkbox"/> Mobile	<input checked="" type="checkbox"/> Workstation	<input checked="" type="checkbox"/> Standard <input checked="" type="checkbox"/> Modern Standby or InstantGo*	<input type="checkbox"/> LAN <input type="checkbox"/> WLAN	<input checked="" type="checkbox"/> Either Used <input type="checkbox"/> Not Used
Method:	Automated by Intel® PETS with test operator interaction				
Description:	Validate that BIOS can continue booting the system if the end-user chooses not to continue with the provisioning process.				
Objective:	Verify that BIOS can detect provisioning process override and continue to boot.				
Setup:	Insert a USB key formatted to FAT16 or FAT32 into the SUT.				



ID:	CS_035
Procedure:	<ol style="list-style-type: none"> 1. Bring the SUT to the base state of S0/MeOn. This is done to ensure that it can be safely shutdown from any prior test. 2. For a provisioned SUT, set the active power package on the SUT to Power Package 1 (Intel® ME on in S0). This is done to ensure that the Intel® ME moves to the MeOff state after system shutdown. 3. If the SUT is in an <i>In-Provisioning</i> state, return it to a <i>Pre-Provisioning</i> state. 4. Shutdown the SUT, and confirm that Intel® ME is in the MeOff state. 5. The following step(s) to perform Intel® ME un-configuration and verify the system BIOS is configured to enable USB Key provisioning are dependent on Intel® APS usage: <ul style="list-style-type: none"> — If the Intel® APS is used, Intel® PETS check if the Intel® ME has been configured to perform un-configure operation on RTC clear: <ol style="list-style-type: none"> i. In the case that Intel® ME is un-configured by RTC-clear, Intel® PETS ensures Intel® ME is not configured by clearing the CMOS, and then prompt the test operator to ensure the system BIOS is configured to enable USB Key provisioning, before booting the SUT to Host OS. ii. In the case that Intel® ME would not be un-configured by RTC-clear, the test operator is prompted to manually un-configure the Intel® ME by system-specific means, ensure that the system BIOS is configured to enable USB Key provisioning, and then boot the SUT to Host OS. — If the Intel® APS is not used, Intel® PETS prompts the test operator in one of the following two ways: <ol style="list-style-type: none"> i. In the case that Intel® ME is un-configured by RTC-clear, the test operator is prompted to safely bring the system to G3 state, disconnect the CMOS battery, wait 15 seconds for all electricity to dissipate from the system, reattach the CMOS battery, reattach AC-power, ensure the system BIOS is configured to enable USB Key provisioning, and then boot the SUT to Host OS. ii. In the case that Intel® ME would not be un-configured by RTC-clear, the test operator is prompted to manually un-configure Intel® ME by system-specific means, ensure the system BIOS is configured to enable USB Key provisioning, and then boot the SUT to Host OS.
Procedure: (continued)	<ol style="list-style-type: none"> 6. The Intel® PETS will prompt the test operator to insert a formatted USB key into the SUT. 7. The Intel® PETS will place a file called SetUp.bin on the USB Key, containing a single consumable record (USB file version 4) including the following configuration information: <ol style="list-style-type: none"> a. Intel® MEBX password (both old and new) The password which was entered in the SUT configuration for the Intel® ME password is used as the new password. b. FQDN "provisionServer.compliance.com" (to update ConfigServerFQDN) c. CA (Certificate Authority) hash 8. Request the test operator to not acknowledge the provisioning prompt (respond 'No' to the prompt) on the SUT during the next boot. The system should continue booting to Host OS. 9. Restart the SUT to the base state of S0/MeOn. The test operator should not acknowledge the provisioning prompt (respond 'No' to the prompt) during the boot process and the system should continue booting to Host OS.
Procedure: (continued)	<ol style="list-style-type: none"> 10. Verify the SUT has booted to Host OS. 11. On the SUT, confirm the SUT remains in <i>Pre-provisioning</i> mode. 12. Read the Setup.bin from USB Key and verify that the file records were not changed.
Pass Criteria:	The test passes if the SUT is not configured and instead boots normally; the file records on the USB Key are not changed.
References:	For details on the USB Key processing, refer the <i>Intel® ME BIOS Writers Guide</i> . Additional details about USB Key contents are available in the <i>Intel® Management Engine USB Key Local Provisioning Architecture Specification EDS</i> .

6.5.8 USB Key Drive Compliancey

ID:	CS_036				
Title:	USB Key Drive Compliancey				
Requirement:	Mandatory - for FAT16 format, optional for FAT32 formatted USB Keys				
System:					
	Form Factor		System Power Model	Intel® AMT Network Interface	
	<input checked="" type="checkbox"/> Desktop <input checked="" type="checkbox"/> Mobile	<input checked="" type="checkbox"/> Workstation	<input checked="" type="checkbox"/> Standard <input checked="" type="checkbox"/> Modern Standby or InstantGo*	<input type="checkbox"/> LAN <input type="checkbox"/> WLAN	<input checked="" type="checkbox"/> Either Used <input type="checkbox"/> Not Used



ID:	CS_036
Method:	Automated by Intel® PETS with test operator interaction
Description:	Validate that the BIOS can recognize USB file format version 4, and pass a record to the Intel® MEBX on various sizes of USB Keys from various vendors formatting with FAT16. Optionally, USB Keys with FAT32 formatting may be validated as well.
Objective:	Verify that the BIOS is able to read the USB Key formatted FAT16 with file format version 4, process it, and correctly mark it as read. It is recommended to test also with FAT32 USB Key.
Setup:	Insert a USB key formatted to FAT16 or FAT32 into the SUT.
Procedure:	<ol style="list-style-type: none"> 1. Bring the SUT to the base state of S0/MeOn. This is done to ensure that it can be safely shutdown from any prior test. 2. For a provisioned SUT, set the active power package on the SUT to Power Package 1 (Intel® ME on in S0). This is done to ensure that the Intel® ME moves to the MeOff state after system shutdown. 3. If the SUT is in an <i>In-Provisioning</i> state, return it to a <i>Pre-Provisioning</i> state. 4. Shutdown the SUT, and confirm that Intel® ME is in the MeOff state. 5. The following step(s) to perform Intel® ME un-configuration and verify the system BIOS is configured to enable USB Key provisioning are dependent on Intel® APS usage: <ul style="list-style-type: none"> — If the Intel® APS is used, Intel® PETS check if the Intel® ME has been configured to perform un-configure operation on RTC clear: <ol style="list-style-type: none"> i. In the case that Intel® ME is un-configured by RTC-clear, Intel® PETS ensures Intel® ME is not configured by clearing the CMOS, and then prompt the test operator to ensure the system BIOS is configured to enable USB Key provisioning, before booting the SUT to Host OS. ii. In the case that Intel® ME would not be un-configured by RTC-clear, the test operator is prompted to manually un-configure the Intel® ME by system-specific means, ensure that the system BIOS is configured to enable USB Key provisioning, and then boot the SUT to Host OS. — If the Intel® APS is not used, Intel® PETS prompts the test operator in one of the following two ways: <ol style="list-style-type: none"> i. In the case that Intel® ME is un-configured by RTC-clear, the test operator is prompted to safely bring the system to G3 state, disconnect the CMOS battery, wait 15 seconds for all electricity to dissipate from the system, reattach the CMOS battery, reattach AC-power, ensure the system BIOS is configured to enable USB Key provisioning, and then boot the SUT to Host OS. ii. In the case that Intel® ME would not be un-configured by RTC-clear, the test operator is prompted to manually un-configure Intel® ME by system-specific means, ensure the system BIOS is configured to enable USB Key provisioning, and then boot the SUT to Host OS.
Procedure: (continued)	<ol style="list-style-type: none"> 6. The Intel® PETS will prompt the test operator to insert a formatted USB key into the SUT. 7. The Intel® PETS will place a file called Setup.bin on the USB Key, containing a single consumable record (USB file version 4) including the following configuration information: <ol style="list-style-type: none"> a. Intel® MEBX password (both old and new) The password which was entered in the SUT configuration for the Intel® ME password is used as the new password. b. FQDN "provisionServer.compliance.com" (to update ConfigServerFQDN) c. CA (Certificate Authority) hash 8. Request the test operator to acknowledge the provisioning prompt on the SUT during the next boot. The system should continue booting to Host OS. 9. Restart the SUT to the base state of S0/MeOn. The test operator should acknowledge the provisioning prompt during the boot process and the system should continue booting to Host OS.
Procedure: (continued)	<ol style="list-style-type: none"> 10. Verify the SUT has booted to Host OS. 11. On the SUT, confirm the FQDN and CA hash were passed correctly to Intel® ME firmware. 12. Restart the SUT to the base state of S0/MeOn. 13. Verify the SUT has booted to Host OS. 14. Request the test operator to confirm that SUT has booted to Host OS with no provisioning prompts during the boot process. 15. Read the Setup.bin from USB Key and verify that the file was updated correctly to erase the used configuration record. 16. Prompt the user to repeat this test with different USB Keys from different vendors and with different sizes.
Pass Criteria:	The test passes if the system is configured with each USB Key in FAT16 format, without any errors. If FAT32 format is tested, the system should be configured with the USB Key that was formatted with a FAT32 file system.
References:	For details on the USB Key processing, refer the <i>Intel® ME BIOS Writers Guide</i> . Additional details about USB Key contents are available in the <i>Intel® Management Engine USB Key Local Provisioning Architecture Specification EDS</i> .



6.5.9 USB Key File Configuration Disabled at Factory Default

ID:	CS_037																			
Title:	USB Key File Configuration Disabled at Factory Default																			
Requirement:	Mandatory																			
System:	<table><tr><th colspan="2">Form Factor</th><th>System Power Model</th><th colspan="2">Intel® AMT Network Interface</th></tr><tr><td><input checked="" type="checkbox"/> Desktop</td><td><input checked="" type="checkbox"/> Workstation</td><td><input checked="" type="checkbox"/> Standard</td><td><input type="checkbox"/> LAN</td><td><input checked="" type="checkbox"/> Either Used</td></tr><tr><td><input checked="" type="checkbox"/> Mobile</td><td></td><td><input checked="" type="checkbox"/> Modern Standby or InstantGo*</td><td><input type="checkbox"/> WLAN</td><td><input type="checkbox"/> Not Used</td></tr></table>					Form Factor		System Power Model	Intel® AMT Network Interface		<input checked="" type="checkbox"/> Desktop	<input checked="" type="checkbox"/> Workstation	<input checked="" type="checkbox"/> Standard	<input type="checkbox"/> LAN	<input checked="" type="checkbox"/> Either Used	<input checked="" type="checkbox"/> Mobile		<input checked="" type="checkbox"/> Modern Standby or InstantGo*	<input type="checkbox"/> WLAN	<input type="checkbox"/> Not Used
Form Factor		System Power Model	Intel® AMT Network Interface																	
<input checked="" type="checkbox"/> Desktop	<input checked="" type="checkbox"/> Workstation	<input checked="" type="checkbox"/> Standard	<input type="checkbox"/> LAN	<input checked="" type="checkbox"/> Either Used																
<input checked="" type="checkbox"/> Mobile		<input checked="" type="checkbox"/> Modern Standby or InstantGo*	<input type="checkbox"/> WLAN	<input type="checkbox"/> Not Used																
Method:	Automated by Intel® PETS with test operator interaction																			
Description:	Validate that BIOS prevents the USB Key provisioning flow with factory default settings.																			
Objective:	Verify that USB Key configuration is not possible when factory default system BIOS settings are applied to the SUT.																			
Setup:	Insert a USB key formatted to FAT16 or FAT32 into the SUT.																			
Procedure:	<ol style="list-style-type: none">1. Bring the SUT to the base state of S0/MeOn. This is done to ensure that it can be safely shutdown from any prior test.2. For a provisioned SUT, set the active power package on the SUT to Power Package 1 (Intel® ME on in S0). This is done to ensure that the Intel® ME moves to the MeOff state after system shutdown.3. If the SUT is in an <i>In-Provisioning</i> state, return it to a <i>Pre-Provisioning</i> state.4. Shutdown the SUT, and confirm that Intel® ME is in the MeOff state.5. The following step(s) to perform Intel® ME un-configuration and verify the system BIOS is configured with factory default settings are dependent on Intel® APS usage:<ul style="list-style-type: none">— If the Intel® APS is used, Intel® PETS check if the Intel® ME has been configured to perform un-configure operation on RTC clear:<ol style="list-style-type: none">i. In the case that Intel® ME is un-configured by RTC-clear, Intel® PETS ensures Intel® ME is not configured by clearing the CMOS, and then prompt the test operator to ensure the system BIOS is configured with factory default settings, before booting the SUT to Host OS.ii. In the case that Intel® ME would not be un-configured by RTC-clear, the test operator is prompted to manually un-configure the Intel® ME by system-specific means, ensure that the system BIOS is configured with factory default settings, and then boot the SUT to Host OS.— If the Intel® APS is not used, Intel® PETS prompts the test operator in one of the following two ways:<ol style="list-style-type: none">i. In the case that Intel® ME is un-configured by RTC-clear, the test operator is prompted to safely bring the system to G3 state, disconnect the CMOS battery, wait 15 seconds for all electricity to dissipate from the system, reattach the CMOS battery, reattach AC-power, ensure the system BIOS is configured with factory default settings, and then boot the SUT to Host OS.ii. In the case that Intel® ME would not be un-configured by RTC-clear, the test operator is prompted to manually un-configure Intel® ME by system-specific means, ensure the system BIOS is configured with factory default settings, and then boot the SUT to Host OS.																			
Procedure: (continued)	<ol style="list-style-type: none">6. The Intel® PETS will prompt the test operator to insert a formatted USB key into the SUT.7. The Intel® PETS will place a file called Setup.bin on the USB Key, containing a single consumable record (USB file version 4) including the following configuration information:<ol style="list-style-type: none">a. Intel® MEBX password (both old and new) The password which was entered in the SUT configuration for the Intel® ME password is used as the new password.b. FQDN "provisionServer.compliance.com" (to update ConfigServerFQDN)c. CA (Certificate Authority) hash8. Request the test operator to verify that there is no provisioning prompt displayed on the SUT during the next boot. The system should continue booting to Host OS.9. Restart the SUT to the base state of S0/MeOn.																			
Procedure: (continued)	<ol style="list-style-type: none">10. Verify the SUT has booted to Host OS.11. Request the test operator to confirm that no provisioning prompt appeared on the SUT during the boot.12. On the SUT, confirm the SUT remains in <i>Pre-provisioning</i> mode.13. Read the Setup.bin from USB Key and verify that the file records were not changed.																			

ID:	CS_037
Pass Criteria:	The test passes if the SUT is not configured and instead boots normally; the file records on the USB Key are not changed.
References:	For details on the USB Key processing, refer the <i>Intel® ME BIOS Writers Guide</i> . Additional details about USB Key contents are available in the <i>Intel® Management Engine USB Key Local Provisioning Architecture Specification EDS</i> .

6.6 Remote and Host Based Configuration

The section serves as a checklist for the environment setup and testing of Intel® ME firmware Remote Configuration (RCFG) and Host Based Configuration feature support.

6.6.1 Test Environment

The System Under Test (SUT) is to be configured with Intel® AMT set in manual provisioning mode with static IP address or DHCP. The management console may be a laptop or a desktop with a version of Windows* supported by Intel® PETS, and the SUT should have a version of Windows* supported by Intel® PETS as well. The test network is comprised of a hub/switch and network cables. The SUT should have only one HDD.

Tools for Testing:

- Intel® PETS: The latest version of the tool from the Intel® CSME Compliancy and Debug kit release. Refer the Intel® PETS User Guide for exact instructions on how to load and setup the Intel® PETS software.
- System Under Test (SUT): Should be connected to Intel® APS 3. In case an Intel® APS 3 is not available, select the Manual configuration in the Intel® PETS SUT profile configuration menu.
- Intel® PETS Local Agent: The local agent must be installed on the SUT.

6.6.2 Remote Configuration Support

ID:	CS_040				
Title:	Remote Configuration Support				
Requirement:	Mandatory - exempt for systems that do not support Remote Configuration (PKI-CH)				
System:	Form Factor		System Power Model	Intel® AMT Network Interface	
	<input checked="" type="checkbox"/> Desktop <input checked="" type="checkbox"/> Mobile	<input checked="" type="checkbox"/> Workstation	<input checked="" type="checkbox"/> Standard <input checked="" type="checkbox"/> Modern Standby or InstantGo*	<input type="checkbox"/> LAN <input type="checkbox"/> WLAN	<input checked="" type="checkbox"/> Either Used <input type="checkbox"/> Not Used
Method:	Automated by Intel® PETS				
Description:	Verify that the necessary settings to allow the Intel® ME system to be remotely configured are present on the SUT.				
Objective:	Verify that the Intel® AMT platform can be provisioned using certificates under DHCP and automatic configuration mode. Remote Configuration (also called 'Zero Touch Configuration') is a feature that can help IT customers deploy and activate Intel® AMT.				
Setup:	The initial state of the SUT should be S0/MeOn with Host OS running. Intel® AMT should be provisioned via manual mode.				
Procedure:	1. On the SUT, extract the root certificate hashes. 2. Confirm that Remote Configuration (RCFG) is enabled.				
Pass Criteria:	The test passes if Remote Configuration (RCFG) is enabled.				



ID:	CS_040
References:	For details on the Remote Configuration control, refer the <i>Intel® Management Engine Bring Up Guide</i> .

6.6.3 Hosted Based Configuration Support

ID:	CS_041				
Title:	Host Based Configuration Support				
Requirement:	Mandatory				
System:	Form Factor		System Power Model	Intel® AMT Network Interface	
	<input checked="" type="checkbox"/> Desktop <input checked="" type="checkbox"/> Mobile	<input checked="" type="checkbox"/> Workstation	<input checked="" type="checkbox"/> Standard <input checked="" type="checkbox"/> Modern Standby or InstantGo*	<input type="checkbox"/> LAN <input type="checkbox"/> WLAN	<input checked="" type="checkbox"/> Either Used <input type="checkbox"/> Not Used
Method:	Automated by Intel® PETS				
Description:	Verify an Intel® AMT compliant system can be provisioned using Host Based Configuration. NOTE: At the end of the test, Intel® PETS fully unprovision the SUT. User have to manually reprovision the SUT if you would like to run other tests that require a provisioned system.				
Objective:	Verify that Intel® AMT can be provisioned using Host Based Configuration into Client Control Mode (CCM).				
Setup:	The initial state of the SUT should be S0/MeOn with Host OS running. Intel® AMT should be fully unprovisioned. Intel® Management Engine BIOS Extension (Intel® MEBX) full unprovision menu, the CMOS clear mechanism, or the BIOS unconfigure without password mechanisms may be used to fully unprovision the SUT. Refer the <i>Intel® Management Engine BIOS Extension User's Guide</i> or <i>Intel® ME BIOS Writers Guide</i> documents for details.				
Procedure:	<ol style="list-style-type: none"> 1. If the SUT is in an <i>In-Provisioning</i> state, return it to a <i>Pre-Provisioning</i> state. 2. If the SUT is provisioned, fully unprovision it. 3. Verify that the LMS service is running. 4. Get the \$\$OSAdmin credentials on the SUT via Intel® AMT. 5. Use the credentials to get the Intel® AMT general settings digest realm. 6. Compute a network administrator password based on the MD5 hash of the digest realm. 7. Use the network administrator password to provision the SUT via Intel® AMT Host Based Configuration to Client Control Mode. 8. Verify that the provisioning state of the SUT is <i>Post-Provisioning</i>. 9. Fully unprovision the SUT via Intel® AMT. 				
Pass Criteria:	Test passes if Intel® AMT system is provisioned by Host Based Configuration into Client Control Mode.				

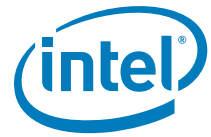
6.6.4 Embedded Host Based Configuration Support

ID:	CS_042				
Title:	Embedded Host Based Configuration Support				
Requirement:	Optional - for use with embedded systems only				
System:	Form Factor		System Power Model	Intel® AMT Network Interface	
	<input checked="" type="checkbox"/> Desktop <input checked="" type="checkbox"/> Mobile	<input checked="" type="checkbox"/> Workstation	<input checked="" type="checkbox"/> Standard <input checked="" type="checkbox"/> Modern Standby or InstantGo*	<input type="checkbox"/> LAN <input type="checkbox"/> WLAN	<input checked="" type="checkbox"/> Either Used <input type="checkbox"/> Not Used
Method:	Automated by Intel® PETS				



ID:	CS_042
Description:	<p>Verify an Intel® AMT compliant system can be provisioned using Embedded Host Based Configuration (EHBC), where supported, to enter Administrator Control Mode (ACM).</p> <p>Warning: Platforms should not be configured to support EHBC unless all security aspects has been understood and taken into account.</p> <p>NOTE: At the end of the test, Intel® PETS fully unprovision the SUT. User have to manually reprovision the SUT if user would like to run other tests that require a provisioned system.</p>
Objective:	Verify that Intel® AMT can be provisioned using Embedded Host Based Configuration into Administrator Control Mode (ACM).
Setup:	The initial state of the SUT should be S0/MeOn with Host OS running. Intel® AMT should be fully unprovisioned. Intel® Management Engine BIOS Extension (Intel® MEBX) full unprovision menu, the CMOS clear mechanism, or the BIOS unconfigure without password mechanisms may be used to fully unprovision the SUT. Refer the <i>Intel® Management Engine BIOS Extension User's Guide</i> or <i>Intel® ME BIOS Writers Guide</i> documents for details.
Procedure:	<ol style="list-style-type: none">1. If the SUT is in an <i>In-Provisioning</i> state, return it to a <i>Pre-Provisioning</i> state.2. If the SUT is provisioned, fully unprovision it.3. Verify that the LMS service is running.4. Get the \$\$OSAdmin credentials on the SUT via Intel® AMT.5. Use the credentials to get the Intel® AMT general settings digest realm.6. Compute a network administrator password based on the MD5 hash of the digest realm.7. Use the network administrator password to provision the SUT via Intel® AMT Embedded Host Based Configuration to Administrator Control Mode.8. Verify that the provisioning state of the SUT is <i>Post-Provisioning</i>.9. Fully unprovision the SUT via Intel® AMT.
Pass Criteria:	Test passes if Intel® AMT system is provisioned by Embedded Host Based Configuration into Administrator Control Mode.

§ §



7 SPI Flash Interface

7.1 Overview

The test cases in this chapter are created to verify the correct configuration of the Intel® PCH SPI Host Controller. Test cases in this section verify implementation of SPI Dual and Quad I/O Fast Read, SPI Flash Descriptor mode, and ensure compliance with Intel® CSME and Intel® GbE requirements.

7.2 Tools for Testing

Intel® Platform Enablement Test Suite (PETS)—Use latest version of this kit. Refer the Intel® PETS user guide available in the Intel® CSME Compliancy kit for details instructions on how to load and setup the Intel® PETS software.

Intel® Flash Image Tool (Fit.exe)

Intel® Flash Programming Tool—Available in DOS (Fpt.exe), EFI (Fpt.efi), Windows* 32-bit (Ftpw.exe), and Windows* 64-bit operating systems (Fptw-64).

7.3 Test Environment

The System Under Test (SUT) is to be configured in manual configuration mode a with wired LAN or wireless LAN dynamic IP address. The DHCP server connecting the SUT and Management Console (MC) must be configured to ensure that the wired LAN and wireless LAN addresses reside on separate subnets. The MC could be a laptop or desktop system running a version of Windows* supported by PETS. The network configuration consists of a hub or switch, network cables, and a wireless Access Point (AP).



7.4 Test Coverage Summary

Test ID	Test Case Title	PETS/Manual	Form Factor	Network Factor
SPI_001	Descriptor Mode Test	PETS	DT/MB	LAN+WLAN; WLAN only
SPI_002	Serial Flash Discoverable Parameter Test	PETS	DT/MB	LAN+WLAN; WLAN only
SPI_003	4 Kbytes Erasable Blocks Test	PETS	DT/MB	LAN+WLAN; WLAN only
SPI_004	SPI Flash Size Test	PETS	DT/MB	LAN+WLAN; WLAN only
SPI_005	SPI Flash VSCC Test	PETS	DT/MB	LAN+WLAN; WLAN only
SPI_006	Flash Descriptor Security Override Test	PETS	DT/MB	LAN+WLAN; WLAN only
SPI_007	Single Input, Dual or Quad Output Fast Read Test	PETS	DT/MB	LAN+WLAN; WLAN only
SPI_008	Dual and Quad I/O Fast Read	PETS	DT/MB	LAN+WLAN; WLAN only

7.5 Descriptor Mode Test

Test ID	SPI_001
Test Case Title:	Descriptor Mode Test
Mandatory/Optional:	Mandatory
Description:	Descriptor Mode is required for all SKUs of the PCH to ensure proper operation of features such as the Intel® ME, Intel Integrated LAN driver, and PCH softstraps.
Objective:	Verify the SPI flash controller in the PCH is operating in Descriptor Mode.
Procedure:	1. Boot to the target OS. 2. Verify the Flash Descriptor Valid Signature (FDBAR + 10h) is set to 0FF0A55Ah.
Test Pass/Fail Criteria:	Test passes if FDVS is 0FF0A55Ah.

7.6 Serial Flash Discoverable Parameter Test

Test ID	SPI_002
Test Case Title:	Serial Flash Discoverable Parameter (SFDP) Test
Mandatory/Optional:	Mandatory
Description:	Proper SFDP support in the SPI flash device may be used to enable advanced SPI features like the Quad I/O Fast Read.



Test ID	SPI_002
Objective:	Verify that the SPI flash controller in the PCH is able to detect a valid SFDP table in the SPI flash device.
Procedure:	<ol style="list-style-type: none"> 1. Boot to target OS. 2. Does flash device 0 in the SUT supports SFDP? <ul style="list-style-type: none"> • If Yes, <ul style="list-style-type: none"> — Verify that the Component Property Parameter Table Valid (CPPTV) bit 31 of the Vendor Specific Component Capabilities 0 register (VSCC0⁴) is set to 1b. • If No, <ul style="list-style-type: none"> — Inform the test operator that SFDP support in the SPI flash device may be used to enable advanced SPI features like the Quad I/O Fast Read³. 3. Read the number of SPI parts by means of the Number of Components (NC) bits [9:8] in the Flash Map 0 (FLMAP0) register at (FDBAR + 14h). <ul style="list-style-type: none"> • If the number of components is 01b (2 Components) continue to next step else end test. 4. Does flash device 1 in the SUT supports SFDP? <ul style="list-style-type: none"> • If Yes, <ul style="list-style-type: none"> — Verify that the Component Property Parameter Table Valid (CPPTV) bit 31 of the Vendor Specific Component Capabilities 1 register (VSCC1⁴) is set to 1b. • If No, <ul style="list-style-type: none"> — Inform the test operator that SFDP support in the SPI flash device may be used to enable advanced SPI features like that Quad I/O Fast Read³. <p>Notes:</p> <ol style="list-style-type: none"> 1. VSCC0 register is located at (VTBA⁴ + C4h). 2. VSCC1 register is located at (VTBA⁴ + C4h + (n*8)h), where n=1. 3. Test considered pass, this is just additional information to user. 4. Refer SPI Programming Guide for details of these registers.
Test Pass/Fail Criteria:	Test passes if all steps return expected values.

7.7 4 Kbytes Erasable Blocks Test

Test ID	SPI_003
Test Case Title:	4 Kbytes Erasable blocks Test
Mandatory/Optional:	Mandatory
Description:	The SPI Flash device must provide uniform 4 Kbytes erasable blocks/sectors throughout the entire part. This is required by Intel® CSME firmware.

Test ID	SPI_003
Objective:	Verify the SPI flash device supports uniform 4 Kbytes erasable blocks.
Procedure:	<p>Part 1: Verify registers.</p> <ol style="list-style-type: none"> 1. Boot to the target OS. 2. Verify the SUT is operating in Descriptor Mode by confirming that the Flash Descriptor Valid (FDV) bit 14 in the Hardware Sequencing Flash Status (HSFS) register (SPIBAR + 04h) has been set to '1'. 3. Verify all flash components support 4 Kbytes erasable blocks by confirming that the Block/Sector Erase Size (BERASE) bits [4:3] in the Hardware Sequencing Flash Status (HSFS) register (SPIBAR + 04) are set to 01b. <p>Part 2: Check against SPI flash device datasheet.</p> <ol style="list-style-type: none"> 1. Using the "MEInfo"¹ tool, read the SPI flash device ID from the SUT. 2. Verify the SPI flash device ID(s) read from the SUT are found in the vsccommn.bin² SPI part registry cached in Intel® PETS. <p>Notes:</p> <ol style="list-style-type: none"> 1. The "MEInfo" tool is part of the Intel® Management Engine Firmware release package, under System Tools folder. 2. The vsccommn.bin file is updated relative to the latest official version for each Intel® PETS release.
Test Pass/Fail Criteria:	Test passes if all steps return expected values.

7.8 SPI Flash Size Test

Test ID	SPI_004
Test Case Title:	SPI Flash Size Test
Mandatory/Optional:	Mandatory
Description:	Intel® PCH SKUs each have different requirements for SPI flash sizes. This test verifies that the SPI flash device has enough space to store the whole SPI image created by Intel® FIT tool.
Objective:	Verify the correct SPI flash size is used for a given PCH SKU contained in the SUT.
Procedure:	<ol style="list-style-type: none"> 1. Boot to target OS. 2. Read following information from SPI Flash Descriptor in the SUT: <ul style="list-style-type: none"> • The number of SPI parts by means of the Number of Components (NC) bits [9:8] in the Flash Map 0 (FLMAP0) register at (FDBAR + 14h). • The size of the first flash component by means of the Component 0 Density (CODEN) bits [3:0] in the Flash Components Record (FLCOMP) register at (FCBA + 0h). • If the number of components is 01b (2 Components), read the size of the second flash component by means of the Component 1 Density (C1DEN) bits [7:4] in the Flash Components Record (FLCOMP) register at (FCBA + 0h). 3. Compare the SUT flash size against the: <ul style="list-style-type: none"> • SPI flash device manufacturer datasheet¹. <p>Note: Intel® PETS maintain a list of SPI flash device sizes.</p>
Test Pass/Fail Criteria	<p>The test passes if the following conditions is true:</p> <p>The flash components' sizes in the SUT are less than or equal to the size stated in the SPI device manufacturer datasheet.</p>



7.9 SPI Flash Vendor Specific Capabilities (VSCC) Test

Test ID	SPI_005
Test Case Title:	SPI Flash Vendor Specific Component Capabilities (VSCC) Test.
Mandatory/Optional:	Mandatory
Description:	The VSCC registers are defined in two places. Host-based VSCCn registers (for example, VSCC0 and VSCC1) in memory mapped space and the Intel® CSME VSCC Table in the SPI Flash Descriptor. Intel® CSME only uses the VSCC table in the SPI Flash Descriptor, while the memory map VSCCn registers are used by BIOS and GbE software. The Intel® CSME VSCC table is created using the FIT tool by ODM/OEM, while the memory mapped VSCCn registers are programmed by BIOS. Incorrect VSCCn registers configuration may affect SPI flash functionality and also may lead to premature flash device wear out.
Objective:	To verify VSCCn registers in memory mapped space and VSCC table in SPI Flash Descriptor is configured correctly.
Procedure:	<ol style="list-style-type: none"> 1. Boot to the target OS. 2. Read the Vendor Specific Component Capabilities Registers (VSCCn), in the memory mapped space, where these register are located at (SPIBAR + C4h) and (SPIDBAR + C4h + (1 * 8)h) respectively. 3. Verify the VSCCn values with the SPI Flash device manufacturer datasheet. 4. Read the VSCC table from the SPI flash device on the target system. The base address of the table is located at offset (FDBAR₁ + EFCh). The Intel® CSME VSCC Table Base Address (VTBA) and the Intel® CSME VSCC Table Length (VTL) are located at (FDBAR + EFCh). 5. Every record in the table is 2 DWORDs long, the first 32 bits contain the SPI flash device's JEDEC ID, and the following 32 bits represent its VSCC value. 6. Iterate through the VSCC table searching for the matching JEDEC ID of the SPI devices in use on the SUT and verify the associated VSCC values matches both the SPI flash device manufacturer datasheet and the Intel® CSME VSCC value. <p>Note: FDBAR is located at address 0 of the SPI flash device chip select 0.</p>
Test Pass/Fail Criteria:	Test results pass if VSCC0 or VSCC0 and VSCC1, and the VCSS table in SPI Flash Descriptor align with the Intel® CSME VSCC and SPI flash device manufacturer datasheet settings.



7.10 Flash Descriptor Security Override Test

Test ID	SPI_006
Test Case Title:	Flash Descriptor Security Override Test
Mandatory/Optional:	Mandatory
Description:	This boots the platform in Intel® CSME Test Mode. This gives the ability to override Flash descriptor permissions debug/repair depot environments. This must NOT be default behavior.
Objective:	This test is to verify the platform has the ability to enable and disable Intel® CSME manufacturing mode, and to be able to reprogram the entire SPI flash.
Procedure:	<ol style="list-style-type: none">1. Boot platform without having HDA_SDO asserted high on the rising edge of PWROK. Verify that FDOPSS is set to '1'. FDOPSS is in MMIO space (SPIBAR + 0x4) bit 132. Boot platform with having HDA_SDO asserted high on the rising edge of PWROK. Verify that FDOPSS is set to '0'. FDOPSS is in MMIO space (SPIBAR + 0x4) bit 13. This assertion of HDA_SDO can be with a jumper or through another external mechanism. Care should be taken to ensure that assertion of this mechanism to assert HDA_SDO cannot be done remotely. <p>PETS helps automate testing of this capability. Perform the test by enabling "State after G3 to S5" at BIOS setting.</p> <p>Alternate Procedure</p> <ol style="list-style-type: none">1. Configure the platform with Intel® CSME Firmware.2. Use FPT /d to dump the image.3. Use Flash Programming Tool (FPT) to lock the image down using the - closemnf. Boot system from a G3 state.4. Use FPT /d to dump the image. This test should fail.5. Use the physical jumper to override the protection (asserts HDA_SDO high during rising edge of PWROK).6. Use FPT /d to dump the image. This test should now pass.
Test Pass/Fail Criteria:	Test passes if FDOPSS bit is set to '1' by default and set to '0' when intending to enter Intel® CSME Test Mode.

7.11 Serial Flash Single Input, Dual, or Quad Output Fast Read Test

Test ID	SPI_007
Test Case Title:	Single Input, Dual or Quad Output Fast Read Test
Mandatory/Optional:	Mandatory
Description:	This test is to verify that the flash parts supports Single Input, Dual, or Quad Output fast read if selected. This is a new mode of operation for serial flash that increases the read speed of SPI flash. If incorrectly configured there could be undesired operation.



Test ID	SPI_007
Objective:	This test is to verify that the flash parts supports Single Input, Dual, or Quad Output fast read if selected.
Procedure:	<p>PETS asks the user whether 'Single Input Dual or Quad Output Fast Read' is supported.</p> <p>If yes,</p> <ol style="list-style-type: none"> 1. PETS verifies that FLCOMP bit 20 is set to 1b. 2. PETS then uses Serial Flash Discovery Parameters to verify that all flash parts in the system support 'Single Input, Dual or Quad Output Fast Read'. 3. PETS checks whether softstraps are enabled to support Dual or Quad Output Fast Read Function. <ol style="list-style-type: none"> a. For Dual Output Read, PETS checks if FLCOMP bit 12 is set to 1 b. For Quad Output Read. PETS checks if FLCOMP bit 14 is set to 1 <p>Note: Quad Output Fast Read is not supported if the Flash device does not have SFDP.</p> <p>If No,</p> <ol style="list-style-type: none"> 1. PETS verifies that FLCOMP bit 20 is set to 0b
Test Pass/Fail Criteria:	<p>Test fails if there is an invalid configuration with single input, dual, or quad output fast read.</p> <p>Test results passes if settings are not invalid, and if single input, dual output fast read is verified by SFDP.</p>

Test ID	SPI_008
Test Case Title:	Dual and Quad I/O Fast Read
Mandatory/Optional:	Mandatory
Description:	This test is to verify that the flash parts supports Dual or Quad I/O Fast Read. This is a new mode of operation for serial flash that increases the read speed of SPI flash. If incorrectly configured there could be undesired operation.
Objective:	This test is to verify that the flash parts supports Dual or Quad I/O Fast Read
Procedure:	<p>PETS asks the user whether 'Dual or Quad I/O Fast Read' is supported.</p> <p>If yes,</p> <ol style="list-style-type: none"> 1. PETS uses Serial Flash Discovery Parameters (SFDP) to verify that all flash parts in the system support 'Dual or Quad I/O Fast Read'. 2. PETS then check if <ol style="list-style-type: none"> a. if FLCOMP bit 13 is set to 1 if Dual I/O fast read is supported; or b. FLCOMP bit 15 is set to 1 if Quad I/O fast read is supported. 3. PETS verifies that FLCOMP bit 20 set to 1 <p>If No,</p> <ol style="list-style-type: none"> 1. PETS then check if <ol style="list-style-type: none"> a. offset FLCOMP bit 13 is set to 0 if Dual I/O Fast Read is not supported; or 2. FLCOMP bit 15 is set to 0 if Quad I/O Fast Read is not supported.
Test Pass/Fail Criteria:	<p>Test fails if there is an invalid configuration with single input, Dual or Quad I/O Fast Read and if serial flash part does not support Serial Flash Discovery Parameters, Dual and Quad I/O Fast Read would not be supported</p> <p>Test results passes if settings are not invalid, and if single input, Dual or Quad I/O Fast Read is verified by SFDP.</p>

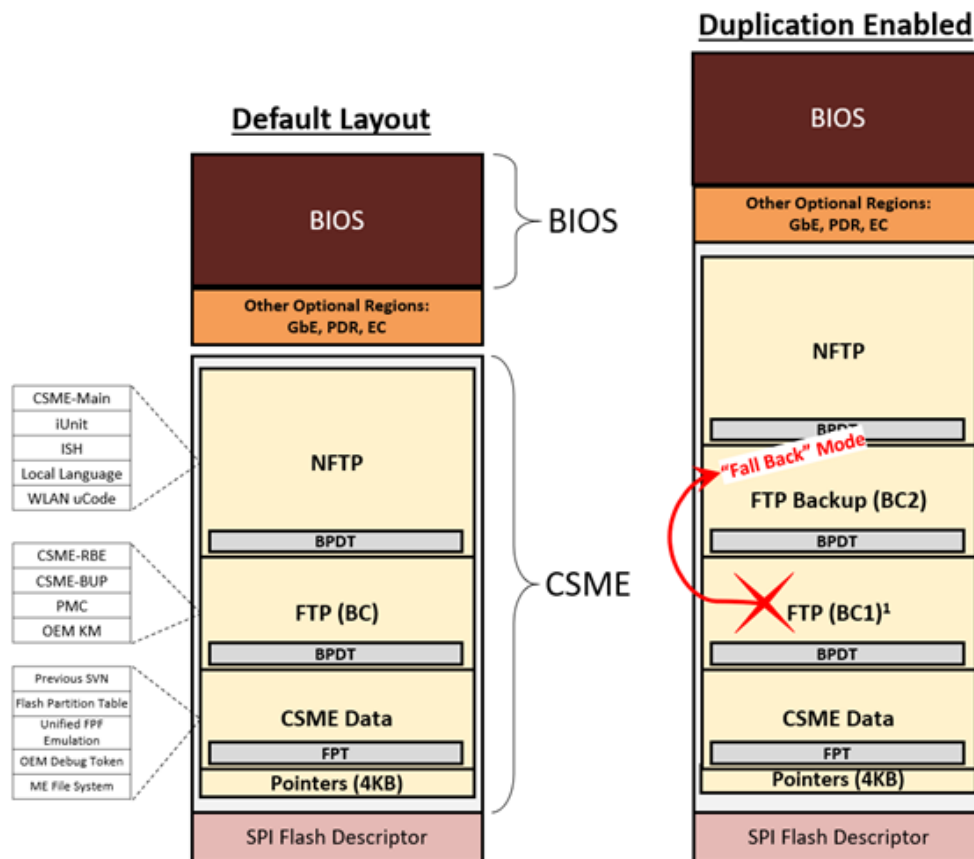
8 Intel® CSME Resiliency Compliance

The Intel® Converged Security and Management Engine Resiliency Compliance section serves test list for confirming CSME resiliency feature is enabled properly on OEM platform

8.1 Layout Overview with Boot Critical Redundancy

Below is a high-level diagram depicting Intel® CSME layout relative to other SPI regions, where:

- FTP: Fault Tolerant Partition
- BC: Boot Critical
- NFTP: Non-Fault Tolerant Partition



Note: TGL/RKL supports TCCS components included in BC1/2. Duplication of "Pointers" region also optionally available through an Intel® FIT configuration.



8.1.1 Layout Pointers

Intel® CSME ROM will look for layout configuration at the beginning of CSME region starting with the Pointers region. Intel® FIT tool will generate the locations and the pointers where ROM will use to find each of the main partitions from above diagram (FTP, NFTP, Data).

Offset (bytes) Layout 1.6 (CSME 12, 14)	Offset (bytes) Layout 1.7 (CSME 13, 15)	Description (Boot Critical Redundancy Disabled)
19 to 16	27:24	Data partition base offset (pointer to Flash partition Table)
23 to 20	31:28	Data partition size
27 to 24	35:32	FTP (boot critical) partition base offset (Pointer to logical boot partition 1 - BPDT 1)
31 to 28	39:36	FTP (boot critical) partition size
35 to 32	43:40	NFTP partition base offset (Pointer to logical boot partition 2 - BPDT 2)
39 to 36	47:44	NFTP partition size

Offset (bytes) Layout 1.6 (CSME 12, 14)	Offset (bytes) Layout 1.7 (CSME 13, 15)	Description (Boot Critical Redundancy Enabled)
19 to 16	27:24	Data partition base offset (pointer to Flash partition Table)
23 to 20	31:28	Data partition size
27 to 24	35:32	Primary FTP (BC1) partition base offset (Pointer to logical Boot Partition 1 - BPDT 1)
31 to 28	39:36	Primary FTP (BC1) partition size (Boot Partition 1)
35 to 32	43:40	Backup FTP (BC2) partition base offset (Pointer to logical boot partition 2 - BPDT 2)
39 to 36	47:44	Backup FTP (BC2) partition size (Boot Partition 2)
43 to 40	51:48	NFTP partition base offset (Pointer to logical boot partition 3 - BPDT 3)
47 to 44	55:52	NFTP partition size (Boot Partition 3)

8.1.2 BPDT

The Boot Partition Descriptor Table (BPDT) is a table of offsets to all individual sub-partitions contained within each of the LBPs (Logical Boot Partition). A sub-partition is as a sub-division of the logical boot partition.

The BPDT contains a header, immediately followed by 0 or more entries (number of following entries is indicated in the header).

Note that the BPDT is not signed and therefore its consumers must treat its contents with care.



Table 8-1. BPDT Layout in Intel® CSME Region

BPDT Header			
Field Name	Offset	Size (bytes)	Description
Signature	0	4	Validity signature. For a valid BPDT (aka "green"), this value must be 0x000055AA. During IFWI update, this value is modified. The value of 0x00AA55AA indicates the BPDT is valid and can be booted from, however the firmware update is still in progress (aka "yellow" - recovery mode). Any other value indicates an invalid BPDT structure (aka "red").
Descriptor Count	4	2	Number of BPDT entries following this header
Version	6	1	Version of this BPDT structure. '1' - Layout 1.6 (CSME 12 and 14) '2' - Layout 1.7 (CSME 13 and 15)
Reserved	7	1	Reserved
CRC32 checksum	8	4	CRC32 checksum of entire BPDT structure (Header and Entries) –The signature bytes [3:0] will not be checked
IFWI Version	12	4	Version of the particular IFWI build as marked by the build server
FIT Tool Version	16	8	Major/Minor/Build/Hotfix version of the FIT tool that was used to stitch the image. Not used by firmware
BPDT Entry			
Type	0	4	Bits 0:15 - type of the logical sub-partition indicated by this entry. Should be one of the following: 1 = CSME RBE 2 = CSME BUP 7 = CSME Main 8 = ISH 14 = PMC 15 = iUnit 18 = WLAN uCode 19 = Local Language 20 = OEM Key Manifest 21 = CSME Defaults 23 = IOM FW (TypeC)
Sub-partition offset	4	4	Offset of the logical sub-partition indicated by this entry. The offset is indicated in bytes from the beginning of the Boot Partition.
Sub-partition size	8	4	Size of the logical sub-partition indicated by this entry. The size is indicated in bytes.



8.1.3 High-Level Flow

1. CSME ROM finds BC1 offset from "Pointers" section attempts boot from BC1, if failure during boot (signature/integrity check fails), Reset and switch to BC2 and boot
2. When booting from BC2, continue boot to fully Normal CSME functionality with NFTP as well
3. Indicate in FWSTS that CSME booting from BC2 ("Fallback") while CSME remains in full functional working state as "Normal Mode"
4. To recover corrupted BC1, OEM may do normal CSME FW Update operation.

8.1.4 Firmware Status (FWSTS1) Register Indication Scenarios

Primary FTP Failure (BC1) Status	NFTP Failure Status	FWSTS Indication	OEM Action Required	Expected Outcome
Yes	Yes	FWSTS1.bit0-3 (Current State): Recovery [2] FWSTS1.bit10 (BC1 Boot Failed): Yes [1]	CSME FW update	Recovered Primary FTP (BC1) Recovered NFTP
Yes	No	FWSTS1.bit0-3 (Current State): Normal [2] FWSTS1.bit10 (BC1 Boot Failed): Yes [1]	CSME FW update	Recovered Primary FTP (BC1)
No	Yes	FWSTS1.bit0-3 (Current State): Recovery [2] FWSTS1.bit10 (BC1 Boot Failed): No [0]	CSME FW update	Recovered NFTP
No	No	FWSTS1.bit0-3 (Current State): Normal [2] FWSTS1.bit10 (BC1 Boot Failed): No [0]	No action required	N/A



8.2 Test Environment

The system under test is to be configured with the Intel® CSME **not** in manufacturing mode (fpt -closemfn completed).

8.3 Test Coverage Summary

Form Factor:

D = Desktop, M = Mobile, A = All in one

Network:

LAN = systems with LAN interface and test is performed using LAN interface

WLAN = systems with WLAN interface and test is performed using the WLAN interface

Test ID	Test Case Title	PETS/Manual	Form Factor	Network
Resilience_01	Boot Critical Redundancy Enabled	Manual	D M A	LAN or WLAN
Resilience_02	Critical Code Corruption - BPDT	Manual	D M A	LAN or WLAN
Resilience_03	Critical Code Corruption - BUP	Manual	D M A	LAN or WLAN
Resilience_04	Critical Code Corruption - PMC	Manual	D M A	LAN or WLAN
Resilience_05	Critical Code Corruption - TCSS	Manual	D M A	LAN or WLAN
Resilience_06	Recovery of Corrupted Primary Boot Critical (BC1) Partition	Manual	D M A	LAN or WLAN

8.4 Boot Critical Redundancy Enabled

Test ID:	Resilience_01
Test Case Title:	Boot Critical Redundancy Enabled
Mandatory/Optional:	Optional
Description:	The system is not in the Intel® ME Manufacturing Mode—when the system completes this test. This test is to confirm Boot Critical Redundancy Resiliency Feature is properly enabled and recognized by CSME. Do not perform any image corruption in this test.
Objective:	Verify "Boot Critical Code Redundancy" is properly enabled and system normally booting to primary partition
Procedure:	<ol style="list-style-type: none"> 1. Build image using FIT with redundancy enabled: Build -> Build Settings -> under "Image Build Settings", set "Redundancy Enabled" to "True". 2. Boot system at least once to OS. 3. Confirm MEInfo output shows "Boot critical code redundancy" as "Enabled" 4. Confirm "Current Boot Partition" is "1" 5. Confirm FWSTS1.bit10 = "0" also indicating "Current Boot Partition" is Primary FTP/BC1 where "0" means no failure in booting BC1.
Test Pass/Fail Criteria:	Pass: "Boot critical code redundancy" = "Enabled" AND "Current Boot Partition" = "1" Fail: "Boot critical code redundancy" = "Disabled"



8.5 Critical Code Corruption - BPDT1

Test ID:	Resilience_02
Test Case Title:	Critical Code Corruption – BPDT
Mandatory/Optional:	Optional
Description:	The system is not in the Intel® ME Manufacturing Mode—when the system completes this test. This test is to confirm CSME can fallback to Backup copy of FTP (BC2) when BC1 is corrupted.
Objective:	Verify Intel® CSME automatically falls back to BC2 when BC1 is corrupted.
Procedure:	<ol style="list-style-type: none"> 1. Build image using FIT with redundancy enabled: Build -> Build Settings -> under "Image Build Settings", set "Redundancy Enabled" to "True". 2. Boot system at least once to OS. 3. Place system in G3 and dump full SPI image. 4. From Layout Pointers, retrieve offset of "Boot Partition 1 (BP1)" (offset value located @ 35:32 within layout pointers). 5. "Boot Partition 1" starts with BPDT structure, manually corrupt structure writing "0xffffffff" at its offset 0 and save as "Corrupted_BPDT1.bin" 6. While system is in G3, flash Corrupted_BPDT1.bin image to SPI 7. Power up SUT and boot to OS 8. Confirm the following: <ol style="list-style-type: none"> a. MEInfo shows: "Current Boot Partition" = "2". b. FWSTS1.bit0-3 (Current State): Normal [5]. c. FWSTS1.bit10 (BC1 Boot Failed): Yes [1].
Test Pass/Fail Criteria:	<p>Pass: All below conditions must be met to pass the test:</p> <ol style="list-style-type: none"> 1. MEInfo shows: "Current Boot Partition" = "2". 2. FWSTS1.bit0-3 (Current State): Normal [5]. 3. FWSTS1.bit10 (BC1 Boot Failed): Yes [1]. <p>Fail: No Boot</p>



8.6 Critical Code Corruption - BUP

Test ID:	Resilience_03
Test Case Title:	Critical Code Corruption – BUP
Mandatory/Optional:	Optional
Description:	The system is not in the Intel® ME Manufacturing Mode—when the system completes this test. This test is to confirm CSME can fallback to Backup copy of FTP (BC2) when BC1 is corrupted.
Objective:	Verify Intel® CSME automatically falls back to BC2 when BC1 is corrupted.
Procedure:	<ol style="list-style-type: none">1. Build image using FIT with redundancy enabled: Build -> Build Settings -> under "Image Build Settings", set "Redundancy Enabled" to "True".2. Boot system at least once to OS.3. Place system in G3 and dump full SPI image.4. From Layout Pointers, retrieve offset of "Boot Partition 1 (BP1)" (offset value located @ 35:32 within layout pointers).5. "Boot Partition 1" starts with BPD1 structure. Within BPD1 find the BPD1 Entry for "CSME BUP" (type 2) and manually Corrupt partition content at offset 700KB [do 4 KB erase] and save as "Corrupted_BUP.bin" (Refer BPD1 details above).6. While system is in G3, flash Corrupted_BUP.bin image to SPI7. Power up SUT and boot to OS (expect to refer global reset)8. Confirm the following:<ol style="list-style-type: none">a. MEInfo shows: "Current Boot Partition" = "2".b. FWSTS1.bit0-3 (Current State): Normal [5]c. FWSTS1.bit10 (BC1 Boot Failed): Yes [1].
Test Pass/Fail Criteria:	<p>Pass: All below conditions must be met to pass the test:</p> <ol style="list-style-type: none">1. MEInfo shows: "Current Boot Partition" = "2".2. FWSTS1.bit0-3 (Current State): Normal [5].3. FWSTS1.bit10 (BC1 Boot Failed): Yes [1]. <p>Fail: No Boot</p>



8.7 Critical Code Corruption - PMC

Test ID:	Resilience_04
Test Case Title:	Critical Code Corruption – PMC
Mandatory/Optional:	Optional
Description:	The system is not in the Intel® ME Manufacturing Mode—when the system completes this test. This test is to confirm CSME can fallback to Backup copy of FTP (BC2) when BC1 is corrupted.
Objective:	Verify Intel® CSME automatically falls back to BC2 when BC1 is corrupted.
Procedure:	<ol style="list-style-type: none"> 1. Build image using FIT with redundancy enabled: Build -> Build Settings -> under "Image Build Settings", set "Redundancy Enabled" to "True". 2. Boot system at least once to OS. 3. Place system in G3 and dump full SPI image. 4. From Layout Pointers, retrieve offset of "Boot Partition 1 (BP1)" (offset value located @ 35:32 within layout pointers). 5. "Boot Partition 1" starts with BPD1 structure. Within BPD1 find the BPD1 Entry for "PMC" (type 14 or 0xE) and manually Corrupt the 4KB pointed by sub-partition offset [do 4 KB erase] and save as "Corrupted_PMC.bin" (Refer BPD1 details above). 6. While system is in G3, flash Corrupted_PMC.bin image to SPI 7. Power up SUT and boot to OS (expect to refer global reset) 8. Confirm the following: <ol style="list-style-type: none"> a. MEInfo shows: "Current Boot Partition" = "2". b. FWSTS1.bit0-3 (Current State): Normal [2]. c. FWSTS1.bit10 (BC1 Boot Failed): Yes [1].
Test Pass/Fail Criteria:	<p>Pass: All below conditions must be met to pass the test:</p> <ol style="list-style-type: none"> 1. MEInfo shows: "Current Boot Partition" = "2". 2. FWSTS1.bit0-3 (Current State): Normal [5] 3. FWSTS1.bit10 (BC1 Boot Failed): Yes [1]. <p>Fail: No Boot</p>



8.8 Critical Code Corruption - TypeC

Test ID:	Resilience_05
Test Case Title:	Critical Code Corruption – TypeC
Mandatory/Optional:	Optional
Description:	The system is not in the Intel® ME Manufacturing Mode—when the system completes this test. This test is to confirm CSME can fallback to Backup copy of FTP (BC2) when BC1 is corrupted.
Objective:	Verify Intel® CSME automatically falls back to BC2 when BC1 is corrupted.
Procedure:	<ol style="list-style-type: none">1. Build image using FIT with redundancy enabled: Build -> Build Settings -> under "Image Build Settings", set "Redundancy Enabled" to "True".2. Boot system at least once to OS.3. Place system in G3 and dump full SPI image.4. From Layout Pointers, retrieve offset of "Boot Partition 1 (BP1)" (offset value located @ 35:32 within layout pointers).5. "Boot Partition 1" starts with BPD1 structure. Within BPD1 find the BPD1 Entry for "IOM FW (TypeC)" (type 23 or 0x17) and manually Corrupt the 4KB pointed by sub-partition offset [do 4 KB erase] and save as "Corrupted_TypeC.bin" (Refer BPD1 details above).6. While system is in G3, flash Corrupted_TypeC.bin image to SPI7. Power up SUT and boot to OS (expect to refer global reset)8. Confirm the following:<ol style="list-style-type: none">a. MEInfo shows: "Current Boot Partition" = "2".b. FWSTS1.bit0-3 (Current State): Normal [5]c. FWSTS1.bit10 (BC1 Boot Failed): Yes [1].
Test Pass/Fail Criteria:	<p>Pass: All below conditions must be met to pass the test:</p> <ol style="list-style-type: none">1. MEInfo shows: "Current Boot Partition" = "2".2. FWSTS1.bit0-3 (Current State): Normal [5].3. FWSTS1.bit10 (BC1 Boot Failed): Yes [1]. <p>Fail: No Boot</p>



8.9 Recovery of Corrupted Primary Boot Critical (BC1) Partition

Test ID:	Resilience_06
Test Case Title:	Recovery of Corrupted Primary Boot Critical (BC1) Partition
Mandatory/Optional:	Optional
Description:	The system is not in the Intel® ME Manufacturing Mode—when the system completes this test. This test is to confirm CSME can boot from primary FTP (BC1) after FWupdate repaired corruption
Objective:	Verify Intel® CSME boot normally form BC1 after a successful FWUpdate repair BC1 corruption
Procedure:	<ol style="list-style-type: none"> 1. Perform Resilience_03 test above 2. Perform CSME FW Update (using FWUpdLcl or OEM Capsule update) 3. Confirm the following: <ol style="list-style-type: none"> a. MEInfo shows: "Current Boot Partition" = "1" b. FWSTS1.bit0-3 (Current State): Normal [5] c. FWSTS1.bit10 (BC1 Boot Failed): No [0]
Test Pass/Fail Criteria:	<p>Pass: All below conditions must be met to pass the test:</p> <ol style="list-style-type: none"> 1. MEInfo shows: "Current Boot Partition" = "1" 2. FWSTS1.bit0-3 (Current State): Normal [5] 3. FWSTS1.bit10 (BC1 Boot Failed): No [0] <p>Fail: Any of below conditions can fail this test:</p> <ol style="list-style-type: none"> 1. MEInfo shows: "Current Boot Partition" = "2" 2. FWSTS1.bit0-3 (Current State): Recovery [2] 3. FWSTS1.bit10 (BC1 Boot Failed): Yes [1]

§ §



9 Enhanced Serial Peripheral Interface (eSPI)

9.1 Introduction

The purpose of this chapter is to describe the test required in order to verify the eSPI configurations and functionality are according to Intel® compliancy. eSPI is a bus interface between the SoC/PCH and EC on Intel® IA platforms. It introduces Real-Time Flash Sharing through its MAF and SAF configurations, allocate low voltage of 1.8V to I/O buffers, reduces pin count, and allows for higher bandwidth.

9.2 Test Environment Setup

Tests in this chapter differ in implementation according to the SUT's (System Under Test) configuration; where SUTs can be configured to run with MAF or SAF enabled.

9.3 Tools for Testing

- Intel® Flash Image Tool (Intel® FIT)
- Intel® Flash Programming Tool (Intel® FPT)
- Intel® MEManuf
- Intel® FWupdate Tool
- Intel® Platform Flash Tool (Intel® PFT)

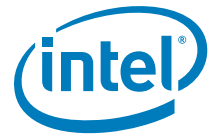
9.4 Test Coverage Summary

Platform, Operating System Support, How? Column describes the test methodology.

OS Support: W = Microsoft* Windows *, AOS = Android OS

How?: A = Fully Automated using Intel® PETS, I = Interactive using Intel® PETS and M = Manual.

Test ID	Test Case Title	PETS Package Name	OS Supported	How?
eSPI_001	Bootting with MAF configurations (straps set to MAF defaults)	N/A	W	M
eSPI_003	Platform boots with EC region	N/A	W	M
eSPI_004	Platform boots with EC region in different location	N/A	W	M
eSPI_005	Platform boots without EC region	N/A	W	M
eSPI_006	IFWI with empty EC region	N/A	W	M
eSPI_007	IFWI with empty EC binary	N/A	W	M
eSPI_008	Platform boots with default EC region permissions	N/A	W	M
eSPI_009	Platform boots with EC Read-Only permission to BIOS region	N/A	W	M



Test ID	Test Case Title	PETS Package Name	OS Supported	How?
eSPI_010	Platform boots with EC Read-Only permission to BIOS region and BIOS with RW permissions to EC	N/A	W	M
eSPI_011	Perform FWUpdate with MAF configurations	N/A	W	M

9.5 Booting with MAF Configurations (Straps Set to MAF Defaults)

Test ID:	eSPI_001
Test Case Title:	Bootting with MAF configurations (straps set to MAF defaults)
Platform:	Platforms with MAF configuration
Mandatory/Optional:	Mandatory
Objective:	Verify that the platform boots with default MAF configuration
Test Pass Criteria:	Test passes if platform boots to OS
Description:	Platform should boot to OS with all MAF straps set to default
Procedure:	<ol style="list-style-type: none"> 1. Follow Intel® SPI Programming Guide and review all soft straps applicable to MAF 2. Build IFWI with default straps for MAF using Intel® FIT 3. Flash IFWI onto the platform 4. Check that platform boots to OS

9.6 Platform Boots with EC Region

Test ID:	eSPI_003
Test Case Title:	Platform boots with EC region
Platform:	Platforms with SAF/MAF configuration
Mandatory/Optional:	Mandatory
Objective:	Verify that the platform boots with EC region
Test Pass Criteria:	Test passes if platform boots to OS
Description:	Setting the EC region in Intel® FIT and flashing the platform with IFWI that would successfully boot the platform to OS
Procedure:	<ol style="list-style-type: none"> 1. Create and IFWI in Intel® FIT with EC region 2. Flash IFWI onto the platform 3. Check that platform boots to OS



9.7 Platform Boots with EC Region in Different Place

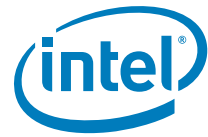
Test ID:	eSPI_004
Test Case Title:	Platform boots with EC region in different location
Platform:	Platforms with SAF/MAF configuration
Mandatory/Optional:	Mandatory
Objective:	Verify that the platform boots with EC region set in a different place
Test Pass Criteria:	Test passes if platform boots to OS
Description:	Stitching an EC region from a different place and flashing the IFWI that would successfully boot the platform to OS
Procedure:	<ol style="list-style-type: none">1. Create IFWI in Intel® FIT with EC region at a different location2. Flash IFWI onto the platform3. Check that the platform is booting to OS

9.8 Platform Boots without EC Region

Test ID:	eSPI_005
Test Case Title:	Platform boots without EC region
Platform:	Platform configured with No Flash Sharing
Mandatory/Optional:	Mandatory
Objective:	Verify that the platform boots successfully to OS without EC region
Test Pass Criteria:	Test passes if platform boots to OS
Description:	No Flash Sharing is a configuration in which EC resides on its own separate flash device.
Procedure:	<ol style="list-style-type: none">1. Create IFWI in Intel® FIT with EC region disabled2. Make sure Intel® FIT tool does not return any errors3. Flash IFWI onto the platform4. Check that the platform is booting to OS

9.9 IFWI with Empty EC Region

Test ID:	eSPI_006
Test Case Title:	IFWI with empty EC region
Platform:	Platforms with SAF/MAF configuration
Mandatory/Optional:	Mandatory
Objective:	Ensure that Intel® FIT tool prevents building an image with empty EC region



Test ID:	eSPI_006
Test Pass Criteria:	Intel® FIT does not build IFWI with empty EC region
Description:	EC region is mandatory when EC region is enabled in Intel® FIT. Intel® FIT should return error in building when EC region is enabled but no EC binary is provided
Procedure:	<ol style="list-style-type: none"> 1. Enable EC region in Intel® FIT 2. Create IFWI without providing EC region 3. Check that Intel® FIT does not build IFWI successfully

9.10 IFWI with Empty EC Binary

Test ID:	eSPI_007
Test Case Title:	IFWI with empty EC binary
Platform:	Platforms with SAF/MAF configuration
Mandatory/Optional:	Mandatory
Objective:	Verify that Intel® FIT does not create an IFWI if provided with an empty EC binary
Test Pass Criteria	Intel® FIT returns appropriate error and does not build IFWI
Description:	Providing EC binary is mandatory in SAF and MAF configurations, Intel® FIT should prevent building an image with an empty EC binary
Procedure:	<ol style="list-style-type: none"> 1. Enable EC region in Intel® FIT. 2. Do not provide 16byte EC binary as input. 3. Provide EC FW binary as input only. 4. Check that Intel® FIT does not complete IFWI building and return appropriate error.

9.11 Platform Boots with Default EC Region Permissions

Test ID:	eSPI_008
Test Case Title:	Platform boots with default EC region permissions
Platform:	Platforms with MAF configuration (Requires EOM for EC region)
Mandatory/Optional:	Mandatory
Objective:	Verify that EC region default permissions are loaded successfully and platform boots to OS
Test Pass Criteria:	Test passes if platform boots to OS, EOM is set, and Intel® MEManuf -EOL check passes
Description:	EC region is set with default Read/Write permissions to its own region.
Procedure:	<ol style="list-style-type: none"> 1. Create IFWI with default descriptor permissions in Intel® FIT. 2. Flash IFWI onto the platform. 3. Boot platform to OS. 4. Run Intel® FPT -closemef EC. 5. Run Intel® MEManuf -EOL. 6. Make sure that Intel® MEManuf -EOL check passes.



9.12 Platform Boots with EC Read-Only Permission to BIOS Region

Test ID:	eSPI_009
Test Case Title:	Platform boots with EC Read-Only permission to BIOS region
Platform:	Platforms with MAF configuration (Requires EOM for EC region)
Mandatory/Optional:	Mandatory
Objective:	This test is to verify that the platform is boot successfully to OS with EC having only read permission to BIOS region and with default permission for the other regions
Test Pass Criteria:	Test passes if platform boots to OS, EOM is set, and Intel® MEManuf -EOL check passes
Description:	EC region can be configured to Read-Only from BIOS region.
Procedure:	<ol style="list-style-type: none">1. Create IFWI with EC Read-Only access to BIOS region in descriptor permissions in Intel® FIT. They should be as follows:<ol style="list-style-type: none">a. EC read access should have a value of 0x103 in Intel® FIT2. Flash IFWI onto the platform.3. Boot platform to OS.4. Run Intel® FPT -closemfnf EC.5. Run Intel® MEManuf -EOL.6. Make sure that Intel® MEManuf -EOL check passes.

9.13 Platform Boots with EC Read-Only Permission to BIOS Region and BIOS with RW Permissions to EC

Test ID:	eSPI_010
Test Case Title:	Platform boots with EC Read-Only permission to BIOS region and BIOS with RW permissions to EC
Platform:	Platforms with MAF configuration (Requires EOM for EC region)
Mandatory/Optional:	Mandatory
Objective:	This test is to verify that the platform is boot successfully to OS with EC having only read permission to BIOS region and with BIOS have RW permissions to EC region
Test Pass Criteria:	Test passes if platform boots to OS, EOM is set, and Intel® MEManuf -EOL check passes
Description:	EC region can be configured to Read-Only from BIOS region as well as having BIOS with RW permissions to EC region
Procedure:	<ol style="list-style-type: none">1. Create IFWI with EC Read-Only access to BIOS region and BIOS with RW permissions to EC region in descriptor permissions in Intel® FIT. They should be as follows:<ol style="list-style-type: none">a. EC read access should have a value of 0x103 in Intel® FITb. Host CPU/BIOS read access should have a value of either 0x10F or 0x11Fc. Host CPU/BIOS write access should have a value of either 0x10A or 0x11A2. Flash IFWI onto the platform.3. Boot platform to OS.4. Run Intel® FPT -closemfnf EC.5. Run Intel® MEManuf -EOL.6. Make sure that Intel® MEManuf -EOL check passes.



9.14 Perform FWUpdate with MAF Configurations

Test ID:	eSPI_011
Test Case Title:	Perform FWUpdate with MAF configurations
Platform:	Platforms with MAF configurations
Mandatory/Optional:	Mandatory
Objective:	This test is to verify that the FWupdate flow works properly with MAF configurations and platform boots to OS
Test Pass Criteria:	Test passes if FWupdate flow is successfully completed with MAF configurations in place.
Description:	Ensuring that the platform would successfully boot with MAF configurations after performing a FWUpdate flow
Procedure:	<ol style="list-style-type: none">1. Follow steps 1 and 2 of test eSPI_001.2. Perform FWUpdate process on the platform - refer the System Tools User Guide for more information on the FWUpdate flow.3. Verify that platform can boot to OS after FWUpdate is completed.

§ §



10 Intel® CSME Power Management for Corporate Designs—Stress Testing

This chapter covers system power flow transitions, which involve the Intel® ME firmware (and/or software). Intel® Active Management Technology (Intel® AMT), as an application operating within in the Intel® ME, related configurations and flows found in Corporate designs are also included herein. The tests in this chapter are specifically intended to cover topics related to stress testing of the System Under Test (SUT).

10.1 System Power States

The following section describes power states that exist beyond the standard ACPI System Level Sx (S0, S3, S4, and S5) system S-states. Refer the main Power Management chapter for further details on Deep Sx and Intel® ME Power Gating.

10.2 Test Environment and System Configuration

Each test in this chapter contains a section outlining the test configuration.

Unless, where stated otherwise, Intel® AMT should be provisioned.

Because of the nature of the stress test and the flows that run, some tests are better suited for execution in an environment, where the SUT is configured to boot to DOS (via USB Key) or UEFI Shell. These tests are designated by the “(DOS/UEFI)” tag on their name as well as description in the test configuration.

The Intel® AMT networking interface used by the test, if any, is documented in the test configuration section as well. ‘LAN’ and ‘WLAN’ indicate that the test is explicitly using the respective LAN and/or wireless LAN (WLAN) interface. Some tests may have a combination of targeted network configurations. Example: WLAN-only and/or LAN+WLAN.

The test should be run on the SUT only in the case, where a matching network configuration is described.

Note: Not all Workstation and Intel® AMT Server designs may have Intel® AMT wireless LAN interface support.

Other details about the configuration of the SUT are described on a per-test basis. Refer the test contents for details.

10.2.1 Test Parameters

Each test in this chapter contains a table describing the system configuration to which the test is applicable. Below are some example test parameters blocks:

Example 2: Three-state with double trigger



System Power Source		AC+DC or AC-only
Power States	Initial	S0/MeOn (CM0,CM0-PG)
	Final	S0/MeOn (CM0,CM0-PG)
	Trigger	Remote Power Cycle
Intel® AMT	Power Package	PP2 (Intel® ME on in S0, wake in Sx/AC)
	WLAN Link Policy	LP3 (Enabled in S0, Sx/AC) where available

Example 1: Two-state with single trigger.

System Power Source		AC+DC or AC-only
Power States	Initial	S5/MeOn (CM3)
	Middle	G3/MeOff (CM-Off)
	Final	S5/MeOn (CM3)
	Trigger	Power loss → Power attach
Intel® AMT	Power Package	PP2 (Intel® ME on in S0, wake in Sx/AC)
	WLAN Link Policy	LP3 (Enabled in S0, Sx/AC) where available

System Power Source:

Describes the initial power source configuration of the system. Can be one of 'AC-only', 'DC-only', 'AC+DC', 'AC+DC,AC-only' (AC+DC or AC-only). The system may transition to different power source configurations during the test.

Power States:

Describes the 'Initial', 'Middle' (where applicable), and 'Final' power states of the SUT. The description is provided in terms of basic ACPI Sx states (S0, S3, S4, S5, G3) as well as Intel® ME availability ('MeOn' or 'MeOff'). Exact detail of system power states, including Deep Sx and/or Intel® ME power gating availability, is provided in each test. Included is also the 'Trigger' used to initiate the power flow transition. Many tests are limited one trigger, but some tests have two.

Intel® AMT:

Describes the 'Power Package' and 'WLAN Link Policy' (where available and applicable) that apply to the test. The Power Package controls, when manageability is available on the SUT and what power states the SUT and particularly the Intel® ME may transition to and from. The WLAN Link Policy describes, relative to Wireless LAN support, when manageability is available via Intel® AMT Wireless Networking support.

10.2.2 Tools for Testing

The following tools, as provided by Intel, may be used to execute automated tests listed herein:

- Intel® PETS: The latest version of the tool from the Intel® ME Compliancy and Debug kit release. Refer the Intel® PETS User Guide for exact instructions on how to load and setup the Intel® PETS software.
- Intel® Automated Power Switch (Intel® APS): The SUT should be connected to an Intel® APS 3 unit. In case an Intel® APS 3 is not available, select the Manual configuration in the Intel® PETS SUT profile configuration menu.
- Intel® PETS Local Agent: The local agent must be installed on the SUT.



10.2.3 Test Environment Setup

The SUT is to be configured with Intel® AMT set in manual provisioning mode with static IP address or DHCP. The management console may be a laptop or a desktop with a version of Microsoft* Windows supported by Intel® Platform Enablement Test Suite (Intel® PETS), and the SUT should have a version of Microsoft* Windows supported by Intel® PETS as well. The test network is comprised of a hub/switch and network cables. The SUT should have only one HDD.

While completing tests within this chapter, especially those which send the system to a specific S-state (S3, S4, S5, Deep Sx, etc.), it is important to ensure that the network wake events are properly configured for each applicable device (LAN and/or WLAN).

If not properly configured, the system may wake from a given S-state unexpectedly during test execution as a result of various network traffic within the test environment, and cause the test to result in a *false failure*.

The following Host OS LAN/WLAN driver settings allow the network device to process specific network frames **without** waking the system, where supported.

- Address Resolution Protocol (ARP) offload should be **enabled**
- Neighbor Solicitation (NS) offload should be **enabled**

The following Host OS LAN/WLAN driver settings allow the network device to wake the system, where supported, when specific network frames are received.

- Wake on Magic Packet should be **disabled**
- Wake on Pattern Match should be **disabled**
- Wake on Magic Packet from power off state should be **disabled**

Note: The wording used for the Host OS driver settings above may vary, and in some cases may not be available depending on driver support or system configuration.

Beyond the guidance in this section, refer individual test setup information for details on specifically, when to enable relevant wake functionality in the network device, as applicable to the test. In all other cases, the above settings should be applied by default.

10.2.4 Test Step Execution and Verification

The tests described in this chapter contain test steps, which are executed by Intel® PETS. While Intel® PETS brings a certain level of convenience and speed to the testing process, there are times where manual verification of steps is critical toward issue triage and debug.

Review the Test Step Execution and Verification section found in the main Intel® ME Power Management chapter before starting any test in this chapter.

The tests in this chapter are designed to run individually through a large number of iterations. Some of them require changing the system configuration before run. When performing very large numbers of iterations, the tests may take many hours, and in some cases several days.

Intel validation runs each of these tests, the number of iterations indicated. Each OEM should decide on the tolerance level required for their boards, and choose an appropriate number of iterations.



The tests in this section are not designed to run automatically one after the other, the test operator must place the SUT into the appropriate starting state, and then run the test in cycle. However each test individually ends with the SUT in the same state as when it started, allowing for easy iteration.

Apart from where explicitly mentioned, the Intel® AMT idle timeout value should be set larger than 1 minute to ensure the system does not pass the timeout before the required state is verified.

Tests that require the Intel® AMT idle timeout may fail if there is noise on the network preventing the Intel® ME from entering an idle state. Ensure that routers with spanning tree, for example, are not present on the test network.

If the platform is configured with Deep Sx or SUS Well Down enabled (on mobile platforms), according to the enabled Deep Sx S-state (Deep S4/S5), expect the Intel® ME to transition to CM-Off, when reaching that specific Sx state.

When running long iterations, ensure that the management console is set not to go to sleep, as this will pause the test.

Ensure that the SUT can boot to the designated Host OS without prompting the test operator for any actions (such as, scanning drivers and so forth); as this will affect stress tests, which boot the SUT to the Host OS.

Following Test step has been added to Power Flows, which ends at S0 state resuming back from S4 Hibernation. This will ensure System resumed from S4 state only and no other Sx state.

Verify that windows booted from hibernate i.e. value should be 0x02. "Run the following power shell command" Get-WinEvent-ProviderName Microsoft-Windows-Kernel-boot-MaxEvents 10 | where-Object{\$_.message -like "The boot type*"}

10.2.5 Setup Environment Tests

Review the Setup Environment Tests section found in the main Intel® ME Power Management chapter before starting any test in this chapter. Those tests are also valid for confirming basic test environment configuration and should be run before any other automated test described in this chapter.

Because Intel® AMT is provisioned in many of the tests in this chapter, it is strongly recommended to run the Setup Environment Tests for that technology as well before running any test in this chapter.

10.3 Test Coverage Summary

Test Requirements:

In general, all **applicable** tests are considered Mandatory in this section except for those specifically described as Optional or those which meet an Exemption. Refer the test Requirement section for details on test applicability.

Form Factor:

Mobile designs are broadly covered by the tests in this chapter, Desktop, All-in-One, and Workstation designs are Exempted, where classified as Non-Mobile (AC-only) systems. Refer the test Requirement section for Exemption details.

**System Power Model:**

Tests, which involve S3 flows will not support Modern Standby or Microsoft* Windows InstantGo. Refer the test Requirement section for Exemption details.

Network Configuration:

In general, all tests may run on systems with any combination of LAN and/or WLAN network interface support. For tests that work with a subset of configurations, such as LAN-only or LAN+WLAN. Refer the test Configuration section for details.

Methodology:

All tests are implemented in the Intel® PETS PM_Stress_Testing.xml test package.

Test ID	Test Case Title	SUT Boot Target
PM_ST_1	S5/CM3 to G3 to S5/CM3 via Power Cycle (DOS/UEFI)	DOS or UEFI Shell
PM_ST_2	Remote Power Cycle S0/CM0 (DOS/UEFI)	DOS or UEFI Shell
PM_ST_3	Remote Reset S0/CM0 (DOS/UEFI)	DOS or UEFI Shell
PM_ST_4	S3/CM3 to S3/CM-Off to S3/CM3 via AC-detach/attach	Microsoft* Windows
PM_ST_5	S0/CM0 to S3/CM-Off to S0/CM0 via Suspend/Resume	Microsoft* Windows
PM_ST_6	S0/CM0 to S3/CM3 to S0/CM0 via Suspend/Resume	Microsoft* Windows
PM_ST_7	S0/CM0 to S5/CM3 to S0/CM0 via Power Button Override (DOS/UEFI)	DOS or UEFI Shell
PM_ST_8	S0/CM0 to S4/CM-Off to S0/CM0 via Hibernate and WoL/WoWLAN	Microsoft* Windows
PM_ST_9	S0/CM0 to S4/CM3 to S0/CM0 via Hibernate and Remote Power-Up	Microsoft* Windows
PM_ST_10	S0/CM0 to S5/CM-Off to S0/CM0 via Shutdown and Power Button press	Microsoft* Windows
PM_ST_11	S0/CM0 to S5/CM3 to S0/CM0 via Shutdown and Remote Power-Up	Microsoft* Windows
PM_ST_12	S3/CM3 to S3/CM-Off to S3/CM3 via Intel® AMT idle timeout and Intel® AMT network access	Microsoft* Windows
PM_ST_13	S0/CM0 to S3/CM3 to S0/CM0 via Suspend and Remote Power-Up	Microsoft* Windows
PM_ST_14	S0/CM0 to S3/CM-Off to S0/CM0 via Suspend and Power Button press	Microsoft* Windows
PM_ST_16	Remote Power Cycle S0/CM0 (DOS/UEFI)	DOS or UEFI Shell
PM_ST_17	Remote Reset S0/CM0 (DOS/UEFI)	DOS or UEFI Shell
PM_ST_18	S5/CM3 to S5/CM-Off to S5/CM3 via AC-detach/attach	Microsoft* Windows
PM_ST_19	S5/CM3 to S5/CM-Off to S5/CM3 via Intel® AMT idle timeout and Intel® AMT network access	Microsoft* Windows
PM_ST_20	S0/CM0 to S3/CM3 to S0/CM0 via AC Attach (PP2)	Microsoft* Windows
PM_ST_21	S0/CM0 to S4/CM3 to S0/CM0 via AC Attach (PP2)	Microsoft* Windows
PM_ST_22	S0/CM0 to S5/CM3 to S0/CM0 via AC Attach (PP2)	Microsoft* Windows
PM_ST_23	S0/CM0 to S3/CM-Off to S0/CM0 via AC Attach (PP1)	Microsoft* Windows
PM_ST_24	S0/CM0 to S4/CM-Off to S0/CM0 via AC Attach (PP1)	Microsoft* Windows
PM_ST_25	S0/CM0 to S5/CM-Off to S0/CM0 via AC Attach (PP1)	Microsoft* Windows
PM_ST_26	S0/CM0 to S3/CM-Off to S0/CM0 via AC Attach	Microsoft* Windows
PM_ST_27	S0/CM0 to S4/CM-Off to S0/CM0 via AC Attach	Microsoft* Windows
PM_ST_28	S0/CM0 to S5/CM-Off to S0/CM0 via AC Attach	Microsoft* Windows
PM_ST_29	S0/CM0 to S3/CM-Off to S0/CM0 via AC Detach (PP2)	Microsoft* Windows
PM_ST_30	S0/CM0 to S4/CM-Off to S0/CM0 via AC Detach (PP2)	Microsoft* Windows
PM_ST_31	S0/CM0 to S5/CM-Off to S0/CM0 via AC Detach (PP2)	Microsoft* Windows
PM_ST_32	S0/CM0 to S3/CM-Off to S0/CM0 via AC Detach (PP1)	Microsoft* Windows
PM_ST_33	S0/CM0 to S4/CM-Off to S0/CM0 via AC Detach (PP1)	Microsoft* Windows
PM_ST_34	S0/CM0 to S5/CM-Off to S0/CM0 via AC Detach (PP1)	Microsoft* Windows



10.4 PM_ST_1 - S5/CM3 to G3 to S5/CM3 via Power Cycle (DOS/UEFI)

ID	PM_ST_1		
Title	S5/CM3 to G3/CM-Off to S5/CM3 via power cycle (AC+DC,AC-only/PP2/LP3)		
Requirement	Mandatory	Exemptions	None
Method	Automated by Intel® PETS		
Objective	This test checks the SUT power flow from S5/CM3 to G3/CM-Off to S5/CM3 via power cycle with the parameters outlined below.		
Configuration	Intel® AMT should be provisioned via manual mode. The SUT should be configured to boot to either DOS (via USB key) or UEFI shell. This test assumes that either LAN-only, WLAN-only, or both LAN and WLAN network interfaces are available on the SUT.		
Parameters	System Power Source		AC+DC or AC-only
	Power States	Initial	S5/MeOn (CM3)
		Middle	G3/MeOff (CM-Off)
		Final	S5/MeOn (CM3)
		Trigger	Power loss ➡ Power attach
	Intel® AMT	Power Package	PP2 (Intel® ME on in S0, wake in Sx/AC)
		WLAN Link Policy	LP3 (Enabled in S0, Sx/AC) where available
Setup	<ol style="list-style-type: none"> Set the SUT power source to AC+DC where supported; otherwise AC-only. Bring the SUT to the base state of S0/MeOn (CM0,CM0-PG). Set the active power package on the SUT to Power Package 2 (Intel® ME on in S0, wake in Sx/AC). Set the Intel® AMT WLAN link policy on the SUT to Link Policy 3 (Enabled in S0, Sx/AC), if the WLAN network interface is available. Shutdown the SUT via the brief Power Button press. Verify that the SUT is in S5/MeOn (CM3). Verify that Intel® AMT on the SUT responds to version queries via all available network interfaces. 		
Procedure	<ol style="list-style-type: none"> Remove power from the SUT via AC-detach, and if necessary also via DC-detach. Wait for 10 seconds before continuing to allow full power drain from the SUT. Verify that the SUT is in G3/MeOff (CM-Off). Set the SUT power source to AC+DC where supported; otherwise AC-only. For systems with DC-power support, consult the system design as it may be preferred to connect DC-power before AC-power. Verify that the SUT is in S5/MeOn (CM3). Verify that Intel® AMT on the SUT responds to version queries via all available network interfaces. <p>Repeat this procedure for the remaining number of cycles desired in the stress test.</p>		
Pass Criteria	<p>Test passes, if all steps are completed successfully for at least the recommended number of iterations as set by the OEM per the tolerance level of the system design.</p> <p>Suggested Iterations: Mobile: >=2000, Desktop/AIO/Workstation: >=750</p>		

10.5 PM_ST_2 - Remote Power Cycle S0/CM0 (DOS/UEFI)

ID	PM_ST_2		
Title	S0/CM0 to S0/CM0 via Remote Power Cycle (AC+DC, AC-only/PP2/LP3)		
Requirement	Mandatory	Exemptions	None
Method	Automated by Intel® PETS		



ID	PM_ST_2		
Objective	This test checks the SUT power flow from S0/CM0 to S0/CM0 via Remote Power Cycle with the parameters outlined below.		
Configuration	<p>Intel® AMT should be provisioned via manual mode.</p> <p>The SUT should be configured to boot to either DOS (via USB key) or UEFI shell.</p> <p>This test assumes that either LAN-only, WLAN-only, or both LAN and WLAN network interfaces are available on the SUT. Where both network interfaces are available, LAN shall be the initial active network interface in the test, and WLAN shall be the secondary network interface.</p>		
Parameters	System Power Source		AC+DC or AC-only
	Power States	Initial	S0/MeOn (CM0,CM0-PG)
		Final	S0/MeOn (CM0,CM0-PG)
		Trigger	Remote Power Cycle
	Intel® AMT	Power Package	PP2 (Intel® ME on in S0, wake in Sx/AC)
		WLAN Link Policy	LP3 (Enabled in S0, Sx/AC) where available
Setup	<ol style="list-style-type: none"> Set the SUT power source to AC+DC where supported; otherwise AC-only. Bring the SUT to the base state of S0/MeOn (CM0,CM0-PG). Set the active power package on the SUT to Power Package 2 (Intel® ME on in S0, wake in Sx/AC). Set the Intel® AMT WLAN link policy on the SUT to Link Policy 3 (Enabled in S0, Sx/AC), if the WLAN network interface is available. Verify that Intel® AMT on the SUT responds to version queries via all available network interfaces. 		
Procedure	<ol style="list-style-type: none"> Send a Remote Power Cycle command to the SUT via Intel® AMT by means of the active network interface. Verify that the SUT is in S0/MeOn (CM0,CM0-PG). If the active network interface is WLAN, wait 2 minutes before proceeding. Verify that Intel® AMT on the SUT responds to version queries via all available network interfaces. If available, set the active network interface to WLAN (from LAN) to run the following: <ol style="list-style-type: none"> Send a Remote Power Cycle command to the SUT via Intel® AMT by means of the WLAN network interface. Verify that the SUT is in S0/MeOn (CM0,CM0-PG). Wait 2 minutes before proceeding. Verify that Intel® AMT on the SUT responds to version queries via all available network interfaces. <p>Repeat this procedure for the remaining number of cycles desired in the stress test.</p>		
Pass Criteria	<p>Test passes, if all steps are completed successfully for at least the recommended number of iterations as set by the OEM per the tolerance level of the system design with no flash logs found.</p> <p>Suggested Iterations: Mobile: >=2000, Desktop/AIO/Workstation: >=750</p>		

10.6 PM_ST_3 - Remote Reset S0/CM0 (DOS/UEFI)

ID	PM_ST_3		
Title	S0/CM0 to S0/CM0 via Remote Reset (AC+DC, AC-only/PP2/LP3)		
Requirement	Mandatory	Exemptions	None
Method	Automated by Intel® PETS		
Objective	This test checks the SUT power flow from S0/CM0 to S0/CM0 via Remote Reset with the parameters outlined below.		
Configuration	<p>Intel® AMT should be provisioned via manual mode.</p> <p>The SUT should be configured to boot to either DOS (via USB key) or UEFI shell.</p> <p>This test assumes that either LAN-only, WLAN-only, or both LAN and WLAN network interfaces are available on the SUT. Where both network interfaces are available, LAN shall be the initial active network interface in the test, and WLAN shall be the secondary network interface.</p>		



ID	PM_ST_3		
Parameters	System Power Source		AC+DC or AC-only
	Power States	Initial	S0/MeOn (CM0,CM0-PG)
		Final	S0/MeOn (CM0,CM0-PG)
		Trigger	Remote Reset
	Intel® AMT	Power Package	PP2 (Intel® ME on in S0, wake in Sx/AC)
		WLAN Link Policy	LP3 (Enabled in S0, Sx/AC), where available
Setup	<ol style="list-style-type: none"> Set the SUT power source to AC+DC where supported; otherwise AC-only. Bring the SUT to the base state of S0/MeOn (CM0,CM0-PG). Set the active power package on the SUT to Power Package 2 (Intel® ME on in S0, wake in Sx/AC). Set the Intel® AMT WLAN link policy on the SUT to Link Policy 3 (Enabled in S0, Sx/AC), if the WLAN network interface is available. Verify that Intel® AMT on the SUT responds to version queries via all available network interfaces. 		
Procedure	<ol style="list-style-type: none"> Send a Remote Reset command to the SUT via Intel® AMT by means of the active network interface. Verify that the SUT is in S0/MeOn (CM0,CM0-PG). If the active network interface is WLAN, wait 2 minutes before proceeding. Verify that Intel® AMT on the SUT responds to version queries via all available network interfaces. If available, set the active network interface to WLAN (from LAN) to run the following: <ol style="list-style-type: none"> Send a Remote Reset command to the SUT via Intel® AMT by means of the WLAN network interface. Verify that the SUT is in S0/MeOn (CM0,CM0-PG). Wait 2 minutes before proceeding. Verify that Intel® AMT on the SUT responds to version queries via all available network interfaces. <p>Repeat this procedure for the remaining number of cycles desired in the stress test.</p>		
Pass Criteria	<p>Test passes, if all steps are completed successfully, for at least the recommended number of iterations as set by the OEM per the tolerance level of the system design with no flash logs found.</p> <p>Suggested Iterations: Mobile: >=2000, Desktop/AIO/Workstation: >=750</p>		

10.7 PM_ST_4 - S3/CM3 to S3/CM-Off to S3/CM3 via AC-detach/Attach

ID	PM_ST_4		
Title	S3/CM3 to S3/CM3-PG with AC Wake to S3/CM3 via AC-detach/AC-attach (AC+DC/PP2/LP3)		
Requirement	Mandatory	Exemptions	<input checked="" type="checkbox"/> Non-Mobile (AC-only) systems <input checked="" type="checkbox"/> Microsoft Windows* InstantGo* systems
Method	Automated by Intel® PETS		
Objective	This test checks the SUT power flow from S3/CM3 to S3/CM3-PG with AC Wake to S3/CM3 via AC-detach/AC-attach with the parameters outlined below.		
Configuration	<p>Intel® AMT should be provisioned via manual mode.</p> <p>This test assumes that either LAN-only, WLAN-only, or both LAN and WLAN network interfaces are available on the SUT.</p>		



ID	PM_ST_4		
Parameters	System Power Source		AC+DC
	Power States	Initial	S3/MeOn (CM3)
		Middle	S3/CM3-PG with Ac Wake
		Final	S3/MeOn (CM3)
		Trigger	AC-detach ➡ AC-attach
	Intel® AMT	Power Package	PP2 (Intel® ME on in S0, wake in Sx/AC)
		WLAN Link Policy	LP3 (Enabled in S0, Sx/AC) where available
Setup	<ol style="list-style-type: none"> 1. Set the SUT power source to AC+DC. 2. Bring the SUT to the base state of S0/MeOn (CM0,CM0-PG), and confirm that the Host OS is available. 3. Verify that a DC battery is connected to the SUT, and that it is charged to atleast 90% for long run testing. 4. Set the active power package on the SUT to Power Package 2 (Intel® ME on in S0, wake in Sx/AC). 5. Set the Intel® AMT WLAN link policy on the SUT to Link Policy 3 (Enabled in S0, Sx/AC), if the WLAN network interface is available. 6. Ensure that the Host OS network device drivers are configured to not wake the SUT. This includes enabling ARP and/or NS Offload features where available to prevent unexpected host wake events. Most especially, ensure that the Host OS Wireless Wake on LAN driver setting on the SUT is disabled, if the WLAN network interface is available. 7. Suspend the SUT via the Host OS. 8. Verify that the SUT is in S3/MeOn (CM3). 9. Verify that Intel® AMT on the SUT responds to version queries via all available network interfaces. 		
Procedure	<ol style="list-style-type: none"> 10. Set the SUT power source to DC-only. 11. Verify that the SUT is in S3/CM3-PG with AC Wake. 12. Set the SUT power source to AC+DC. 13. Verify that Intel® AMT on the SUT responds to version queries via all available network interfaces. 14. Verify that the SUT is in S3/MeOn (CM3). <p>Repeat this procedure for the remaining number of cycles desired in the stress test.</p>		
Pass Criteria	<p>Test passes, if all steps are completed successfully for at least the recommended number of iterations as set by the OEM per the tolerance level of the system design with no flash logs found.</p> <p>Suggested Iterations: Mobile: >=2000, Portable AIO >= 750</p>		



10.8 PM_ST_5 - S0/CM0 to S3/CM-Off to S0/CM0 via Suspend/Resume

ID	PM_ST_5	
Title	S0/CM0 to S3/CM-Off to S0/CM0 via Host OS suspend/resume (AC+DC,AC-only/PP1/LP3)	
Requirement	Mandatory	Exemptions <input checked="" type="checkbox"/> Microsoft Windows* InstantGo* systems
Method	Automated by Intel® PETS	
Objective	This test checks the SUT power flow from S0/CM0 to S3/CM-Off to S0/CM0 via Host OS suspend/resume with the parameters outlined below.	
Configuration	Intel® AMT should be provisioned via manual mode. This test assumes that either LAN-only, WLAN-only, or both LAN and WLAN network interfaces are available on the SUT.	
Parameters	System Power Source	AC+DC or AC-only
	Power States	Initial S0/MeOn (CM0,CM0-PG)
		Middle S3/MeOff (CM-Off)
		Final S0/MeOn (CM0,CM0-PG)
		Trigger Host OS suspend/resume
	Intel® AMT	Power Package PP1 (Intel® ME on in S0) WLAN Link Policy LP3 (Enabled in S0, Sx/AC) where available
Setup	<ol style="list-style-type: none"> Set the SUT power source to AC+DC where supported; otherwise AC-only. Bring the SUT to the base state of S0/MeOn (CM0,CM0-PG), and confirm that the Host OS is available. Set the active power package on the SUT to Power Package 1 (Intel® ME in S0). Set the Intel® AMT WLAN link policy on the SUT to Link Policy 3 (Enabled in S0, Sx/AC), if the WLAN network interface is available. Ensure that the Host OS network device drivers are configured to not wake the SUT. This includes enabling ARP and/or NS Offload features where available to prevent unexpected host wake events. Most especially, ensure that the Host OS Wireless Wake on LAN driver setting on the SUT is disabled, if the WLAN network interface is available. Record the Host OS last boot time on the SUT (to verify successful return from S3). Verify that Intel® AMT on the SUT responds to version queries via all available network interfaces. 	
Procedure	<ol style="list-style-type: none"> Suspend the SUT via the Host OS. Verify that the SUT is in S3/MeOff (CM-Off). Briefly press the Power Button on the SUT. Verify that the SUT is in S0/MeOn (CM0,CM0-PG). Verify that the Host OS on the SUT is available. Verify that Intel® AMT on the SUT responds to version queries via all available network interfaces. Verify the Host OS last boot time on the SUT matches the boot time recorded before entry into S3. Verify the second nibble of the FWSTS2 register on the SUT have a value of 0x60xxxxxx. <p>Repeat this procedure for the remaining number of cycles desired in the stress test.</p> <p>Check if there are any flash log. Success if there is no flash log.(Can test flash log by "MEInfo-FWSTS")</p>	
Pass Criteria	<p>Test passes, if all steps are completed successfully for at least the recommended number of iterations as set by the OEM per the tolerance level of the system design with no flash logs found.</p> <p>Suggested Iterations: Mobile: >=2000, Desktop/AIO/Workstation: >=750</p>	



10.9 PM_ST_6 - S0/CM0 to S3/CM3 to S0/CM0 via Suspend/Resume

ID	PM_ST_6	
Title	S0/CM0 to S3/CM3-PG to S0/CM0 via Host OS suspend/resume (AC+DC,AC-only/PP2/LP3)	
Requirement	Mandatory	Exemptions <input checked="" type="checkbox"/> Microsoft Windows* InstantGo* systems
Method	Automated by Intel® PETS	
Objective	This test checks the SUT power flow from S0/CM0 to S3/CM3-PG to S0/CM0 via Host OS suspend/resume with the parameters outlined below.	
Configuration	Intel® AMT should be provisioned via manual mode. This test assumes that either LAN-only, WLAN-only, or both LAN and WLAN network interfaces are available on the SUT.	
Parameters	System Power Source AC+DC or AC-only	
	Power States	Initial S0/MeOn (CM0,CM0-PG)
		Middle S3/MeOn (CM3)
		Final S0/MeOn (CM0,CM0-PG)
		Trigger Host OS suspend/resume
	Intel® AMT	Power Package PP2 (Intel® ME on in S0, wake in Sx/AC) WLAN Link Policy LP3 (Enabled in S0, Sx/AC) where available
Setup	<ol style="list-style-type: none"> Set the SUT power source to AC+DC where supported; otherwise AC-only. Bring the SUT to the base state of S0/MeOn (CM0,CM0-PG), and confirm that the Host OS is available. Set the active power package on the SUT to Power Package 2 (Intel® ME on in S0, wake in Sx/AC). Set the Intel® AMT WLAN link policy on the SUT to Link Policy 3 (Enabled in S0, Sx/AC), if the WLAN network interface is available. Ensure that the Host OS network device drivers are configured to not wake the SUT. This includes enabling ARP and/or NS Offload features where available to prevent unexpected host wake events. Most especially, ensure that the Host OS Wireless Wake on LAN driver setting on the SUT is disabled, if the WLAN network interface is available. Record the Host OS last boot time on the SUT (to verify successful return from S3). Verify that Intel® AMT on the SUT responds to version queries via all available network interfaces. 	
Procedure	<ol style="list-style-type: none"> Suspend the SUT via the Host OS. Verify that the SUT is in S3/MeOn (CM3). Briefly press the Power Button on the SUT. Verify that the SUT is in S0/MeOn (CM0,CM0-PG). Verify that the Host OS on the SUT is available. Verify that Intel® AMT on the SUT responds to version queries via all available network interfaces. Verify the Host OS last boot time on the SUT matches the boot time recorded before entry into S3. Verify the second nibble of the FWSTS2 register on the SUT have a value of 0x68xxxxxx. <p>Repeat this procedure for the remaining number of cycles desired in the stress test.</p> <p>Check if there are any flash log. Success if there is no flash log.(Can test flash log by "MEInfo -FWSTS")</p>	
Pass Criteria	<p>Test passes, if all steps are completed successfully for at least the recommended number of iterations as set by the OEM per the tolerance level of the system design with no flash logs found.</p> <p>Suggested Iterations: Mobile: >=2000, Desktop/AIO/Workstation: >=750</p>	



10.10 PM_ST_7 - S0/CM0 to S5/CM3 to S0/CM0 via Power Button Override (DOS/UEFI)

ID	PM_ST_7		
Title	S0/CM0 to S5/CM3 to S0/CM0 via Power Button override cycle (AC+DC, AC-only/PP2/LP3)		
Requirement	Mandatory	Exemptions	None
Method	Automated by Intel® PETS		
Objective	This test checks the SUT power flow from S0/CM0 to S5/CM3 to S0/CM0 via Power Button override cycle with the parameters outlined below.		
Configuration	Intel® AMT should be provisioned via manual mode. The SUT should be configured to boot to either DOS (via USB key) or UEFI shell. This test assumes that either LAN-only, WLAN-only, or both LAN and WLAN network interfaces are available on the SUT.		
Parameters	System Power Source		AC+DC or AC-only
	Power States	Initial	S0/MeOn (CM0,CM0-PG)
		Middle	S5/MeOn (CM3)
		Final	S0/MeOn (CM0,CM0-PG)
		Trigger	Power Button override ➡ Power Button press
	Intel® AMT	Power Package	PP2 (Intel® ME on in S0, wake in Sx/AC)
		WLAN Link Policy	LP3 (Enabled in S0, Sx/AC), where available
Setup	1. Set the SUT power source to AC+DC where supported; otherwise AC-only . 2. Bring the SUT to the base state of S0/MeOn (CM0,CM0-PG). 3. Set the active power package on the SUT to Power Package 2 (Intel® ME on in S0, wake in Sx/AC). 4. Set the Intel® AMT WLAN link policy on the SUT to Link Policy 3 (Enabled in S0, Sx/AC), if the WLAN network interface is available.		
Procedure	5. Shutdown the SUT via a Power Button press for more than 5 seconds . 6. Verify that the SUT is in S5/MeOn (CM3). 7. Verify that Intel® AMT on the SUT responds to version queries via all available network interfaces. 8. Briefly press the Power Button on the SUT. 9. Verify that the SUT is in S0/MeOn (CM0,CM0-PG). 10. Verify that Intel® AMT on the SUT responds to version query via the LAN network interface. 11. Verify that, after 2 minutes , Intel® AMT on the SUT responds to version query via the WLAN network interface, if available. Repeat this procedure for the remaining number of cycles desired in the stress test.		
Pass Criteria	Test passes, if all steps are completed successfully, for at least the recommended number of iterations as set by the OEM per the tolerance level of the system design with no flash logs found. Suggested Iterations: Mobile: >=2000, Desktop/AIO/Workstation: >=750		

10.11 PM_ST_8 - S0/CM0 to S4/CM-Off to S0/CM0 via Hibernate and WoL/WoWLAN

ID	PM_ST_8		
Title	S0/CM0 to S4/CM-Off to S0/CM0 via Host OS hibernate/magic packet cycle (AC+DC, AC-only/PP1/LP3)		
Requirement	Mandatory	Exemptions	<input checked="" type="checkbox"/> System without LAN support
Method	Automated by Intel® PETS		
Objective	This test checks the SUT power flow from S0/CM0 to S4/CM-Off to S0/CM0 via Host OS hibernate and magic packet cycle with the parameters outlined below.		



ID	PM_ST_8		
Configuration	<p>Intel® AMT should be provisioned via manual mode.</p> <p>If Deep S4 and/or Deep S5 are supported on the SUT, confirm the following:</p> <ul style="list-style-type: none"> The SUT and/or BIOS are properly configured to permit Deep S4/S5 entry. The correct Deep Sx policy is applied to the SUT profile in Intel® PETS. <p>This test assumes that LAN-only network interfaces are available on the SUT, where network interfaces are available, LAN shall be the initial active network interface in the test.</p>		
Parameters	System Power Source		AC+DC or AC-only
	Power States	Initial	S0/MeOn (CM0,CM0-PG)
		Middle	S4, S5, Deep S4, Deep S5/MeOff (CM-Off)
		Final	S0/MeOn (CM0,CM0-PG)
		Trigger	Host OS hibernate ➡ Magic Packet receipt
	Intel® AMT	Power Package	PP1 (Intel® ME on in S0)
Setup	<ol style="list-style-type: none"> Set the SUT power source to AC+DC where supported; otherwise AC-only. Bring the SUT to the base state of S0/MeOn (CM0,CM0-PG), and confirm that the Host OS is available. Set the active power package on the SUT to Power Package 1 (Intel® ME in S0). Ensure that the Host OS network device drivers are configured to not wake the SUT. This includes enabling ARP and/or NS Offload features, where available to prevent unexpected host wake events. Verify that Intel® AMT on the SUT responds to version query via the LAN network interface. 		
Procedure	<ol style="list-style-type: none"> Hibernate the SUT via the Host OS. Verify that the SUT is in S4,S5,Deep S4,Deep S5/MeOff (CM-Off). Send three magic packets, at 2 second intervals, by means of the active network interface. Verify that the SUT is in S0/MeOn (CM0,CM0-PG). Verify that the Host OS on the SUT is available. Verify that Intel® AMT on the SUT responds to version query via the LAN network interface. Verify that windows booted from hibernate i.e. value should be 0x02. "Run the following power shell command" Get-WinEvent-ProviderName Microsoft-Windows-Kernel-boot-MaxEvents 10 where-Object{\$_.message -like "The boot type*"} Verify the second nibble of the FWSTS2 register on the SUT have a value of 0x60xxxxxx. <p>Repeat this procedure for the remaining number of cycles desired in the stress test.</p> <p>Check if there are any flash log. Success if there is no flash log.(Can test flash log by "MEInfo -FWSTS")</p>		
Pass Criteria	<p>Test passes, if all steps are completed successfully for at least the recommended number of iterations as set by the OEM per the tolerance level of the system design with no flash logs found.</p> <p>Suggested Iterations: Mobile: >=2000, Desktop/AIO/Workstation: >=750</p>		



10.12 PM_ST_9 - S0/CM0 to S4/CM3 to S0/CM0 via Hibernate and Remote Power-Up

ID	PM_ST_9	
Title	S0/CM0 to S4/CM3 to S0/CM0 via Host OS hibernate/Remote Power Up cycle (AC+DC,AC-only/PP2/LP3)	
Requirement	Mandatory	Exemptions None
Method	Automated by Intel® PETS	
Objective	This test checks the SUT power flow from S0/CM0 to S4/CM3 to S0/CM0 via Host OS hibernate and Remote Power Up cycle with the parameters outlined below.	
Configuration	<p>Intel® AMT should be provisioned via manual mode.</p> <p>This test assumes that either LAN-only, WLAN-only, or both LAN and WLAN network interfaces are available on the SUT. Where both network interfaces are available, LAN shall be the initial active network interface in the test, and WLAN shall be the secondary network interface.</p>	
Parameters	System Power Source	
	Power States	Initial S0/MeOn (CM0,CM0-PG)
		Middle S4, S5/MeOn (CM3)
		Final S0/MeOn (CM0,CM0-PG)
		Trigger Host OS hibernate → Remote Power Up
	Intel® AMT	Power Package PP2 (Intel® ME on in S0, wake in Sx/AC) WLAN Link Policy LP3 (Enabled in S0, Sx/AC) where available
Setup	<ol style="list-style-type: none"> Set the SUT power source to AC+DC where supported; otherwise AC-only. Bring the SUT to the base state of S0/MeOn (CM0,CM0-PG), and confirm that the Host OS is available. Set the active power package on the SUT to Power Package 2 (Intel® ME on in S0, wake in Sx/AC). Set the Intel® AMT WLAN link policy on the SUT to Link Policy 3 (Enabled in S0, Sx/AC), if the WLAN network interface is available. Ensure that the Host OS network device drivers are configured to not wake the SUT. This includes enabling ARP and/or NS Offload features, where available to prevent unexpected host wake events. Verify that Intel® AMT on the SUT responds to version queries via all available network interfaces. 	
Procedure	<ol style="list-style-type: none"> Hibernate the SUT via the Host OS. Verify that the SUT is in S4,S5/MeOn (CM3). Send a Remote Power Up command to the SUT via Intel® AMT by means of the active network interface. Verify that the SUT is in S0/MeOn (CM0,CM0-PG). Verify that the Host OS on the SUT is available. Verify that Intel® AMT on the SUT responds to version queries via all available network interfaces. Verify that windows booted from hibernate i.e. value should be 0x02. "Run the following power shell command" Get-WinEvent-ProviderName Microsoft-Windows-Kernel-boot-MaxEvents 10 where-Object{\$_.message -like "The boot type*"} Verify the second nibble of the FWSTS2 register on the SUT have a value of 0x68xxxxxx. If available, set the active network interface to WLAN (from LAN) to run the following: <ol style="list-style-type: none"> Hibernate the SUT via the Host OS. Verify that the SUT is in S4,S5/MeOn (CM3). Send a Remote Power Up command to the SUT via Intel® AMT by means of the WLAN network interface. Verify that the SUT is in S0/MeOn (CM0,CM0-PG). Verify that the Host OS on the SUT is available. Verify that Intel® AMT on the SUT responds to version queries via all available network interfaces. Verify the second nibble of the FWSTS2 register on the SUT have a value of 0x68xxxxxx. <p>Repeat this procedure for the remaining number of cycles desired in the stress test.</p> <p>Check if there are any flash log. Success if there is no flash log.(Can test flash log by "MEInfo -FWSTS")</p>	



ID	PM_ST_9
Pass Criteria	Test passes, if all steps are completed successfully, for at least the recommended number of iterations as set by the OEM per the tolerance level of the system design with no flash logs found. Suggested Iterations: Mobile: >=2000, Desktop/AIO/Workstation: >=750

10.13 PM_ST_10 - S0/CM0 to S5/CM-Off to S0/CM0 via Shutdown and Power Button Press

ID	PM_ST_10		
Title	S0/CM0 to S5/CM-Off to S0/CM0 via Host OS shutdown/Power Button press cycle (AC+DC, AC-only/PP1/LP3)		
Requirement	Mandatory	Exemptions	None
Method	Automated by Intel® PETS		
Objective	This test checks the SUT power flow from S0/CM0 to S5/CM-Off to S0/CM0 via Host OS shutdown and Power Button press cycle with the parameters outlined below.		
Configuration	<p>Intel® AMT should be provisioned via manual mode.</p> <p>If Deep S5 is supported on the SUT, confirm the following:</p> <ul style="list-style-type: none"> The SUT and/or BIOS are properly configured to permit Deep S5 entry. The correct Deep Sx policy is applied to the SUT profile in Intel® PETS. <p>This test assumes that either LAN-only, WLAN-only, or both LAN and WLAN network interfaces are available on the SUT.</p>		
Parameters	System Power Source		AC+DC or AC-only
	Power States	Initial	S0/MeOn (CM0,CM0-PG)
		Middle	S4, S5, Deep S4, Deep S5/MeOff (CM-Off)
		Final	S0/MeOn (CM0,CM0-PG)
		Trigger	Host OS shutdown ➡ Power Button press
	Intel® AMT	Power Package	PP1 (Intel® ME on in S0)
		WLAN Link Policy	LP3 (Enabled in S0, Sx/AC) where available
Setup	<ol style="list-style-type: none"> Set the SUT power source to AC+DC where supported; otherwise AC-only. Bring the SUT to the base state of S0/MeOn (CM0,CM0-PG), and confirm that the Host OS is available. Set the active power package on the SUT to Power Package 1 (Intel® ME in S0). Set the Intel® AMT WLAN link policy on the SUT to Link Policy 3 (Enabled in S0, Sx/AC), if the WLAN network interface is available. Ensure that the Host OS network device drivers are configured to not wake the SUT. This includes enabling ARP and/or NS Offload features, where available to prevent unexpected host wake events. Verify that Intel® AMT on the SUT responds to version queries via all available network interfaces. 		



ID	PM_ST_10
Procedure	<p>7. Shutdown the SUT via the Host OS.</p> <p>8. Verify that the SUT is in S5, Deep S5/MeOff (CM-Off).</p> <p>9. Briefly press the Power Button on the SUT.</p> <p>10. Verify that the SUT is in S0/MeOn (CM0, CM0-PG).</p> <p>11. Verify that the Host OS on the SUT is available.</p> <p>12. Verify that Intel® AMT on the SUT responds to version queries via all available network interfaces.</p> <p>13. Verify the second nibble of the FWSTS2 register on the SUT have a value of 0x60xxxxxx.</p> <p>Repeat this procedure for the remaining number of cycles desired in the stress test.</p> <p>Check if there are any flash log. Success if there is no flash log. (Can test flash log by "MEInfo -FWSTS")</p>
Pass Criteria	<p>Test passes, if all steps are completed successfully for at least the recommended number of iterations as set by the OEM per the tolerance level of the system design with no flash logs found.</p> <p>Suggested Iterations: Mobile: >=2000, Desktop/AIO/Workstation: >=750</p>



10.14 PM_ST_11 - S0/CM0 to S5/CM3 to S0/CM0 via Shutdown and Remote Power-Up

ID	PM_ST_11		
Title	S0/CM0 to S5/CM3 to S0/CM0 via Host OS shutdown/Remote Power Up cycle (AC+DC, AC-only/PP2/LP3)		
Requirement	Mandatory	Exemptions	None
Method	Automated by Intel® PETS		
Objective	This test checks the SUT power flow from S0/CM0 to S5/CM3 to S0/CM0 via Host OS shutdown and Remote Power Up cycle with the parameters outlined below.		
Configuration	Intel® AMT should be provisioned via manual mode. This test assumes that either LAN-only, WLAN-only, or both LAN and WLAN network interfaces are available on the SUT. Where both network interfaces are available, LAN shall be the initial active network interface in the test, and WLAN shall be the secondary network interface.		
Parameters	System Power Source		AC+DC or AC-only
	Power States	Initial	S0/MeOn (CM0,CM0-PG)
		Middle	S5/MeOn (CM3)
		Final	S0/MeOn (CM0,CM0-PG)
		Trigger	Host OS shutdown ➔ Remote Power Up
	Intel® AMT	Power Package	PP2 (Intel® ME on in S0, wake in Sx/AC)
		WLAN Link Policy	LP3 (Enabled in S0, Sx/AC) where available
Setup	<ol style="list-style-type: none"> Set the SUT power source to AC+DC where supported; otherwise AC-only. Bring the SUT to the base state of S0/MeOn (CM0,CM0-PG), and confirm that the Host OS is available. Set the active power package on the SUT to Power Package 2 (Intel® ME on in S0, wake in Sx/AC). Set the Intel® AMT WLAN link policy on the SUT to Link Policy 3 (Enabled in S0, Sx/AC), if the WLAN network interface is available. Ensure that the Host OS network device drivers are configured to not wake the SUT. This includes enabling ARP and/or NS Offload features, where available to prevent unexpected host wake events. Verify that Intel® AMT on the SUT responds to version queries via all available network interfaces. 		



ID	PM_ST_11
Procedure	<p>7. Shutdown the SUT via the Host OS.</p> <p>8. Verify that the SUT is in S5/MeOn (CM3).</p> <p>9. Verify that Intel® AMT on the SUT responds to version queries via all available network interfaces.</p> <p>10. Send a Remote Power Up command to the SUT via Intel® AMT by means of the active network interface.</p> <p>11. Verify that the SUT is in S0/MeOn (CM0,CM0-PG).</p> <p>12. Verify that the Host OS on the SUT is available.</p> <p>13. Verify that Intel® AMT on the SUT responds to version queries via all available network interfaces.</p> <p>14. Verify the second nibble of the FWSTS2 register on the SUT have a value of 0x68xxxxxx.</p> <p>15. If available, set the active network interface to WLAN (from LAN) to run the following:</p> <ol style="list-style-type: none"> Shutdown the SUT via the Host OS. Verify that the SUT is in S5/MeOn (CM3). Verify that Intel® AMT on the SUT responds to version queries via all available network interfaces. Send a Remote Power Up command to the SUT via Intel® AMT by means of the WLAN network interface. Verify that the SUT is in S0/MeOn (CM0,CM0-PG). Verify that the Host OS on the SUT is available. Verify that Intel® AMT on the SUT responds to version queries via all available network interfaces. Verify the second nibble of the FWSTS2 register on the SUT have a value of 0x68xxxxxx. <p>Repeat this procedure for the remaining number of cycles desired in the stress test.</p> <p>Check if there are any flash log. Success if there is no flash log.(Can test flash log by "MEInfo -FWSTS")</p>
Pass Criteria	<p>Test passes, if all steps are completed successfully for at least the recommended number of iterations as set by the OEM per the tolerance level of the system design with no flash logs found.</p> <p>Suggested Iterations: Mobile: >=2000, Desktop/AIO/Workstation: >=750</p>



10.15 PM_ST_12 - S3/CM3 to S3/CM-Off to S3/CM3 via Intel® AMT Idle Timeout and Intel® AMT Network Access

ID	PM_ST_12		
Title	S3/CM3 to S3/CM3-PG to S3/CM3 via Intel® AMT idle timeout/Intel® AMT network access (AC+DC/PP2/LP3)		
Requirement	Mandatory	Exemptions	<input checked="" type="checkbox"/> Microsoft Windows* InstantGo* systems
Method	Automated by Intel® PETS		
Objective	This test checks the SUT power flow from S3/CM3 to S3/CM3-PG to S3/CM3 via AC-detach/AC-attach with the parameters outlined below.		
Configuration	Intel® AMT should be provisioned via manual mode. This test assumes that either LAN-only, WLAN-only, or both LAN and WLAN network interfaces are available on the SUT. Where both network interfaces are available, LAN shall be the initial active network interface in the test, and WLAN shall be the secondary network interface.		
Parameters	System Power Source		AC+DC
	Power States	Initial	S3/MeOn (CM3)
		Middle	S3/CM3-PG
		Final	S3/MeOn (CM3)
		Trigger	Intel® AMT idle timeout ➔ Intel® AMT network access
	Intel® AMT	Power Package	PP2 (Intel® ME on in S0, wake in Sx/AC)
		WLAN Link Policy	LP3 (Enabled in S0, Sx/AC), where available
Setup	<ol style="list-style-type: none"> Set the SUT power source to AC+DC. Bring the SUT to the base state of S0/MeOn (CM0,CM0-PG), and confirm that the Host OS is available. Set the active power package on the SUT to Power Package 2 (Intel® ME on in S0, wake in Sx/AC). Set the Intel® AMT WLAN link policy on the SUT to Link Policy 3 (Enabled in S0, Sx/AC), if the WLAN network interface is available. Ensure the Intel® AMT idle timeout on the SUT is set to 1 minute. Ensure that the Host OS network device drivers are configured to not wake the SUT. This includes enabling ARP and/or NS Offload features where available to prevent unexpected host wake events. Most especially, ensure that the Host OS Wireless Wake on LAN driver setting on the SUT is disabled, if the WLAN network interface is available. Suspend the SUT via the Host OS. Verify that the SUT is in S3/MeOn (CM3). Verify that Intel® AMT on the SUT responds to version queries via all available network interfaces. 		
Procedure	<ol style="list-style-type: none"> Wait for 3 minutes to allow the Intel® ME on the SUT to move to MeOff (CM3-PG) after Intel® AMT idle timeout. Verify that the SUT is in S3/CM3-PG. Verify that Intel® AMT on the SUT responds to version query by means of the active network interface. Verify that the SUT is in S3/MeOn (CM3). Verify that Intel® AMT on the SUT responds to version queries via all available network interfaces. If available, set the active network interface to WLAN (from LAN) to run the following: <ol style="list-style-type: none"> Wait for 3 minutes to allow the Intel® ME on the SUT to move to MeOff (CM3-PG) after Intel® AMT idle timeout. Verify that the SUT is in S3/CM3-PG. Verify that Intel® AMT on the SUT responds to version query via the WLAN network interface. Verify that the SUT is in S3/MeOn (CM3). Verify that Intel® AMT on the SUT responds to version queries via all available network interfaces. <p>Repeat this procedure for the remaining number of cycles desired in the stress test.</p>		



ID	PM_ST_12
Pass Criteria	Test passes, if all steps are completed successfully for at least the recommended number of iterations as set by the OEM per the tolerance level of the system design with no flash logs found. Suggested Iterations: Mobile: >=2000, Portable AIO >= 750

10.16 PM_ST_13 - S0/CM0 to S3/CM3 to S0/CM0 via Suspend and Remote Power-Up

ID	PM_ST_13		
Title	S0/CM0 to S3/CM3 to S0/CM0 via Host OS suspend/Remote Power Up cycle (AC+DC,AC-only/PP2/LP3)		
Requirement	Mandatory	Exemptions	<input checked="" type="checkbox"/> Microsoft Windows* InstantGo* systems
Method	Automated by Intel® PETS		
Objective	This test checks the SUT power flow from S0/CM0 to S3/CM3 to S0/CM0 via Host OS suspend and Remote Power Up cycle with the parameters outlined below.		
Configuration	Intel® AMT should be provisioned via manual mode. This test assumes that either LAN-only, WLAN-only, or both LAN and WLAN network interfaces are available on the SUT. Where both network interfaces are available, LAN shall be the initial active network interface in the test, and WLAN shall be the secondary network interface.		
Parameters	System Power Source		AC+DC or AC-only
	Power States	Initial	S0/MeOn (CM0,CM0-PG)
		Middle	S3/MeOn (CM3)
		Final	S0/MeOn (CM0,CM0-PG)
		Trigger	Host OS suspend ➡ Remote Power Up
	Intel® AMT	Power Package	PP2 (Intel® ME on in S0, wake in Sx/AC)
		WLAN Link Policy	LP3 (Enabled in S0, Sx/AC) where available
Setup	<ol style="list-style-type: none"> Set the SUT power source to AC+DC where supported; otherwise AC-only. Bring the SUT to the base state of S0/MeOn (CM0,CM0-PG), and confirm that the Host OS is available. Set the active power package on the SUT to Power Package 2 (Intel® ME on in S0, wake in Sx/AC). Set the Intel® AMT WLAN link policy on the SUT to Link Policy 3 (Enabled in S0, Sx/AC), if the WLAN network interface is available. Ensure that the Host OS network device drivers are configured to not wake the SUT. This includes enabling ARP and/or NS Offload features where available to prevent unexpected host wake events. Most especially, ensure that the Host OS Wireless Wake on LAN driver setting on the SUT is disabled, if the WLAN network interface is available. Verify that Intel® AMT on the SUT responds to version queries via all available network interfaces. 		



ID	PM_ST_13
Procedure	<p>7. Suspend the SUT via the Host OS.</p> <p>8. Verify that the SUT is in S3/MeOn (CM3).</p> <p>9. Verify that Intel® AMT on the SUT responds to version queries via all available network interfaces.</p> <p>10. Send a Remote Power Cycle command to the SUT via Intel® AMT by means of the WLAN network interface.</p> <p>11. Verify that the SUT is in S0/MeOn (CM0,CM0-PG).</p> <p>12. Verify that the Host OS on the SUT is available.</p> <p>13. Verify that Intel® AMT on the SUT responds to version queries via all available network interfaces.</p> <p>14. Verify the second nibble of the FWSTS2 register on the SUT have a value of 0x68xxxxxx.</p> <p>15. If available, set the active network interface to WLAN (from LAN) to run the following:</p> <ol style="list-style-type: none"> Shutdown the SUT via the Host OS. Verify that the SUT is in S3/MeOn (CM3). Verify that Intel® AMT on the SUT responds to version queries via all available network interfaces. Send a Remote Power Up command to the SUT via Intel® AMT by means of the WLAN network interface. Verify that the SUT is in S0/MeOn (CM0,CM0-PG). Verify that the Host OS on the SUT is available. Verify that Intel® AMT on the SUT responds to version queries via all available network interfaces. Verify the second nibble of the FWSTS2 register on the SUT have a value of 0x68xxxxxx. <p>Repeat this procedure for the remaining number of cycles desired in the stress test.</p> <p>Check if there are any flash log. Success if there is no flash log.(Can test flash log by "MEInfo-FWSTS")</p>
Pass Criteria	<p>Test passes, if all steps are completed successfully for at least the recommended number of iterations as set by the OEM per the tolerance level of the system design with no flash logs found.</p> <p>Suggested Iterations: Mobile: >=2000, Desktop/AIO/Workstation: >=750</p>

10.17 PM_ST_14 - S0/CM0 to S3/CM-Off to S0/CM0 via Suspend and Power Button Press

ID	PM_ST_14		
Title	S0/CM0 to S3/CM3-PG with AC Wake to S0/CM0 via Host OS suspend/Power Button press cycle (DC-only/PP2/LP3)		
Requirement	Mandatory	Exemptions	<input checked="" type="checkbox"/> Non-Mobile (AC-only) systems <input checked="" type="checkbox"/> Microsoft Windows* InstantGo* systems
Method	Automated by Intel® PETS		
Objective	This test checks the SUT power flow from S0/CM0 to S3/CM-Off to S0/CM0 via Host OS suspend and Power Button press cycle with the parameters outlined below.		
Configuration	Intel® AMT should be provisioned via manual mode. This test assumes that either LAN-only, WLAN-only, or both LAN and WLAN network interfaces are available on the SUT.		
Parameters	System Power Source		DC-only
	Power States	Initial	S0/MeOn (CM0,CM0-PG)
		Middle	S3/MeOff (CM-Off) with AC Wake
		Final	S0/MeOn (CM0,CM0-PG)
		Trigger	Host OS suspend ➡ Remote Power Up
	Intel® AMT	Power Package	PP2 (Intel® ME on in S0, wake in Sx/AC)
		WLAN Link Policy	LP3 (Enabled in S0, Sx/AC) where available



ID	PM_ST_14
Setup	<ol style="list-style-type: none"> 1. Set the SUT power source to AC+DC. 2. Bring the SUT to the base state of S0/MeOn (CM0,CM0-PG), and confirm that the Host OS is available. 3. Verify that a DC battery is connected to the SUT, and that it is charged to atleast 90% for long run testing. 4. Set the SUT power source to DC-only. 5. Set the active power package on the SUT to Power Package 2 (Intel® ME on in S0, wake in Sx/AC). 6. Set the Intel® AMT WLAN link policy on the SUT to Link Policy 3 (Enabled in S0, Sx/AC), if the WLAN network interface is available. 7. Ensure that the Host OS network device drivers are configured to not wake the SUT. This includes enabling ARP and/or NS Offload features where available to prevent unexpected host wake events. Most especially, ensure that the Host OS Wireless Wake on LAN driver setting on the SUT is disabled, if the WLAN network interface is available. 8. Verify that Intel® AMT on the SUT responds to version queries via all available network interfaces.
Procedure	<ol style="list-style-type: none"> 9. Suspend the SUT via the Host OS. 10. Verify that the SUT is in S3/CM3-PG with AC Wake. 11. Briefly press the Power Button on the SUT. 12. Verify that the SUT is in S0/MeOn (CM0,CM0-PG). 13. Verify that the Host OS on the SUT is available. 14. Verify that Intel® AMT on the SUT responds to version queries via all available network interfaces. 15. Verify the second nibble of the FWSTS2 register on the SUT have a value of 0x60xxxxx. <p>Repeat this procedure for the remaining number of cycles desired in the stress test.</p> <p>Check if there are any flash log. Success if there is no flash log.(Can test flash log by "MEInfo-FWSTS")</p>
Pass Criteria	<p>Test passes, if all steps are completed successfully, for at least the recommended number of iterations as set by the OEM per the tolerance level of the system design with no flash logs found.</p> <p>Suggested Iterations: Mobile: >=2000, Portable AIO: >=750</p>



10.18 PM_ST_16 - Remote Power Cycle S0/CM0 (DOS/UEFI)

ID	PM_ST_16		
Title	S0/CM0 to S0/CM0 via Remote Power Cycle (AC+DC,AC-only/PP1/LP3)		
Requirement	Mandatory	Exemptions	None
Method	Automated by Intel® PETS		
Objective	This test checks the SUT power flow from S0/CM0 to S0/CM0 via Remote Reset with the parameters outlined below.		
Configuration	Intel® AMT should be provisioned via manual mode. The SUT should be configured to boot to either DOS (via USB key) or UEFI shell. This test assumes that either LAN-only, WLAN-only, or both LAN and WLAN network interfaces are available on the SUT. Where both network interfaces are available, LAN shall be the initial active network interface in the test, and WLAN shall be the secondary network interface.		
Parameters	System Power Source		AC+DC or AC-only
	Power States	Initial	S0/MeOn (CM0,CM0-PG)
		Final	S0/MeOn (CM0,CM0-PG)
		Trigger	Remote Power Cycle
	Intel® AMT	Power Package	PP1 (Intel® ME on in S0)
		WLAN Link Policy	LP3 (Enabled in S0, Sx/AC) where available
Setup	<ol style="list-style-type: none">1. Set the SUT power source to AC+DC where supported; otherwise AC-only.2. Bring the SUT to the base state of S0/MeOn (CM0,CM0-PG).3. Set the active power package on the SUT to Power Package 1 (Intel® ME in S0).4. Set the Intel® AMT WLAN link policy on the SUT to Link Policy 3 (Enabled in S0, Sx/AC), if the WLAN network interface is available.5. Verify that Intel® AMT on the SUT responds to version queries via all available network interfaces.		
Procedure	<ol style="list-style-type: none">6. Send a Remote Power Cycle command to the SUT via Intel® AMT by means of the active network interface.7. Verify that the SUT is in S0/MeOn (CM0,CM0-PG).8. If the active network interface is WLAN, wait 2 minutes before proceeding.9. Verify that Intel® AMT on the SUT responds to version queries via all available network interfaces.10. If available, set the active network interface to WLAN (from LAN) to run the following:<ol style="list-style-type: none">a. Send a Remote Power Cycle command to the SUT via Intel® AMT by means of the WLAN network interface.b. Verify that the SUT is in S0/MeOn (CM0,CM0-PG).c. Wait 2 minutes before proceeding.d. Verify that Intel® AMT on the SUT responds to version queries via all available network interfaces. Repeat this procedure for the remaining number of cycles desired in the stress test.		
Pass Criteria	Test passes, if all steps are completed successfully, for at least the recommended number of iterations as set by the OEM per the tolerance level of the system design with no flash logs found. Suggested Iterations: Mobile: >=2000, Desktop/AIO/Workstation: >=750		

10.19 PM_ST_17 - Remote Reset S0/CM0 (DOS/UEFI)

ID	PM_ST_17		
Title	S0/CM0 to S0/CM0 via Remote Reset (AC+DC,AC-only/PP1/LP3)		
Requirement	Mandatory	Exemptions	None



ID	PM_ST_17	
Method	Automated by Intel® PETS	
Objective	This test checks the SUT power flow from S0/CM0 to S0/CM0 via Remote Reset with the parameters outlined below.	
Configuration	<p>Intel® AMT should be provisioned via manual mode.</p> <p>The SUT should be configured to boot to either DOS (via USB key) or UEFI shell.</p> <p>This test assumes that either LAN-only, WLAN-only, or both LAN and WLAN network interfaces are available on the SUT. Where both network interfaces are available, LAN shall be the initial active network interface in the test, and WLAN shall be the secondary network interface.</p>	
Parameters	System Power Source	
	Power States	AC+DC or AC-only
		Initial
		Final
	Intel® AMT	Trigger
		Power Package
		WLAN Link Policy
Setup	<ol style="list-style-type: none"> Set the SUT power source to AC+DC where supported; otherwise AC-only. Bring the SUT to the base state of S0/MeOn (CM0,CM0-PG). Set the active power package on the SUT to Power Package 1 (Intel® ME in S0). Set the Intel® AMT WLAN link policy on the SUT to Link Policy 3 (Enabled in S0, Sx/AC), if the WLAN network interface is available. Verify that Intel® AMT on the SUT responds to version queries via all available network interfaces. 	
Procedure	<ol style="list-style-type: none"> Send a Remote Reset command to the SUT via Intel® AMT by means of the active network interface. Verify that the SUT is in S0/MeOn (CM0,CM0-PG). If the active network interface is WLAN, wait 2 minutes before proceeding. Verify that Intel® AMT on the SUT responds to version queries via all available network interfaces. If available, set the active network interface to WLAN (from LAN) to run the following: <ol style="list-style-type: none"> Send a Remote Reset command to the SUT via Intel® AMT by means of the WLAN network interface. Verify that the SUT is in S0/MeOn (CM0,CM0-PG). Wait 2 minutes before proceeding. Verify that Intel® AMT on the SUT responds to version queries via all available network interfaces. <p>Repeat this procedure for the remaining number of cycles desired in the stress test.</p>	
Pass Criteria	<p>Test passes, if all steps are completed successfully, for at least the recommended number of iterations as set by the OEM per the tolerance level of the system design with no flash logs found.</p> <p>Suggested Iterations: Mobile: >=2000, Desktop/AIO/Workstation: >=750</p>	



10.20 PM_ST_18 - S5/CM3 to S5/CM-Off to S5/CM3 via AC-detach/Attach

ID	PM_ST_18		
Title	S5/CM3 to S5/CM3-PG with AC Wake to S5/CM3 via AC-detach/AC-attach (AC+DC/PP2/LP3)		
Requirement	Mandatory	Exemptions	<input checked="" type="checkbox"/> Non-Mobile (AC-only) systems
Method	Automated by Intel® PETS		
Objective	This test checks the SUT power flow from S5/CM3 to S5/CM-Off to S5/CM3 via AC-detach/AC-attach with the parameters outlined below.		
Configuration	<p>Intel® AMT should be provisioned via manual mode.</p> <p>If Deep S5 is supported on the SUT, confirm the following:</p> <ul style="list-style-type: none"> The SUT and/or BIOS are properly configured to permit Deep S5 entry. The correct Deep Sx policy is applied to the SUT profile in Intel® PETS. <p>This test assumes that either LAN-only, WLAN-only, or both LAN and WLAN network interfaces are available on the SUT.</p>		
Parameters	System Power Source		AC+DC
	Power States	Initial	S5/MeOn (CM3)
		Middle	S5, Deep S5/CM3-PG with AC Wake
		Final	S5/MeOn (CM3)
		Trigger	AC-detach → AC-attach
	Intel® AMT	Power Package	PP2 (Intel® ME on in S0, wake in Sx/AC)
		WLAN Link Policy	LP3 (Enabled in S0, Sx/AC) where available
Setup	<ol style="list-style-type: none"> Set the SUT power source to AC+DC. Bring the SUT to the base state of S0/MeOn (CM0,CM0-PG), and confirm that the Host OS is available. Verify that a DC battery is connected to the SUT, and that it is charged to atleast 90% for long run testing. Set the active power package on the SUT to Power Package 2 (Intel® ME on in S0, wake in Sx/AC). Set the Intel® AMT WLAN link policy on the SUT to Link Policy 3 (Enabled in S0, Sx/AC), if the WLAN network interface is available. Ensure that the Host OS network device drivers are configured to not wake the SUT. This includes enabling ARP and/or NS Offload features, where available to prevent unexpected host wake events. Shutdown the SUT via the Host OS. Verify that the SUT is in S5/MeOn (CM3). Verify that Intel® AMT on the SUT responds to version queries via all available network interfaces. 		
Procedure	<ol style="list-style-type: none"> Set the SUT power source to DC-only. Verify that the SUT is in S4,S5/MeOff (CM3-PG).with AC Wake. Set the SUT power source to AC+DC. Verify that Intel® AMT on the SUT responds to version queries via all available network interfaces. Verify that the SUT is in S5/MeOn (CM3). <p>Repeat this procedure for the remaining number of cycles desired in the stress test.</p>		
Pass Criteria	<p>Test passes, if all steps are completed successfully, for at least the recommended number of iterations as set by the OEM per the tolerance level of the system design with no flash logs found.</p> <p>Suggested Iterations: Mobile: >=2000, Portable AIO >= 750</p>		



10.21 PM_ST_19 - S5/CM3 to S5/CM-Off to S5/CM3 via Intel® AMT Idle Timeout and Intel® AMT Network Access

ID	PM_ST_19		
Title	S5/CM3 to S5/CM3-PG to S5/CM3 via Intel® AMT idle timeout/Intel® AMT network access (AC+DC/PP2/LP3)		
Requirement	Mandatory	Exemptions	None
Method	Automated by Intel® PETS		
Objective	This test checks the SUT power flow from S5/CM3 to S5/CM3-PG to S5/CM3 via AC-detach/AC-attach with the parameters outlined below.		
Configuration	Intel® AMT should be provisioned via manual mode. This test assumes that either LAN-only, WLAN-only, or both LAN and WLAN network interfaces are available on the SUT. Where both network interfaces are available, LAN shall be the initial active network interface in the test, and WLAN shall be the secondary network interface.		
Parameters	System Power Source		AC+DC
	Power States	Initial	S5/MeOn (CM3)
		Middle	S5/MeOff (CM3-PG)
		Final	S5/MeOn (CM3)
		Trigger	Intel® AMT idle timeout ➔ Intel® AMT network access
	Intel® AMT	Power Package	PP2 (Intel® ME on in S0, wake in Sx/AC)
		WLAN Link Policy	LP3 (Enabled in S0, Sx/AC) where available
Setup	<ol style="list-style-type: none"> Set the SUT power source to AC+DC where supported; otherwise AC-only. Bring the SUT to the base state of S0/MeOn (CM0,CM0-PG), and confirm that the Host OS is available. Set the active power package on the SUT to Power Package 2 (Intel® ME on in S0, wake in Sx/AC). Set the Intel® AMT WLAN link policy on the SUT to Link Policy 3 (Enabled in S0, Sx/AC), if the WLAN network interface is available. Ensure the Intel® AMT idle timeout on the SUT is set to 1 minute. Ensure that the Host OS network device drivers are configured to not wake the SUT. This includes enabling ARP and/or NS Offload features, where available to prevent unexpected host wake events. Shutdown the SUT via the Host OS. Verify that the SUT is in S5/MeOn (CM3). Verify that Intel® AMT on the SUT responds to version queries via all available network interfaces. 		
Procedure	<ol style="list-style-type: none"> Wait for 3 minutes to allow the Intel® ME on the SUT to move to MeOff (CM3-PG) after Intel® AMT idle timeout. Verify that the SUT is in S5/MeOff (CM3-PG). Verify that Intel® AMT on the SUT responds to version query by means of the active network interface. Verify that the SUT is in S5/MeOn (CM3). Verify that Intel® AMT on the SUT responds to version queries via all available network interfaces. If available, set the active network interface to WLAN (from LAN) to run the following: <ol style="list-style-type: none"> Wait for 3 minutes to allow the Intel® ME on the SUT to move to MeOff (CM3-PG) after Intel® AMT idle timeout. Verify that the SUT is in S5/MeOff (CM3-PG). Verify that Intel® AMT on the SUT responds to version query via the WLAN network interface. Verify that the SUT is in S5/MeOn (CM3). Verify that Intel® AMT on the SUT responds to version queries via all available network interfaces. <p>Repeat this procedure for the remaining number of cycles desired in the stress test.</p>		
Pass Criteria	<p>Test passes, if all steps are completed successfully for at least the recommended number of iterations as set by the OEM per the tolerance level of the system design with no flash logs found.</p> <p>Suggested Iterations: Mobile: >=2000, Portable AIO >= 750</p>		



10.22 PM_ST_20 - S0/CM0 to S3/CM3 to S0/CM0 via AC Attach

ID	PM_ST_20		
Title	S0/CM0 to S3/CM3 to S0/CM0 via AC-attach (AC+DC/PP2/LP3)		
Requirement	Mandatory	Exemptions	<input checked="" type="checkbox"/> Non-Mobile (AC-only) systems
Method	Automated by Intel® PETS		
Objective	This test checks the SUT power flow from S0/CM0 to S3/CM3 to S0/CM0 via AC-attach with the parameters outlined below.		
Configuration	Intel® AMT should be provisioned via manual mode. This test assumes that either LAN-only, WLAN-only, or both LAN and WLAN network interfaces are available on the SUT.		
Parameters	System Power Source		DC-only
	Power States	Initial	S0/MeOn (CM0)
		Middle	S3/MeOn (CM3)
		Final	S0/MeOn (CM0)
		Trigger	AC-attach in S3 state
	Intel® AMT	Power Package	PP2 (Intel® ME on in S0, wake in Sx/AC)
		WLAN Link Policy	LP3 (Enabled in S0, Sx/AC) where available
Setup	<ol style="list-style-type: none"> Set the SUT power source to AC+DC. Bring the SUT to the base state of S0/MeOn (CM0,CM0-PG), and confirm that the Host OS is available. Verify that a DC battery is connected to the SUT, and that it is charged to atleast 90% for long run testing. Set the SUT power source to DC-only. Set the active power package on the SUT to Power Package 2 (Intel® ME on in S0, wake in Sx/AC). Set the Intel® AMT WLAN link policy on the SUT to Link Policy 3 (Enabled in S0, Sx/AC), if the WLAN network interface is available. Ensure that the Host OS network device drivers are configured to not wake the SUT. This includes enabling ARP and/or NS Offload features, where available to prevent unexpected host wake events. Record the Host OS last boot time on the SUT (to verify successful return from S3). 		
Procedure	<ol style="list-style-type: none"> Suspend the SUT via the Host OS. Verify that the SUT is in S3/MeOff (CM-Off). Set the SUT Power Source to AC+DC. Verify that the SUT is in S3/MeOn (CM3). Verify that Intel® AMT on the SUT responds to version queries via all available network interfaces. Briefly Press the Power Button on the SUT. Verify that the SUT is in S0/MeOn (CM0). Verify that the Host on the SUT is available. Verify the Host OS last boot time on the SUT matches the boot time recorded before entry into S3. Verify that Intel® AMT on the SUT responds to version queries via all available network interfaces. <p>Repeat this procedure for the remaining number of cycles desired in the stress test.</p> <p>Check if there are any flash log. Success if there is no flash log.(Can test flash log by "MEInfo -FWSTS")</p>		
Pass Criteria	<p>Test passes, if Intel (R) CSME functions Properly when AC Source attached in S3 State with no flash logs found.</p> <p>Suggested Iterations: Mobile: >=2000, Portable AIO >= 750</p>		



10.23 PM_ST_21 - S0/CM0 to S4/CM3 to S0/CM0 via AC-Attach

ID	PM_ST_21	
Title	S0/CM0 to S4/CM3 to S0/CM0 via AC-attach (AC+DC/PP2/LP3)	
Requirement	Mandatory	Exemptions <input checked="" type="checkbox"/> Non-Mobile (AC-only) systems
Method	Automated by Intel® PETS	
Objective	This test checks the SUT power flow from S0/CM0 to S4/CM3 to S0/CM0 via AC-attach with the parameters outlined below.	
Configuration	<p>Intel® AMT should be provisioned via manual mode.</p> <p>If Deep S4 and/or Deep S5 are supported on the SUT, confirm the following:</p> <ul style="list-style-type: none"> The SUT and/or BIOS are properly configured to permit Deep S4/S5 entry. The correct Deep Sx policy is applied to the SUT profile in Intel® PETS. <p>This test assumes that either LAN-only, WLAN-only, or both LAN and WLAN network interfaces are available on the SUT.</p>	
Parameters	System Power Source	
	Power States	DC-only
		S0/MeOn (CM0)
		S4/MeOn (CM3)
		S0/MeOn (CM0)
		AC-attach in S4 state
	Intel® AMT	Power Package PP2 (Intel® ME on in S0, wake in Sx/AC)
		WLAN Link Policy LP3 (Enabled in S0, Sx/AC) where available
Setup	<ol style="list-style-type: none"> Set the SUT power source to AC+DC. Bring the SUT to the base state of S0/MeOn (CM0,CM0-PG), and confirm that the Host OS is available. Verify that a DC battery is connected to the SUT, and that it is charged to atleast 90% for long run testing. Set the SUT power source to DC-only. Set the active power package on the SUT to Power Package 2 (Intel® ME on in S0, wake in Sx/AC). Set the Intel® AMT WLAN link policy on the SUT to Link Policy 3 (Enabled in S0, Sx/AC), if the WLAN network interface is available. Ensure that the Host OS network device drivers are configured to not wake the SUT. This includes enabling ARP and/or NS Offload features, where available to prevent unexpected host wake events. 	
Procedure	<ol style="list-style-type: none"> Hibernate the SUT via the Host OS. Verify that the SUT is in S4/MeOff (CM-Off). Set the SUT Power Source to AC+DC. Verify that the SUT is in S4/M3 (CM3). Verify that Intel® AMT on the SUT responds to version queries via all available network interfaces. Briefly Press the Power Button on the SUT. Verify that the SUT is in S0/MeOn (CM0). Verify that the Host on the SUT is available. Verify that windows booted from hibernate i.e. value should be 0x02. "Run the following power shell command" Get-WinEvent-ProviderName Microsoft-Windows-Kernel-boot-MaxEvents 10 where-Object{\$_.message -like "The boot type*"}. Verify that Intel® AMT on the SUT responds to version queries via all available network interfaces. <p>Repeat this procedure for the remaining number of cycles desired in the stress test.</p> <p>Check if there are any flash log. Success if there is no flash log.(Can test flash log by "MEInfo -FWSTS")</p>	
Pass Criteria	<p>Test passes, if Intel (R) CSME functions Properly, when AC Source attached in S4 State with no flash logs found.</p> <p>Suggested Iterations: Mobile: >=2000, Portable AIO >= 750</p>	



10.24 PM_ST_22 - S0/CM0 to S5/CM3 to S0/CM0 via AC Attach

ID	PM_ST_22		
Title	S0/CM0 to S5/CM3 to S0/CM0 via AC-attach (AC+DC/PP2/LP3)		
Requirement	Mandatory	Exemptions	<input checked="" type="checkbox"/> Non-Mobile (AC-only) systems
Method	Automated by Intel® PETS		
Objective	This test checks the SUT power flow from S0/CM0 to S5/CM3 to S0/CM0 via AC-attach with the parameters outlined below.		
Configuration	<p>Intel® AMT should be provisioned via manual mode.</p> <p>If Deep S5 is supported on the SUT, confirm the following:</p> <ul style="list-style-type: none"> The SUT and/or BIOS are properly configured to permit Deep S5 entry. The correct Deep Sx policy is applied to the SUT profile in Intel® PETS. <p>This test assumes that either LAN-only, WLAN-only, or both LAN and WLAN network interfaces are available on the SUT.</p>		
Parameters	System Power Source		DC-only
	Power States	Initial	S0/MeOn (CM0)
		Middle	S5/MeOn (CM3)
		Final	S0/MeOn (CM0)
		Trigger	AC-attach in S5 state
	Intel® AMT	Power Package	PP2 (Intel® ME on in S0, wake in Sx/AC)
		WLAN Link Policy	LP3 (Enabled in S0, Sx/AC) where available
Setup	<ol style="list-style-type: none"> Set the SUT power source to AC+DC. Bring the SUT to the base state of S0/MeOn (CM0,CM0-PG), and confirm that the Host OS is available. Verify that a DC battery is connected to the SUT, and that it is charged to atleast 90% for long run testing. Set the SUT power source to DC-only. Set the active power package on the SUT to Power Package 2 (Intel® ME on in S0, wake in Sx/AC). Set the Intel® AMT WLAN link policy on the SUT to Link Policy 3 (Enabled in S0, Sx/AC), if the WLAN network interface is available. Ensure that the Host OS network device drivers are configured to not wake the SUT. This includes enabling ARP and/or NS Offload features, where available to prevent unexpected host wake events. 		
Procedure	<ol style="list-style-type: none"> Shutdown the SUT via the Host OS. Verify that the SUT is in S5,Deep S5/MeOff (CM-Off). Set the SUT Power Source to AC+DC. Verify that the SUT is in S5/MeOn (CM3). Verify that Intel® AMT on the SUT responds to version queries via all available network interfaces. Briefly Press the Power Button on the SUT. Verify that the SUT is in S0/MeOn (CM0). Verify that the Host on the SUT is available. Verify that Intel® AMT on the SUT responds to version queries via all available network interfaces. <p>Repeat this procedure for the remaining number of cycles desired in the stress test.</p> <p>Check if there are any flash log. Success if there is no flash log.(Can test flash log by "MEInfo -FWSTS")</p>		
Pass Criteria	<p>Test passes, if Intel (R) CSME functions Properly when AC Source attached in S5 State with no flash logs found.</p> <p>Suggested Iterations: Mobile: >=2000, Portable AIO >= 750</p>		



10.25 PM_ST_23 - S0/CM0 to S3/CM-Off to S0/CM0 via AC Attach

ID	PM_ST_23	
Title	S0/CM0 to S3/CM-Off to S0/CM0 via AC-attach (AC+DC/PP1/LP3)	
Requirement	Mandatory	Exemptions <input checked="" type="checkbox"/> Non-Mobile (AC-only) systems
Method	Automated by Intel® PETS	
Objective	This test checks the SUT power flow from S0/CM0 to S3/CM-Off to S0/CM0 via AC-attach with the parameters outlined below.	
Configuration	Intel® AMT should be provisioned via manual mode. This test assumes that either LAN-only, WLAN-only, or both LAN and WLAN network interfaces are available on the SUT.	
Parameters	System Power Source	
	Power States	DC-only
		Initial
		Middle
		Final
	Intel® AMT	Trigger
		Power Package
		WLAN Link Policy
Setup	<ol style="list-style-type: none"> Set the SUT power source to AC+DC. Bring the SUT to the base state of S0/MeOn (CM0,CM0-PG), and confirm that the Host OS is available. Verify that a DC battery is connected to the SUT, and that it is charged to atleast 90% for long run testing. Set the SUT power source to DC-only. Set the active power package on the SUT to Power Package 1 (Intel® ME in S0). Set the Intel® AMT WLAN link policy on the SUT to Link Policy 3 (Enabled in S0, Sx/AC), if the WLAN network interface is available. Ensure that the Host OS network device drivers are configured to not wake the SUT. This includes enabling ARP and/or NS Offload features, where available to prevent unexpected host wake events. Record the Host OS last boot time on the SUT (to verify successful return from S3). 	
Procedure	<ol style="list-style-type: none"> Suspend the SUT via the Host OS. Verify that the SUT is in S3/MeOff (CM-Off). Set the SUT Power Source to AC+DC. Verify that the SUT is in S3/MeOff (CM-Off). Briefly Press the Power Button on the SUT. Verify that the SUT is in S0/MeOn (CM0). Verify that the Host on the SUT is available. Verify the Host OS last boot time on the SUT matches the boot time recorded before entry into S3. Verify that Intel® AMT on the SUT responds to version queries via all available network interfaces. <p>Repeat this procedure for the remaining number of cycles desired in the stress test.</p> <p>Check if there are any flash log. Success if there is no flash log.(Can test flash log by "MEInfo -FWSTS")</p>	
Pass Criteria	<p>Test passes, if Intel (R) CSME functions properly with no flash logs found i.e. stays MOff, when AC Source attached in S3 State.</p> <p>Suggested Iterations: Mobile: >=2000, Portable AIO >= 750</p>	



10.26 PM_ST_24 - S0/CM0 to S4/CM-Off to S0/CM0 via AC Attach

ID	PM_ST_24		
Title	S0/CM0 to S4/CM-Off to S0/CM0 via AC-attach (AC+DC/PP1/LP3)		
Requirement	Mandatory	Exemptions	<input checked="" type="checkbox"/> Non-Mobile (AC-only) systems
Method	Automated by Intel® PETS		
Objective	This test checks the SUT power flow from S0/CM0 to S4/CM-Off to S0/CM0 via AC-attach with the parameters outlined below.		
Configuration	<p>Intel® AMT should be provisioned via manual mode.</p> <p>If Deep S4 and/or Deep S5 are supported on the SUT, confirm the following:</p> <ul style="list-style-type: none"> The SUT and/or BIOS are properly configured to permit Deep S4/S5 entry. The correct Deep Sx policy is applied to the SUT profile in Intel® PETS. <p>This test assumes that either LAN-only, WLAN-only, or both LAN and WLAN network interfaces are available on the SUT.</p>		
Parameters	System Power Source		DC-only
	Power States	Initial	S0/MeOn (CM0)
		Middle	S4/MeOff (CM-Off)
		Final	S0/MeOn (CM0)
		Trigger	AC-attach in S4 state
	Intel® AMT	Power Package	PP1 (Intel® ME on in S0)
		WLAN Link Policy	LP3 (Enabled in S0, Sx/AC) where available
Setup	<ol style="list-style-type: none"> Set the SUT power source to AC+DC. Bring the SUT to the base state of S0/MeOn (CM0,CM0-PG), and confirm that the Host OS is available. Verify that a DC battery is connected to the SUT, and that it is charged to atleast 90% for long run testing. Set the SUT power source to DC-only. Set the active power package on the SUT to Power Package 1 (Intel® ME in S0). Set the Intel® AMT WLAN link policy on the SUT to Link Policy 3 (Enabled in S0, Sx/AC), if the WLAN network interface is available. Ensure that the Host OS network device drivers are configured to not wake the SUT. This includes enabling ARP and/or NS Offload features, where available to prevent unexpected host wake events. 		
Procedure	<ol style="list-style-type: none"> Hibernate the SUT via the Host OS. Verify that the SUT is in S4/MeOff (CM-Off). Set the SUT Power Source to AC+DC. Verify that the SUT is in S4/MeOff (CM-Off). Briefly Press the Power Button on the SUT. Verify that the SUT is in S0/MeOn (CM0). Verify that the Host on the SUT is available. Verify that windows booted from hibernate i.e. value should be 0x02. "Run the following power shell command" Get-WinEvent-ProviderName Microsoft-Windows-Kernel-boot-MaxEvents 10 where-Object{\$_.message -like "The boot type*"} Verify that Intel® AMT on the SUT responds to version queries via all available network interfaces. <p>Repeat this procedure for the remaining number of cycles desired in the stress test.</p> <p>Check if there are any flash log. Success if there is no flash log.(Can test flash log by "MEInfo -FWSTS")</p>		
Pass Criteria	<p>Test passes, if Intel (R) CSME functions properly with no flash logs found i.e. stays MeOff, when AC Source attached in S4 State.</p> <p>Suggested Iterations: Mobile: >=2000, Portable AIO >= 750</p>		



10.27 PM_ST_25 - S0/CM0 to S5/CM-Off to S0/CM0 via AC Attach

ID	PM_ST_25	
Title	S0/CM0 to S5/CM-Off to S0/CM0 via AC-attach (AC+DC/PP1/LP3)	
Requirement	Mandatory	Exemptions <input checked="" type="checkbox"/> Non-Mobile (AC-only) systems
Method	Automated by Intel® PETS	
Objective	This test checks the SUT power flow from S0/CM0 to S5/CM-Off to S0/CM0 via AC-attach with the parameters outlined below.	
Configuration	<p>Intel® AMT should be provisioned via manual mode.</p> <p>If Deep S5 is supported on the SUT, confirm the following:</p> <ul style="list-style-type: none"> The SUT and/or BIOS are properly configured to permit Deep S5 entry. The correct Deep Sx policy is applied to the SUT profile in Intel® PETS. <p>This test assumes that either LAN-only, WLAN-only, or both LAN and WLAN network interfaces are available on the SUT.</p>	
Parameters	System Power Source	
	Power States	DC-only
		S0/MeOn (CM0)
		S5/MeOff (CM-Off)
		S0/MeOn (CM0)
		AC-attach in S5 state
	Intel® AMT	Power Package PP1 (Intel® ME on in S0)
		WLAN Link Policy LP3 (Enabled in S0, Sx/AC) where available
Setup	<ol style="list-style-type: none"> Set the SUT power source to AC+DC. Bring the SUT to the base state of S0/MeOn (CM0,CM0-PG), and confirm that the Host OS is available. Verify that a DC battery is connected to the SUT, and that it is charged to atleast 90% for long run testing. Set the SUT power source to DC-only. Set the active power package on the SUT to Power Package 1 (Intel® ME in S0). Set the Intel® AMT WLAN link policy on the SUT to Link Policy 3 (Enabled in S0, Sx/AC), if the WLAN network interface is available. Ensure that the Host OS network device drivers are configured to not wake the SUT. This includes enabling ARP and/or NS Offload features, where available to prevent unexpected host wake events. 	
Procedure	<ol style="list-style-type: none"> Shutdown the SUT via the Host OS. Verify that the SUT is in S5,Deep S5/MeOff (CM-Off). Set the SUT Power Source to AC+DC. Verify that the SUT is in S5,Deep S5/MeOff (CM-Off). Briefly Press the Power Button on the SUT. Verify that the SUT is in S0/MeOn (CM0). Verify that the Host on the SUT is available. Verify that Intel® AMT on the SUT responds to version queries via all available network interfaces. <p>Repeat this procedure for the remaining number of cycles desired in the stress test.</p> <p>Check if there are any flash log. Success if there is no flash log.(Can test flash log by "MEInfo -FWSTS")</p>	
Pass Criteria	<p>Test passes, if Intel® CSME functions properly with no flash logs found i.e. stays MOff, when AC Source attached in S5 State.</p> <p>Suggested Iterations: Mobile: >=2000, Portable AIO >= 750</p>	



10.28 PM_ST_26 - S0/CM0 to S3/CM-Off to S0/CM0 via AC Attach

ID	PM_ST_26		
Title	S0/CM0 to S3/CM-Off to S0/CM0 via AC-attach (AC+DC)		
Requirement	Mandatory	Exemptions	<input checked="" type="checkbox"/> Non-Mobile (AC-only) systems <input type="checkbox"/> Instant-go Platforms
Method	Automated by Intel® PETS		
Objective	This test checks the SUT power flow from S0/CM0 to S3/CM-Off to S0/CM0 via AC-attach with the parameters outlined below.		
Configuration	Intel® AMT should not be provisioned i.e. users will have to manually un-provision Intel (R) AMT if it is provisioned. This test assumes that either LAN-only, WLAN-only, or both LAN and WLAN network interfaces are available on the SUT.		
Parameters	System Power Source		DC-only
	Power States	Initial	S0/MeOn (CM0)
		Middle	S3/MeOff (CM-Off)
		Final	S0/MeOn (CM0)
		Trigger	AC-attach in S3 state
	Intel® AMT	Power Package	[Intel (R) AMT Not Provisioned]
		WLAN Link Policy	
Setup	<ol style="list-style-type: none"> Set the SUT power source to AC+DC. Bring the SUT to the base state of S0/MeOn (CM0,CM0-PG), and confirm that the Host OS is available. Verify that a DC battery is connected to the SUT, and that it is charged to atleast 90% for long run testing. Set the SUT power source to DC-only. Ensure Intel (R) AMT is not Provisioned Ensure that the Host OS network device drivers are configured to not wake the SUT. This includes enabling ARP and/or NS Offload features, where available to prevent unexpected host wake events. Record the Host OS last boot time on the SUT (to verify successful return from S3). 		
Procedure	<ol style="list-style-type: none"> Suspend the SUT via the Host OS. Verify that the SUT is in S3/MeOff (CM-Off). Set the SUT Power Source to AC+DC. Verify that the SUT is in S3/MeOff (CM-Off). Briefly Press the Power Button on the SUT. Verify that the SUT is in S0/MeOn (CM0). Verify that the Host on the SUT is available. Verify the Host OS last boot time on the SUT matches the boot time recorded before entry into S3. <p>Repeat this procedure for the remaining number of cycles desired in the stress test.</p> <p>Check if there are any flash log. Success if there is no flash log.(Can test flash log by "MEInfo -FWSTS")</p>		
Pass Criteria	Test passes, if Intel (R) CSME functions Properly with no flash logs found i.e. stays MOFF when AC Source attached in S3 State. Suggested Iterations: Mobile: >=2000, Portable AIO >= 750		



10.29 PM_ST_27 - S0/CM0 to S4/CM-Off to S0/CM0 via AC Attach

ID	PM_ST_27	
Title	S0/CM0 to S4/CM-Off to S0/CM0 via AC-attach (AC+DC)	
Requirement	Mandatory	Exemptions <input checked="" type="checkbox"/> Non-Mobile (AC-only) systems
Method	Automated by Intel® PETS	
Objective	This test checks the SUT power flow from S0/CM0 to S4/CM-Off to S0/CM0 via AC-attach with the parameters outlined below.	
Configuration	<p>Intel® AMT should not be provisioned. i.e. users will have to manually un-provision Intel® AMT, if it is provisioned.</p> <p>If Deep S4 and/or Deep S5 are supported on the SUT, confirm the following:</p> <ul style="list-style-type: none"> • If Deep S4 and/or Deep S5 are supported on the SUT, confirm the following: • The SUT and/or BIOS are properly configured to permit Deep S4/S5 entry. <p>This test assumes that either LAN-only, WLAN-only, or both LAN and WLAN network interfaces are available on the SUT.</p>	
Parameters	System Power Source	
	Power States	DC-only
		Initial
		Middle
		Final
		Trigger
	Intel® AMT	Power Package
		WLAN Link Policy
Setup	<ol style="list-style-type: none"> 1. Set the SUT power source to AC+DC. 2. Bring the SUT to the base state of S0/MeOn (CM0,CM0-PG), and confirm that the Host OS is available. 3. Verify that a DC battery is connected to the SUT, and that it is charged to atleast 90% for long run testing. 4. Set the SUT power source to DC-only. 5. Ensure Intel® AMT is not Provisioned 6. Ensure that the Host OS network device drivers are configured to not wake the SUT. This includes enabling ARP and/or NS Offload features, where available to prevent unexpected host wake events. 	
Procedure	<ol style="list-style-type: none"> 7. Hibernate the SUT via the Host OS. 8. Verify that the SUT is in S4/MeOff (CM-Off). 9. Set the SUT Power Source to AC+DC. 10. Verify that the SUT is in S4/MeOff (CM-Off). 11. Briefly Press the Power Button on the SUT. 12. Verify that the SUT is in S0/MeOn (CM0). 13. Verify that the Host on the SUT is available. 14. Verify that windows booted from hibernate i.e. value should be 0x02. "Run the following power shell command" Get-WinEvent-ProviderName Microsoft-Windows-Kernel-boot-MaxEvents 10 where-Object{\$_.message -like "The boot type*"} <p>Repeat this procedure for the remaining number of cycles desired in the stress test.</p> <p>Check if there are any flash log. Success if there is no flash log.(Can test flash log by "MEInfo -FWSTS")</p>	
Pass Criteria	<p>Test passes, if Intel® CSME functions Properly with no flash logs found i.e. stays MOff, when AC Source attached in S4 State.</p> <p>Suggested Iterations: Mobile: >=2000, Portable AIO >= 750</p>	



10.30 PM_ST_28 - S0/CM0 to S5/CM-Off to S0/CM0 via AC Attach

ID	PM_ST_28	
Title	S0/CM0 to S5/CM-Off to S0/CM0 via AC-attach (AC+DC)	
Requirement	Mandatory	Exemptions <input checked="" type="checkbox"/> Non-Mobile (AC-only) systems
Method	Automated by Intel® PETS	
Objective	This test checks the SUT power flow from S0/CM0 to S5/CM-Off to S0/CM0 via AC-attach with the parameters outlined below.	
Configuration	<p>Intel® AMT should not be provisioned. i.e. users will have to manually un-provision Intel® AMT if it is provisioned.</p> <p>If Deep S5 is supported on the SUT, confirm the following:</p> <ul style="list-style-type: none"> If Deep S5 is supported on the SUT, confirm the following: <ul style="list-style-type: none"> The SUT and/or BIOS are properly configured to permit Deep S5 entry. <p>This test assumes that either LAN-only, WLAN-only, or both LAN and WLAN network interfaces are available on the SUT.</p>	
Parameters	System Power Source	
	Power States	DC-only
		Initial S0/MeOn (CM0)
		Middle S5/MeOff (CM-Off)
		Final S0/MeOn (CM0)
		Trigger AC-attach in S5 state
Intel® AMT	Power Package	[Intel (R) AMT Not Provisioned]
	WLAN Link Policy	
Setup	<ol style="list-style-type: none"> Set the SUT power source to AC+DC. Bring the SUT to the base state of S0/MeOn (CM0,CM0-PG), and confirm that the Host OS is available. Verify that a DC battery is connected to the SUT, and that it is charged to atleast 90% for long run testing. Set the SUT power source to DC-only. Ensure Intel (R) AMT is not Provisioned Ensure that the Host OS network device drivers are configured to not wake the SUT. This includes enabling ARP and/or NS Offload features, where available to prevent unexpected host wake events. 	
Procedure	<ol style="list-style-type: none"> Shutdown the SUT via the Host OS. Verify that the SUT is in S5,Deep S5/MeOff (CM-Off). Set the SUT Power Source to AC+DC. Verify that the SUT is in S5,Deep S5/MeOff (CM-Off). Briefly Press the Power Button on the SUT. Verify that the SUT is in S0/MeOn (CM0). Verify that the Host on the SUT is available. <p>Repeat this procedure for the remaining number of cycles desired in the stress test.</p> <p>Check if there are any flash log. Success if there is no flash log.(Can test flash log by "MEInfo -FWSTS")</p>	
Pass Criteria	<p>Test passes, if Intel (R) CSME functions Properly with no flash logs found i.e. stays MOFF, when AC Source attached in S5 State.</p> <p>Suggested Iterations: Mobile: >=2000, Portable AIO >= 750</p>	



10.31 PM_ST_29 - S0/CM0 to S3/CM-Off to S0/CM0 via AC Detach

ID	PM_ST_29		
Title	S0/CM0 to S3/CM-Off to S0/CM0 via AC-detach (AC+DC/PP2/LP3)		
Requirement	Mandatory	Exemptions	<input checked="" type="checkbox"/> Non-Mobile (AC-only) systems Instant Go Platforms
Method	Automated by Intel® PETS		
Objective	This test checks the SUT power flow from S0/CM0 to S3/CM-Off to S0/CM0 via AC-detach with the parameters outlined below.		
Configuration	Intel® AMT should be provisioned via manual mode. This test assumes that either LAN-only, WLAN-only, or both LAN and WLAN network interfaces are available on the SUT.		
Parameters	System Power Source		DC-only
	Power States	Initial	S0/MeOn (CM0)
		Middle	S3/MeOff (CM-Off)
		Final	S0/MeOn (CM0)
		Trigger	AC-detach in S3 state
	Intel® AMT	Power Package	PP2 (Intel® ME on in S0, wake in Sx/AC)
		WLAN Link Policy	LP3 (Enabled in S0, Sx/AC) where available
Setup	<ol style="list-style-type: none"> Set the SUT power source to AC+DC. Bring the SUT to the base state of S0/MeOn (CM0,CM0-PG), and confirm that the Host OS is available. Set the active power package on the SUT to Power Package 2 (Intel® ME on in S0, wake in Sx/AC). Set the Intel® AMT WLAN link policy on the SUT to Link Policy 3 (Enabled in S0, Sx/AC), if the WLAN network interface is available. Ensure that the Host OS network device drivers are configured to not wake the SUT. This includes enabling ARP and/or NS Offload features, where available to prevent unexpected host wake events. Record the Host OS last boot time on the SUT (to verify successful return from S3). 		
Procedure	<ol style="list-style-type: none"> Suspend the SUT via the Host OS. Verify that the SUT is in S3/MeOn (CM3). Verify that a DC battery is connected to the SUT, and that it is charged to atleast 90% for long run testing. Set the SUT Power Source to DC Only. Verify that the SUT is in S3/MeOff (CM-Off). Set the SUT power source to AC+DC. Verify that the SUT is in S3/MeOn (CM3). Verify that Intel® AMT on the SUT responds to version queries via all available network interfaces. Briefly Press the Power Button on the SUT. Verify that the SUT is in S0/MeOn (CM0). Verify that the Host on the SUT is available. Verify the Host OS last boot time on the SUT matches the boot time recorded before entry into S3. Verify that Intel® AMT on the SUT responds to version queries via all available network interfaces. <p>Repeat this procedure for the remaining number of cycles desired in the stress test.</p> <p>Check if there are any flash log. Success if there is no flash log.(Can test flash log by "MEInfo -FWSTS")</p>		
Pass Criteria	<p>Test passes, if Intel® CSME functions Properly with no flash logs found i.e. become MOff, when AC Source detached in S3 State and becomes MeOn after AC Attached in S3 State.</p> <p>Suggested Iterations: Mobile: >=2000, Portable AIO >= 750</p>		



10.32 PM_ST_30 - S0/CM0 to S4/CM-Off to S0/CM0 via AC Detach

ID	PM_ST_30		
Title	S0/CM0 to S4/CM-Off to S0/CM0 via AC-detach (AC+DC/PP2/LP3)		
Requirement	Mandatory	Exemptions	<input checked="" type="checkbox"/> Non-Mobile (AC-only) systems
Method	Automated by Intel® PETS		
Objective	This test checks the SUT power flow from S0/CM0 to S4/CM-Off to S0/CM0 via AC-detach with the parameters outlined below.		
Configuration	<p>Intel® AMT should be provisioned via manual mode.</p> <p>If Deep S4 and/or Deep S5 are supported on the SUT, confirm the following:</p> <ul style="list-style-type: none"> The SUT and/or BIOS are properly configured to permit Deep S4/S5 entry. The correct Deep Sx policy is applied to the SUT profile in Intel® PETS. <p>This test assumes that either LAN-only, WLAN-only, or both LAN and WLAN network interfaces are available on the SUT.</p>		
Parameters	System Power Source		DC-only
	Power States	Initial	S0/MeOn (CM0)
		Middle	S4/MeOff (CM-Off)
		Final	S0/MeOn (CM0)
		Trigger	AC-detach in S4 state
	Intel® AMT	Power Package	PP2 (Intel® ME on in S0, wake in Sx/AC)
		WLAN Link Policy	LP3 (Enabled in S0, Sx/AC) where available
Setup	<ol style="list-style-type: none"> Set the SUT power source to AC+DC. Bring the SUT to the base state of S0/MeOn (CM0,CM0-PG), and confirm that the Host OS is available. Set the active power package on the SUT to Power Package 2 (Intel® ME on in S0, wake in Sx/AC). Set the Intel® AMT WLAN link policy on the SUT to Link Policy 3 (Enabled in S0, Sx/AC), if the WLAN network interface is available. Ensure that the Host OS network device drivers are configured to not wake the SUT. This includes enabling ARP and/or NS Offload features, where available to prevent unexpected host wake events. 		
Procedure	<ol style="list-style-type: none"> Hibernate the SUT via the Host OS. Verify that the SUT is in S4/M3 (CM3). Verify that a DC battery is connected to the SUT, and that it is charged to at least 90% for long run testing. Set the SUT Power Source to DC Only. Verify that the SUT is in S4/MeOff (CM-Off). Set the SUT power source to AC+DC. Verify that the SUT is in S4/M3 (CM3). Verify that Intel® AMT on the SUT responds to version queries via all available network interfaces. Briefly Press the Power Button on the SUT. Verify that the SUT is in S0/MeOn (CM0). Verify that the Host on the SUT is available. Verify that windows booted from hibernate i.e. value should be 0x02. "Run the following power shell command" Get-WinEvent-ProviderName Microsoft-Windows-Kernel-boot-MaxEvents 10 where-Object{\$_.message -like "The boot type*"} Verify that Intel® AMT on the SUT responds to version queries via all available network interfaces. <p>Repeat this procedure for the remaining number of cycles desired in the stress test.</p> <p>Check if there are any flash log. Success if there is no flash log.(Can test flash log by "MEInfo -FWSTS")</p>		
Pass Criteria	<p>Test passes, if Intel (R) CSME functions Properly with no flash logs found i.e. become MOFF, when AC Source detached in S4 State and becomes MeOn after AC Attached in S4 State.</p> <p>Suggested Iterations: Mobile: >=2000, Portable AIO >= 750</p>		



10.33 PM_ST_31 - S0/CM0 to S5/CM-Off to S0/CM0 via AC Detach

ID	PM_ST_31	
Title	S0/CM0 to S5/CM-Off to S0/CM0 via AC-detach (AC+DC/PP2/LP3)	
Requirement	Mandatory	Exemptions <input checked="" type="checkbox"/> Non-Mobile (AC-only) systems
Method	Automated by Intel® PETS	
Objective	This test checks the SUT power flow from S0/CM0 to S5/CM-Off to S0/CM0 via AC-detach with the parameters outlined below.	
Configuration	<p>Intel® AMT should be provisioned via manual mode.</p> <p>If Deep S5 is supported on the SUT, confirm the following:</p> <ul style="list-style-type: none"> The SUT and/or BIOS are properly configured to permit Deep S5 entry. The correct Deep Sx policy is applied to the SUT profile in Intel® PETS. <p>This test assumes that either LAN-only, WLAN-only, or both LAN and WLAN network interfaces are available on the SUT.</p>	
Parameters	System Power Source	
	Power States	DC-only
		S0/MeOn (CM0)
		S5, Deep S5/MeOff (CM-Off)
		S0/MeOn (CM0)
		AC-detach in S5 state
	Intel® AMT	
	Power Package	PP2 (Intel® ME on in S0, wake in Sx/AC)
	WLAN Link Policy	LP3 (Enabled in S0, Sx/AC) where available
Setup	<ol style="list-style-type: none"> Set the SUT power source to AC+DC. Bring the SUT to the base state of S0/MeOn (CM0,CM0-PG), and confirm that the Host OS is available. Set the active power package on the SUT to Power Package 2 (Intel® ME on in S0, wake in Sx/AC). Set the Intel® AMT WLAN link policy on the SUT to Link Policy 3 (Enabled in S0, Sx/AC), if the WLAN network interface is available. Ensure that the Host OS network device drivers are configured to not wake the SUT. This includes enabling ARP and/or NS Offload features, where available to prevent unexpected host wake events. 	
Procedure	<ol style="list-style-type: none"> Shutdown the SUT via the Host OS. Verify that the SUT is in S5/MeOn (CM3). Verify that a DC battery is connected to the SUT, and that it is charged to atleast 90% for long run testing. Set the SUT Power Source to DC Only. Verify that the SUT is in S5,Deep S5/MeOff (CM-Off). Set the SUT power source to AC+DC. Verify that the SUT is in S5/MeOn (CM3). Verify that Intel® AMT on the SUT responds to version queries via all available network interfaces. Briefly Press the Power Button on the SUT. Verify that the SUT is in S0/MeOn (CM0). Verify that the Host on the SUT is available. Verify that Intel® AMT on the SUT responds to version queries via all available network interfaces. <p>Repeat this procedure for the remaining number of cycles desired in the stress test.</p> <p>Check if there are any flash log. Success if there is no flash log.(Can test flash log by "MEInfo -FWSTS")</p>	
Pass Criteria	<p>Test passes, if Intel® CSME functions Properly with no flash logs found i.e. become MOff, when AC Source detached in S5 State and becomes MeOn after AC Attached in S5 State.</p> <p>Suggested Iterations: Mobile: >=2000, Portable AIO >= 750</p>	



10.34 PM_ST_32 - S0/CM0 to S3/CM-Off to S0/CM0 via AC Detach

ID	PM_ST_32		
Title	S0/CM0 to S3/CM-Off to S0/CM0 via AC-detach (AC+DC/PP1/LP3)		
Requirement	Mandatory	Exemptions	<input checked="" type="checkbox"/> Non-Mobile (AC-only) systems
Method	Automated by Intel® PETS		
Objective	This test checks the SUT power flow from S0/CM0 to S3/CM-Off to S0/CM0 via AC-detach with the parameters outlined below.		
Configuration	Intel® AMT should be provisioned via manual mode. This test assumes that either LAN-only, WLAN-only, or both LAN and WLAN network interfaces are available on the SUT.		
Parameters	System Power Source		DC-only
	Power States	Initial	S0/MeOn (CM0)
		Middle	S3/MeOff (CM-Off)
		Final	S0/MeOn (CM0)
		Trigger	AC-detach in S3 state
	Intel® AMT	Power Package	PP1 (Intel® ME on in S0)
		WLAN Link Policy	LP3 (Enabled in S0, Sx/AC) where available
Setup	<ol style="list-style-type: none"> Set the SUT power source to AC+DC. Bring the SUT to the base state of S0/MeOn (CM0,CM0-PG), and confirm that the Host OS is available. Set the active power package on the SUT to Power Package 1 (Intel® ME in S0). Set the Intel® AMT WLAN link policy on the SUT to Link Policy 3 (Enabled in S0, Sx/AC), if the WLAN network interface is available. Ensure that the Host OS network device drivers are configured to not wake the SUT. This includes enabling ARP and/or NS Offload features, where available to prevent unexpected host wake events. Record the Host OS last boot time on the SUT (to verify successful return from S3). 		
Procedure	<ol style="list-style-type: none"> Suspend the SUT via the Host OS. Verify that the SUT is in S3/MeOff (CM-Off). Verify that a DC battery is connected to the SUT, and that it is charged to atleast 90% for long run testing. Set the SUT Power Source to DC Only Verify that the SUT is in S3/MeOff (CM-Off). Set the SUT power source to AC+DC. Verify that the SUT is in S3/MeOff (CM-Off). Briefly Press the Power Button on the SUT. Verify that the SUT is in S0/MeOn (CM0). Verify that the Host on the SUT is available. Verify the Host OS last boot time on the SUT matches the boot time recorded before entry into S3. Verify that Intel® AMT on the SUT responds to version queries via all available network interfaces. <p>Repeat this procedure for the remaining number of cycles desired in the stress test.</p> <p>Check if there are any flash log. Success if there is no flash log.(Can test flash log by "MEInfo -FWSTS")</p>		
Pass Criteria	<p>Test passes, if Intel® CSME functions Properly become Me-Off, when AC Source detached in S3 State and becomes MeOn after AC Attached in S3 State with no flash logs found.</p> <p>Suggested Iterations: Mobile: >=2000, Portable AIO >= 750</p>		



10.35 PM_ST_33 - S0/CM0 to S4/CM-Off to S0/CM0 via AC Detach

ID	PM_ST_33	
Title	S0/CM0 to S4/CM-Off to S0/CM0 via AC-detach (AC+DC/PP1/LP3)	
Requirement	Mandatory	Exemptions <input checked="" type="checkbox"/> Non-Mobile (AC-only) systems
Method	Automated by Intel® PETS	
Objective	This test checks the SUT power flow from S0/CM0 to S4/CM-Off to S0/CM0 via AC-detach with the parameters outlined below.	
Configuration	<p>Intel® AMT should be provisioned via manual mode.</p> <p>If Deep S4 and/or Deep S5 are supported on the SUT, confirm the following:</p> <ul style="list-style-type: none"> The SUT and/or BIOS are properly configured to permit Deep S4/S5 entry. The correct Deep Sx policy is applied to the SUT profile in Intel® PETS. <p>This test assumes that either LAN-only, WLAN-only, or both LAN and WLAN network interfaces are available on the SUT.</p>	
Parameters	System Power Source	
	Power States	DC-only
		S0/MeOn (CM0)
		S4/MeOff (CM-Off)
		S0/MeOn (CM0)
		AC-detach in S3 state
	Intel® AMT	Power Package PP1 (Intel® ME on in S0)
		WLAN Link Policy LP3 (Enabled in S0, Sx/AC) where available
Setup	<ol style="list-style-type: none"> Set the SUT power source to AC+DC. Bring the SUT to the base state of S0/MeOn (CM0,CM0-PG), and confirm that the Host OS is available. Set the active power package on the SUT to Power Package 1 (Intel® ME in S0). Set the Intel® AMT WLAN link policy on the SUT to Link Policy 3 (Enabled in S0, Sx/AC), if the WLAN network interface is available. Ensure that the Host OS network device drivers are configured to not wake the SUT. This includes enabling ARP and/or NS Offload features, where available to prevent unexpected host wake events. 	
Procedure	<ol style="list-style-type: none"> Hibernate the SUT via the Host OS. Verify that the SUT is in S4/MeOff (CM-Off). Verify that a DC battery is connected to the SUT, and that it is charged to atleast 90% for long run testing. Set the SUT Power Source to DC Only. Verify that the SUT is in S4/MeOff (CM-Off). Set the SUT power source to AC+DC. Verify that the SUT is in S4/MeOff (CM-Off). Briefly Press the Power Button on the SUT. Verify that the SUT is in S0/MeOn (CM0). Verify that the Host on the SUT is available. Verify that windows booted from hibernate i.e. value should be 0x02. "Run the following power shell command" Get-WinEvent-ProviderName Microsoft-Windows-Kernel-boot-MaxEvents 10 where-Object{\$_.message -like "The boot type*"} Verify that Intel® AMT on the SUT responds to version queries via all available network interfaces. <p>Repeat this procedure for the remaining number of cycles desired in the stress test.</p> <p>Check if there are any flash log. Success if there is no flash log.(Can test flash log by "MEInfo -FWSTS")</p>	
Pass Criteria	<p>Test passes, if Intel® CSME functions Properly with no flash logs found i.e. become Me-Off, when AC Source detached in S4 State and becomes MeOn after AC Attached in S4 State.</p> <p>Suggested Iterations: Mobile: >=2000, Portable AIO >= 750</p>	



10.36 PM_ST_34 - S0/CM0 to S5/CM-Off to S0/CM0 via AC Detach

ID	PM_ST_34		
Title	S0/CM0 to S5/CM-Off to S0/CM0 via AC-detach (AC+DC/PP1/LP3)		
Requirement	Mandatory	Exemptions	<input checked="" type="checkbox"/> Non-Mobile (AC-only) systems
Method	Automated by Intel® PETS		
Objective	This test checks the SUT power flow from S0/CM0 to S5/CM-Off to S0/CM0 via AC-detach with the parameters outlined below.		
Configuration	<p>Intel® AMT should be provisioned via manual mode.</p> <p>If Deep S5 is supported on the SUT, confirm the following:</p> <ul style="list-style-type: none"> The SUT and/or BIOS are properly configured to permit Deep S5 entry. The correct Deep Sx policy is applied to the SUT profile in Intel® PETS. <p>This test assumes that either LAN-only, WLAN-only, or both LAN and WLAN network interfaces are available on the SUT.</p>		
Parameters	System Power Source		DC-only
	Power States	Initial	S0/MeOn (CM0)
		Middle	S5, Deep S5/MeOff (CM-Off)
		Final	S0/MeOn (CM0)
		Trigger	AC-detach in S5 state
	Intel® AMT	Power Package	PP1 (Intel® ME on in S0)
		WLAN Link Policy	LP3 (Enabled in S0, Sx/AC) where available
Setup	<ol style="list-style-type: none"> Set the SUT power source to AC+DC. Bring the SUT to the base state of S0/MeOn (CM0,CM0-PG), and confirm that the Host OS is available. Set the active power package on the SUT to Power Package 1 (Intel® ME in S0). Set the Intel® AMT WLAN link policy on the SUT to Link Policy 3 (Enabled in S0, Sx/AC), if the WLAN network interface is available. Ensure that the Host OS network device drivers are configured to not wake the SUT. This includes enabling ARP and/or NS Offload features, where available to prevent unexpected host wake events. 		
Procedure	<ol style="list-style-type: none"> Shutdown the SUT via the Host OS. Verify that the SUT is in S5,Deep S5/MeOff (CM-Off). Verify that a DC battery is connected to the SUT, and that it is charged to atleast 90% for long run testing. Set the SUT Power Source to DC Only. Verify that the SUT is in S5,Deep S5/MeOff (CM-Off). Set the SUT power source to AC+DC. Verify that the SUT is in S5,Deep S5/MeOff (CM-Off). Briefly Press the Power Button on the SUT. Verify that the SUT is in S0/MeOn (CM0). Verify that the Host on the SUT is available. Verify that Intel® AMT on the SUT responds to version queries via all available network interfaces. <p>Repeat this procedure for the remaining number of cycles desired in the stress test.</p> <p>Check if there are any flash log. Success if there is no flash log.(Can test flash log by "MEInfo -FWSTS")</p>		
Pass Criteria	<p>Test passes, if Intel® CSME functions Properly with no flash logs found i.e. become Me-Off, when AC Source detached in S5 State and becomes MeOn after AC Attached in S5 State.</p> <p>Suggested Iterations: Mobile: >=2000, Portable AIO >= 750</p>		

§ §



11 Intel® AMT Tests

This chapter covers Intel® AMT related features and technologies. Among those are the following features which require BIOS and/or system integration:

- System Management BIOS (SMBIOS) and Alert Standard Format (ASF)
- BIOS Boot Option Support and Hardware Inventory
- Platform Event Trap (PET) and Boot Audit Event (BAE)
- Remote Power Control
- Serial-Over-LAN (SOL) and Storage Redirection
- Keyboard, Video and Mouse (KVM) redirection
- Remote Access (Fast Call for Help)
- Settings, Storage, and Security Configuration
- Remote Secure Erase

Intel® AMT feature integration with other Intel technologies, third-party technologies, and extensions of Intel® AMT are also covered:

- Intel® Ready Mode Technology (Intel® RMT)
- Intel® ME Power Gating
- Modern Standby
- Microsoft Windows* InstantGo*
- Discrete Graphics and Switchable Graphics
- Remote Screen Blank (RSB) (extension of Intel® AMT)
- Host and dock TBT
- Discrete LAN

11.1 AMT Over Different LAN Solutions

AMT legacy LAN solution is based on integrated LAN as part of PCH, Starting Comet Lake, AMT supports additional two Intel® LAN options as described below:

- **Discrete LAN:** The new generation of LAN supports 2.5G as discrete LAN. vPro system supports discrete LAN in order to provide the customer AMT features and use the benefit of 2.5G LAN.
An additional use case that is supported in TGL timeframe is Remote Intel AMT Manageability over a discrete NIC connected on board (such as FXVL GbE). The interfaces to the NIC is MCTP over PCIe and MCTP over SMBus, same interfaces used for OOB communication with NIC in the dock.
In a configuration where the integrated GbE is enabled (phy on board) and FXVL is also on board, AMT supports OOB manageability only over the integrated GbE
- **TBT Dock with discrete LAN:** Thunderbolt dock is an on-desk docking station that connects to the host through a USB TypeC cable and enables the connection of multiple peripherals (monitors, keyboard, mouse, wired network (Ethernet), printer, back-up drives, speakers, headset, etc.) and provides charging power to a laptop that is connected to the dock. Thunderbolt™ vPro™ dock connected to a Thunderbolt™ vPro™ supported host does all the above but also enables the vPro capabilities of the system across the network connection on the Thunderbolt vPro docking station. The Thunderbolt™ vPro™ Dock is connected to the Thunderbolt



vPro enabled laptop through Type-C connector/cable using TBT technology. The system solution consists of a host implementing Thunderbolt vPro support connected directly to a stand-alone Thunderbolt docking device. The overall solution allows IT to remotely perform AMT management tasks on the PC connected to the dock – both In-Band and Out Of Band (OOB).

Active LAN Based on Dock Status

Dock Status	Active Connectivity Type
Dock connected	LAN in dock + Wireless
Dock disconnected	Platform Integrated or discrete LAN + Wireless

Active BUS Based on Power State Status

Power State	Active BUS	Comment
S0	PCI i or SMBUS	PCI e is active during TCPIP session.
S x	SMBUS	

11.2 Test System Power Model

Each test in this chapter contains a table describing the system configuration to which the test is applicable. Below is an example environment for a given test:

Form Factor	System Power Model	Intel® AMT Network Interface	LAN Type
<input checked="" type="checkbox"/> Desktop <input checked="" type="checkbox"/> Workstation <input checked="" type="checkbox"/> Mobile	<input checked="" type="checkbox"/> Standard <input checked="" type="checkbox"/> Modern Standby or InstantGo*	<input type="checkbox"/> LAN <input type="checkbox"/> Either Used <input type="checkbox"/> WLAN <input checked="" type="checkbox"/> Not Used	<input type="checkbox"/> Integrated LAN <input type="checkbox"/> Discrete LAN <input type="checkbox"/> TBT Dock LAN

Form Factor	System Power Model	Intel® AMT Network Interface
<input checked="" type="checkbox"/> Desktop <input checked="" type="checkbox"/> Workstation <input checked="" type="checkbox"/> Mobile	<input checked="" type="checkbox"/> Standard <input checked="" type="checkbox"/> Modern Standby or InstantGo*	<input type="checkbox"/> LAN <input type="checkbox"/> Integrated LAN <input type="checkbox"/> WLAN <input type="checkbox"/> Discrete LAN <input type="checkbox"/> Either Used <input type="checkbox"/> TBT Dock LAN <input checked="" type="checkbox"/> Not Used

Form Factor: Describes the kind of system for which the test is applicable. These tests cover feature availability for associated platform. Note that for Workstation form factors, the term 'Intel® AMT Server' may be also used for systems which support Intel® AMT and run a server operating system.

System Power Model: Describes which System Power Model the test is applicable under. A system with 'Standard' configuration follows traditional OS power model wherein sending the system to Sleep results in a S3 resting system state. Systems that support Modern Standby or Microsoft* Windows* InstantGo* move to S0 Low Power



Idle state upon being sent to Sleep. This is usually defined by feature support relative to the operating system in conjunction with BIOS and system device support, but may also be due to the nature of the operating system itself relative to the goals of the test.

Intel® AMT Network Interface: Describes the Intel® AMT networking interface used by the test, if any. 'LAN' and 'WLAN' indicate that the test is explicitly using the respective LAN and/or wireless LAN (WLAN) interface. 'Either Used' indicates that an Intel® AMT network interface is used during the test, but the test itself is not specifically define which specific interface is to be used. 'Not Used' indicates that the test procedure does not rely on the Intel® AMT network interface; even though Intel® Platform Enablement Test Suite (Intel® PETS) or other test methodology may require general networking access to the SUT. Note that not all Workstation and Intel® AMT Server designs may have Intel® AMT wireless LAN interface support.

LAN Type: Describe which LAN type is in used in the setup, it can be one of the three

- Integrated LAN: Integrated LAN which is part of PCH.
- Discrete LAN: Discrete LAN (a.k.a FXVL) in SUT.
- TBT Dock LAN: LAN which is located in TBT dock.

11.3 Test Coverage Summary

The following describes columns in the test coverage summary below. The **Test ID** is the reference identifier for the test in this document and any related tools which reference this document. The **Title** is the name of the test. The **Req.** (Requirement) column describes the requirement for test execution. The **Form Factor**, **OS** (Operating System), and **Net** (Intel® AMT Network Interface) indicate the applicable test system configuration (refer the [Section 11.2](#) for details). **How?** column describes the test methodology.

Req.: M = Mandatory, C = Conditional[†], and O = Optional

[†] Considered the same as Mandatory but with exemptions. Refer test for details.

Form Factor: D = Desktop, M = Mobile, and W = Workstation

Power Model: S = Standard, and M/I = Modern Standby or Microsoft* Windows* InstantGo* (refer above for details)

Net: L = LAN, W = WLAN, E = Either Used, and N = Not Used

LAN Type: **I** = Integrated LAN, **D** = Discrete LAN in SUT, **T** = TBT Dock LAN, **E** = Either Used, and **N** = Not Used

How?: A = Fully automated using Intel® PETS, I = Interactive using Intel® PETS automation, and M = Manual

Table 11-1. Intel® AMT Test Coverage Summary

Test ID	Title	Req.	Form Factor D M W	Power Model S M/I	Net	LAN Type	How?
BIOS Tables							
AMT_001	System Management BIOS (SMBIOS) Table Generation	M	☑ ☑ ☑	☑ ☑	N	N	I
AMT_002	Alert Standard Format (ASF) Table Generation	M	☑ ☑ ☑	☑ ☑	N	N	I
Boot Options, Platform Event Traps, Hardware Assets, and Boot Audit Entry							
AMT_010	BIOS Boot Option Read and Clear	M	☑ ☑ ☑	☑ ☑	E	I	I



Table 11-1. Intel® AMT Test Coverage Summary

Test ID	Title	Req.	Form Factor D M W	Power Model S M/I	Net	LAN Type	How?
AMT_011	Platform Event Trap (PET) Boot Progress Event Support	M	☑ ☑ ☑	☑ ☑	E	I	I
AMT_013	BIOS Hardware Asset Table Update	M	☑ ☑ ☑	☑ ☑	E	I	I
AMT_014	Boot Audit Entry (BAE) Platform Event Trap (PET) Support	M	☑ ☑ ☑	☑ ☑	E	I	A
AMT_015	Boot Audit Entry (BAE) Platform Event Trap (PET) Support with Alternate Boot Device	C	☑ ☑ ☑	☑ ☑	E	I	I
Remote Power Control							
AMT_020	Remote Power Control via Intel® AMT LAN Network Interface for Mobile Systems	M	☐ ☑ ☐	☑ ☑	L	I	A
AMT_021	Remote Power Control via Intel® AMT WLAN Network Interface for Mobile Systems	M	☐ ☑ ☐	☑ ☑	W	N	A
AMT_022	Remote Power Control via Intel® AMT LAN Network Interface for Non-Mobile Systems	M	☑ ☐ ☑	☑ ☐	L	I	A
AMT_023	Remote Power Control via Intel® AMT WLAN Network Interface for Non-Mobile Systems	M	☑ ☐ ☑	☑ ☐	W	N	A
AMT_024	Remote Power Control with S0 Low Power Idle via Intel® AMT LAN Network Interface	M	☑ ☑ ☐	☐ ☑	L	I	I
AMT_025	Remote Power Control with S0 Low Power Idle via Intel® AMT WLAN Network Interface	M	☑ ☑ ☐	☐ ☑	W	N	I
AMT_026	Remote Power Control via Intel® AMT WLAN Network Interface for Mobile Systems supporting Wake On Wireless LAN	C	☐ ☑ ☐	☑ ☐	W	N	A
AMT_027	Remote Power Control via Intel® AMT WLAN Network Interface for Non-Mobile Systems supporting Wake On Wireless LAN	C	☑ ☐ ☑	☑ ☐	W	N	A
AMT_028	Remote Power Control with Host OS interaction via Intel® AMT LAN Network Interface	M	☑ ☑ ☑	☑ ☑	L	I	A
AMT_029	Remote Power Control with Host OS interaction via Intel® AMT WLAN Network Interface	M	☑ ☑ ☑	☑ ☑	W	N	A
Serial-Over-LAN (SOL) and Storage Redirection							
AMT_030	Serial-Over-LAN (SOL) Redirection and BIOS Setup Boot Option over Intel® AMT LAN Network Interface	C	☑ ☑ ☑	☑ ☑	L	I	I
AMT_031	Serial-Over-LAN (SOL) Redirection and BIOS Setup Boot Option over Intel® AMT WLAN Network Interface	C	☑ ☑ ☑	☑ ☑	W	N	I
AMT_032	Serial-Over-LAN (SOL) and Storage Redirection over Intel® AMT LAN Network Interface	M	☑ ☑ ☑	☑ ☑	L	I	I
AMT_033	Serial-Over-LAN (SOL) and Storage Redirection over Intel® AMT WLAN Network Interface	M	☑ ☑ ☑	☑ ☑	W	N	I
AMT_034	Serial-Over-LAN (SOL) and Storage Redirection over Intel® AMT LAN Network Interface with User Consent Enabled	M	☑ ☑ ☑	☑ ☑	L	I	I



Table 11-1. Intel® AMT Test Coverage Summary

Test ID	Title	Req.	Form Factor D M W	Power Model S M/I	Net	LAN Type	How?
AMT_035	Serial-Over-LAN (SOL) and Storage Redirection over Intel® AMT WLAN Network Interface with User Consent Enabled	M	☑ ☑ ☑	☑ ☑	W	N	I
AMT_036	Serial-Over-LAN (SOL) and Storage Redirection with Secure Boot	C	☑ ☑ ☑	☑ ☑	E	I	I
AMT_037	Serial-Over-LAN (SOL) Character Interpretation	C	☑ ☑ ☑	☑ ☑	E	I	I
AMT_038	Serial-Over-LAN (SOL) Redirection during System Restart	O	☑ ☑ ☑	☑ ☑	E	I	I
Keyboard, Video, and Mouse (KVM) Redirection							
AMT_040	Keyboard, Video, and Mouse (KVM) Redirection and BIOS Setup Boot Option over Intel® AMT LAN Network Interface	C	☑ ☑ ☑	☑ ☑	L	I	I
AMT_041	Keyboard, Video, and Mouse (KVM) Redirection and BIOS Setup Boot Option over Intel® AMT WLAN Network Interface	C	☑ ☑ ☑	☑ ☑	W	N	I
AMT_042	Keyboard, Video, and Mouse (KVM) Redirection over Intel® AMT LAN Network Interface	C	☑ ☑ ☑	☑ ☑	L	I	I
AMT_043	Keyboard, Video, and Mouse (KVM) Redirection over Intel® AMT WLAN Network Interface	C	☑ ☑ ☑	☑ ☑	W	N	I
AMT_044	Keyboard, Video, and Mouse (KVM) Redirection over Intel® AMT LAN Network Interface with User Consent Enabled	C	☑ ☑ ☑	☑ ☑	L	I	I
AMT_045	Keyboard, Video, and Mouse (KVM) Redirection over Intel® AMT WLAN Network Interface with User Consent Enabled	C	☑ ☑ ☑	☑ ☑	W	N	I
AMT_046	Keyboard, Video, and Mouse (KVM) Redirection during Warm Reset over Intel® AMT LAN Network Interface	C	☑ ☑ ☑	☑ ☑	L	I	I
AMT_047	Keyboard, Video, and Mouse (KVM) Redirection during Warm Reset over Intel® AMT WLAN Network Interface	C	☑ ☑ ☑	☑ ☑	W	N	I
AMT_048	Keyboard, Video, and Mouse (KVM) Redirection with S0 Low Power Idle via Intel® AMT LAN Network Interface	C	☑ ☑ ☐	☐ ☑	L	I	I
AMT_049	Keyboard, Video, and Mouse (KVM) Redirection with S0 Low Power Idle via Intel® AMT WLAN Network Interface	C	☑ ☑ ☐	☐ ☑	W	N	I
AMT_050	Keyboard, Video, and Mouse (KVM) Redirection in Discrete Graphics Mode	C	☑ ☑ ☑	☑ ☑	E	I	I
AMT_051	Keyboard, Video, and Mouse (KVM) Redirection and Switchable Graphics	C	☑ ☑ ☑	☑ ☑	E	I	I
AMT_052	Keyboard, Video, and Mouse (KVM) with Serial-Over-LAN (SOL) and Storage Redirection	C	☑ ☑ ☑	☑ ☑	E	I	I
AMT_053	Keyboard, Video, and Mouse (KVM) and USB Port Availability Check	C	☑ ☑ ☑	☑ ☑	E	I	I
AMT_054	Keyboard, Video, and Mouse (KVM) with Remote Screen Blank (RSB) Support	C	☑ ☑ ☑	☑ ☑	E	I	I
AMT_055	Keyboard, Video, and Mouse (KVM) with S0 Low Power Idle and Intel® ME Power Gating	C	☑ ☑ ☐	☐ ☑	W	I	I

Table 11-1. Intel® AMT Test Coverage Summary

Test ID	Title	Req.	Form Factor D M W	Power Model S M/I	Net	LAN Type	How?
AMT_056	Keyboard, Video, and Mouse (KVM) Redirection over Intel® AMT WLAN Network Interface for Systems supporting Wake On Wireless LAN	C	☑ ☑ ☑	☑ ☐	W	N	I
AMT_059	Keyboard, Video, and Mouse (KVM) Redirection on Headless Configurations	C	☑ ☑ ☑	☑ ☑	E	I	I
Remote Access (Fast Call for Help)							
AMT_060	Fast Call for Help During System Boot	C	☑ ☑ ☑	☑ ☑	E	I	I
AMT_061	Fast Call for Help During System Boot (End-to-End)	O	☑ ☑ ☑	☑ ☑	L	I	M
Settings, Storage, and Security Configuration							
AMT_070	General Settings Information	O	☑ ☑ ☑	☑ ☑	E	I	I
AMT_071	Security Administration Realm Interface	O	☑ ☑ ☑	☑ ☑	E	I	A
AMT_073	Transport Layer Security (TLS) Authentication	O	☑ ☑ ☑	☑ ☑	E	I	I
AMT_074	Alarm Wake from S5	O	☑ ☑ ☑	☑ ☑	E	I	A
AMT_075	Alarm Wake from S4	O	☑ ☑ ☑	☑ ☑	E	I	A
AMT_076	Alarm Wake from S3	O	☑ ☑ ☑	☑ ☑	E	I	A
Remote Secure Erase							
AMT_080	Clear Remote Secure Erase Boot Option	C	☑ ☑ ☑	☑ ☑	E	I	I
AMT_081	Remote Secure Erase without Drive Authentication	C	☑ ☑ ☑	☑ ☑	E	I	I
AMT_082	Remote Secure Erase with Drive Authentication via Serial-Over-LAN (SOL) Redirection	C	☑ ☑ ☑	☑ ☑	E	I	I
AMT_083	Remote Secure Erase with Drive Authentication via Keyboard, Video, and Mouse (KVM) Redirection	C	☑ ☑ ☑	☑ ☑	E	I	I
AMT_084	Remote Secure Erase with Drive Authentication via Direct Password Input	C	☑ ☑ ☑	☑ ☑	E	I	I
AMT_085	Remote Secure Erase with Drive Authentication Failure via SOL Redirection	C	☑ ☑ ☑	☑ ☑	E	I	I
AMT_086	Remote Secure Erase with Drive Authentication Failure via Direct Password Input	C	☑ ☑ ☑	☑ ☑	E	I	I

11.3.1 Test Environment Setup

When completing tests within this chapter, especially those which send the system to a specific S-state (S3, S4, S5, Deep Sx, etc.), it is important to ensure that the network wake events are properly configured for each applicable device (LAN and/or WLAN).

If not properly configured, the system may wake from a given S-state unexpectedly during test execution as a result of various network traffic within the test environment, and cause the test to result in a *false failure*.

The following Host OS LAN/WLAN driver settings allow the network device to process specific network frames **without** waking the system where supported.

- ARP (Address Resolution Protocol) offload should be **enabled**
- NS (Neighbor Solicitation) offload should be **enabled**



The following Host OS LAN/WLAN driver settings allow the network device to wake the system, where supported, when specific network frames are received.

- Wake on Magic Packet should be **disabled**
- Wake on Pattern Match should be **disabled**
- Wake on Magic Packet from power off state should be **disabled**

Note:

The wording used for the Host OS driver settings above may vary, and in some cases may not be available depending on driver support or system configuration.

For Wake on Wireless LAN testing described in this chapter, the following Host OS WLAN driver settings should be used:

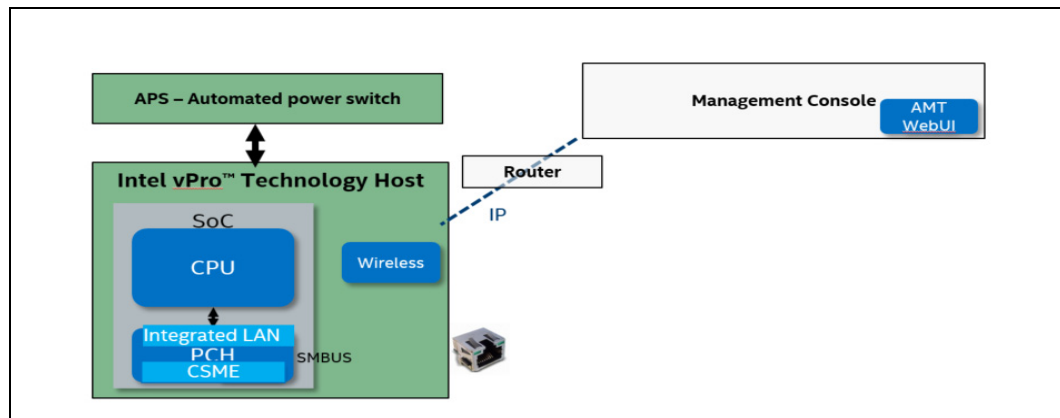
- Allow device to wake the computer should be **enabled**
- Allow the computer to turn off this device to save power should be **enabled**
- Allow only Magic Packet to wake the computer should be **disabled**
- Wake on Magic Packet should be **enabled**
- Wake on Pattern Match should be **enabled**

Beyond the guidance in this section, refer individual test setup information for details on specifically when to enable relevant wake functionality in the network device, as applicable to the test. In all other cases, the above settings should be applied by default.

11.3.1.1 Setup of AMT Over Integrated LAN or WLAN

AMT over discrete LAN system contains the following ingredients:

- Desktop \ Workstation platform which contains:
 - Intel WLAN
 - Intel Integrated LAN



11.3.2 Setup Environment Tests

The following tests are defined as Setup Environment Test (SET) tests. These are intended to confirm basic test environment configuration and should be run before any other automated test described in this chapter.



11.3.2.1 AMT Basic Connectivity with Integrated LAN and WLAN

ID:	Check Intel® AMT Connectivity			
Title:	Intel® AMT basic connectivity check in S0 with Host OS available.			
Requirement:	Optional			
System:	Form Factor <input checked="" type="checkbox"/> Desktop <input checked="" type="checkbox"/> Workstation <input checked="" type="checkbox"/> Mobile	System Power Model <input checked="" type="checkbox"/> Standard <input checked="" type="checkbox"/> Modern Standby or InstantGo*	Intel® AMT Network Interface <input checked="" type="checkbox"/> LAN <input type="checkbox"/> Either Used <input checked="" type="checkbox"/> WLAN <input type="checkbox"/> Not Used	LAN Type <input checked="" type="checkbox"/> Integrated LAN <input type="checkbox"/> Discrete LAN <input type="checkbox"/> TBT Dock LAN
Method:	Automated by Intel® PETS with test operator interaction			
Description:	Before any testing is to begin, it is critical to confirm network connectivity with Intel® AMT. This test assumes that either LAN-only, WLAN-only, or both LAN and WLAN network interfaces are available on the SUT.			
Objective:	Verify that the Management Console can communicate with Intel® AMT on the SUT.			
Setup:	The initial state of the SUT should be S0/MeOn with Host OS running. Intel® AMT should be provisioned via manual mode.			
Procedure:	<ol style="list-style-type: none"> Prompt the test operator to confirm that: <ol style="list-style-type: none"> The SUT supports Intel® AMT. The Host OS is booted on the SUT. Intel® AMT is provisioned on the SUT. The network connection to the Host OS on the SUT is confirmed for all available network interfaces. Query the Intel® ME firmware and confirm that Intel® AMT is available. Verify on the SUT that: <ol style="list-style-type: none"> The Intel® MEI driver is installed. The Local Manageability Service (LMS) is installed and running. Check on the SUT that the Intel® Management and Security Status (Intel® MSS) is installed and issue a warning otherwise (do not fail the test). Confirm for the following configuration information provided to Intel® PETS that: <ol style="list-style-type: none"> The administrator password for Intel® AMT is of a valid length. The IP address used to connect with Intel® AMT is valid. If the WLAN network interface is available: <ol style="list-style-type: none"> Query the Intel® ME firmware and verify there is no wireless micro-code mismatch. Verify that the Host OS WLAN profile and WLAN profile configured in Intel® AMT have the same Network Authentication and Encryption method settings applied. Verify that Intel® AMT on the SUT responds to version queries via all available network interfaces. 			
Pass Criteria:	The test passes if all the steps above pass without failure.			

ID:	Check Intel® AMT Feature Support			
Title:	Intel® AMT basic feature support check in S0 with Host OS available.			
Requirement:	Optional			
System:	Form Factor <input checked="" type="checkbox"/> Desktop <input checked="" type="checkbox"/> Workstation <input checked="" type="checkbox"/> Mobile	System Power Model <input checked="" type="checkbox"/> Standard <input checked="" type="checkbox"/> Modern Standby or InstantGo*	Intel® AMT Network Interface <input checked="" type="checkbox"/> LAN <input type="checkbox"/> Either Used <input checked="" type="checkbox"/> WLAN <input type="checkbox"/> Not Used	LAN Type <input checked="" type="checkbox"/> Integrated LAN <input type="checkbox"/> Discrete LAN <input type="checkbox"/> TBT Dock LAN
Method:	Automated by Intel® PETS			
Description:	Before any testing is to begin, it is critical to confirm feature configuration check with Intel® AMT. This test assumes that either LAN-only, WLAN-only, or both LAN and WLAN network interfaces are available on the SUT.			
Objective:	Verify that the Intel® AMT on the SUT is properly configured to enable feature integration testing.			
Setup:	The initial state of the SUT should be S0/MeOn with Host OS running. Intel® AMT should be provisioned via manual mode.			



ID:	Check Intel® AMT Feature Support
Procedure:	<ol style="list-style-type: none"> 1. Read the platform UUID and confirm that it is not all zero. 2. Query Intel® AMT and confirm that KVM support is enabled. 3. Query Intel® AMT and confirm that KVM is enabled in Intel® MEBX. 4. Verify that the Intel® AMT Serial-Over-LAN (SOL) device is available in the Host OS. 5. Verify that the Intel® AMT SOL and Storage Redirection features are enabled in Intel® MEBX by checking if their interface state can be enabled. 6. Verify basic Windows Management Instrumentation (WMI) support is available from Intel® AMT on the SUT by querying the <code>\$\$OsAdmin</code> account.
Pass Criteria:	The test passes if all the steps above pass without failure.

11.4 BIOS Tables

The section serves as a checklist for the environment setup and testing of BIOS tables.

11.4.1 Test Environment

The System Under Test (SUT) is to be configured with Intel® AMT set in manual provisioning mode with static IP address or DHCP. The management console may be a laptop or a desktop with a version of Microsoft Windows* supported by Intel® PETS, and the SUT should have a version of Microsoft Windows* supported by Intel® PETS as well. The test network is comprised of a hub/switch and network cables. The SUT should have only one system drive attached.

Tools for Testing:

- Intel® PETS: The latest version of the tool from the Intel® CSME Compliancy and Debug kit release. Refer the Intel® PETS User Guide for exact instructions on how to load and setup the Intel® PETS software.
- Intel® Automated Power Switch (Intel® APS): The SUT should be connected to an Intel® APS 3 unit. In case an Intel® APS 3 is not available, select the Manual configuration in the Intel® PETS SUT profile configuration menu.
- Intel® PETS Local Agent: The local agent must be installed on the SUT.

11.4.2 SMBIOS Table Generation

ID:	AMT_001			
Title:	System Management BIOS (SMBIOS) Table Generation			
Requirement:	Mandatory			
System:	Form Factor	System Power Model	Intel® AMT Network Interface	LAN Type
	<input checked="" type="checkbox"/> Desktop <input checked="" type="checkbox"/> Workstation <input checked="" type="checkbox"/> Mobile	<input checked="" type="checkbox"/> Standard <input checked="" type="checkbox"/> Modern Standby or InstantGo*	<input type="checkbox"/> LAN <input type="checkbox"/> Either Used <input type="checkbox"/> WLAN <input checked="" type="checkbox"/> Not Used	<input type="checkbox"/> Integrated LAN <input type="checkbox"/> Discrete LAN <input type="checkbox"/> TBT Dock LAN
Method:	Automated by Intel® PETS with test operator interaction			

ID:	AMT_001
Description:	<p>During POST, the BIOS creates several tables used by Intel® AMT. The BIOS communicates these tables to Intel® ME for storage.</p> <p>There are two aspects to this requirement:</p> <ol style="list-style-type: none"> 1. The tables exist and are formatted correctly within the SMBIOS Type Structures Table. 2. Verify that the data is being transferred correctly to the Intel® ME. <p>These tables include critical data used during Intel® AMT operation along with the following:</p> <ul style="list-style-type: none"> • Type 0 - BIOS Information • Type 1 - System Information • Type 2 - Baseboard (or Module) Information • Type 3 - System Enclosure or Chassis • Type 4 - Processor Information • Type 17 - Memory Device • Type 18 - Memory Error Information (Optional) • Type 19 - Memory Array Mapped Address • Type 22 - Portable Battery (Optional) • Type 27 - Cooling Device (Optional) • Type 130 - Intel® AMT Specific • Type 131 - Intel® Management Engine Platform
Objective:	Verify that the BIOS has created the required table data and communicated data to Intel® ME for storage.
Setup:	The initial state of the SUT should be S0/MeOn with Host OS running. Intel® AMT should be provisioned via manual mode.
Procedure:	<ol style="list-style-type: none"> 1. Extract the following SMBIOS Structures Table locally from the SUT, and display in textual format the following parsed structures within the SMBIOS Table: <ul style="list-style-type: none"> • BIOS Information • System Information • Baseboard (or Module) Information • System Enclosure or Chassis • Processor Information • Memory Device • Memory Error Information (Optional) • Memory Array Mapped Address • Portable Battery (Optional) • Cooling Device (Optional) • Intel® AMT Specific • Intel® Management Engine Platform <p>NOTE: For tables defined by Intel, only those with a length matching specification is displayed. Those which are not aligned to Intel specification should not be displayed.</p> <ol style="list-style-type: none"> 2. Request the test operator to review the tables and to verify that: <ol style="list-style-type: none"> i. all of the expected tables listed are included ii. all of the tables are formatted correctly
Procedure: (continued)	<ol style="list-style-type: none"> 3. Verify that the following tables are present with a length aligned to specification: <ul style="list-style-type: none"> • Type 0 – BIOS Information • Type 1 – System Information • Type 2 – Baseboard (or Module) Information • Type 3 – System Enclosure or Chassis • Type 4 – Processor • Type 17 – Memory Device • Type 19 – Memory Array Mapped Address 4. Verify fixed data in the SMBIOS Type 130 Intel® AMT Specific table. 5. Display configurable data in SMBIOS Type 130 Intel® AMT Specific table and request the test operator to confirm that it is correct 6. If Table SMBIOS Type 22 Portable Battery or SMBIOS Type 27 Cooling Device are available, display them to the test operator, and request them to confirm that they are correct. 7. Open a remote connection to the SUT and display the information exposed by means of the Hardware Asset interface, and request the user to confirm that the information is correct. This confirm that Asset Information is being generated and reported to Intel® ME for storage.
Pass Criteria:	The test passes if all the tables are correctly displayed and show correct information.
References:	For details on Type 130 and Type 131 tables, refer the <i>Intel® ME BIOS Specification</i> .



11.4.3 ASF Table Generation

ID:	AMT_002			
Title:	Alert Standard Format (ASF) Table Generation			
Requirement:	Mandatory			
System:	Form Factor <input checked="" type="checkbox"/> Desktop <input checked="" type="checkbox"/> Workstation <input checked="" type="checkbox"/> Mobile	System Power Model <input checked="" type="checkbox"/> Standard <input checked="" type="checkbox"/> Modern Standby or InstantGo*	Intel® AMT Network Interface <input type="checkbox"/> LAN <input type="checkbox"/> Either Used <input type="checkbox"/> WLAN <input checked="" type="checkbox"/> Not Used	LAN Type <input type="checkbox"/> Integrated LAN <input type="checkbox"/> Discrete LAN <input type="checkbox"/> TBT Dock LAN
Method:	Automated by Intel® PETS with test operator interaction			
Description:	An Intel® AMT compliant BIOS must generate the following ASF tables and send this information to the Intel® ME firmware: <ul style="list-style-type: none"> • ASF! Description Table • ASF_INFO • ASF_ALRT • ASF_RCTL • ASF_RMCP • ASF_ADDR 			
Objective:	Verify that BIOS creates the various ASF! Table Structures required for Intel® AMT functionality. The structures contain the information required by Intel® AMT for remote control, sensor polling, and boot options support.			
Setup:	The initial state of the SUT should be S0/MeOn with Host OS running. Intel® AMT should be provisioned via manual mode.			
Procedure:	<ol style="list-style-type: none"> 1. Extract the ASF! Tables locally from the SUT. 2. Ask the test operator if the SUT supports a watchdog timer and based on the response, verify that the Minimum Watchdog Reset value in ASF_INFO is 0 if not supported, and some other value if it is supported. 3. Display the System ID from the ASF tables, and request the test operator to confirm that it is valid (value is OEM specific). 4. Display the IANA Manufacturer ID from the ASF tables, and request the test operator to confirm that it is valid (value is OEM specific). 5. Ask the test operator if sensors are supported. If yes, display all the sensors, and ask the test operator to confirm that they are correct. 6. Verify that the ASF_RCTL structure contains the following remote operation command/data pairings: <ul style="list-style-type: none"> • 00h/03h - System reset • 00h/02h - System power off • 00h/01h - System power on • 00h/04h - System power cycle reset 7. Verify that the RMCP Boot Options Capabilities Bit Mask from ASF_RMCP table data: <ul style="list-style-type: none"> • Fields 16-31 must be 0x0. • Fields 7-10 must be 0x0. • Fields 3-4 must be 0x0. 			
Procedure: (continued)	<ol style="list-style-type: none"> 8. Display all the Boot Options Capabilities from the RMCP Boot Options Capabilities Bit Mask in the ASF_RMCP table data with their supported/non-supported status, and ask the test operator to confirm that they are correct. 9. Verify that the RMCP Special Commands Bit Mask in the ASF_RMCP table data: <ul style="list-style-type: none"> • Fields 13-15 must be 0x0. • Fields 0-7 must be 0x0. 10. Display the RMCP Special Commands from the RMCP Special Commands Bit Mask in the ASF_RMCP table data with their supported/non supported status, and ask the test operator to confirm that they are correct. 11. Display the RMCP IANA Enterprise ID in the ASF_RMCP table data, and ask the test operator to confirm that it is correct. 12. Display the ASF_ADDR table data, and ask the test operator to confirm that the it is correct. 			

ID:	AMT_002
Procedure: (continued)	<p>13. Extract the following remote control capabilities from both the BIOS and via the Intel® AMT network interface, and verify that they are identical:</p> <p>Boot Options (System Firmware) Capabilities</p> <ul style="list-style-type: none"> · Firmware Verbosity/Screen Blank · Power Button Lock · Reset Button Lock · Lock Keyboard · Sleep Button Lock · User Password Bypass · Forced Progress Events · Firmware Verbosity/Verbose · Firmware Verbosity/Quiet · Configuration Data Reset <p>Special Commands</p> <ul style="list-style-type: none"> · Force PXE Boot · Force Hard-drive Boot · Force Hard-drive Safe-mode Boot · Force Diagnostic Boot · Force CD/DVD Boot <p>System Capabilities</p> <ul style="list-style-type: none"> · Power-Cycle Reset · Power-Down only · Power-Up · Reset <p>Recommended Step (not included with any Intel-provided tool): Use an SMBus sniffer to verify sensor polling is done according to the sensor in ASF_ALRT table.</p>
Pass Criteria:	The test passes if the Intel® PETS and the test operator are able to verify that all the tables have valid data.
References:	The structure and description of the ASF tables can be found at the DMTF web site in document DSP0136 at http://dmtof.org .

11.5 Boot Options, Platform Event Traps, Hardware Assets, and Boot Audit Entry

The section serves as a checklist for the environment setup and covers integration testing of BIOS boot options, Platform Event Traps (PET), hardware asset push, and Boot Audit Entry (BAE) event features in Intel® AMT.

11.5.1 Test Environment

The System Under Test (SUT) is to be configured with Intel® AMT set in manual provisioning mode with static IP address or DHCP. The management console may be a laptop or a desktop with a version of Microsoft Windows* supported by Intel® PETS, and the SUT should have a version of Microsoft Windows* supported by Intel® PETS as well. The test network is comprised of a hub/switch and network cables. The SUT should have only one system drive attached.

Tools for testing:

- Intel® PETS: The latest version of the tool from the Intel® CSME Compliancy and Debug kit release. Refer the Intel® PETS User Guide for exact instructions on how to load and setup the Intel® PETS software.
- Intel® Automated Power Switch (Intel® APS): The SUT should be connected to an Intel® APS 3 unit. In case an Intel® APS 3 is not available, select the Manual configuration in the Intel® PETS SUT profile configuration menu.
- Intel® PETS Local Agent: The local agent must be installed on the SUT.
- Bootable CD/DVD with OS for applicable tests.



Where applicable, the wireless LAN interface on Intel® AMT must be on a different network/subnet than the wired LAN interface. For details on how to enter the network interface details into Intel® PETS, consult the Intel® PETS User Guide.

11.5.2 BIOS Boot Option Read and Clear

ID:	AMT_010																												
Title:	BIOS Boot Option Read and Clear																												
Requirement:	Mandatory																												
System:	<table border="1"> <thead> <tr> <th colspan="2">Form Factor</th><th>System Power Model</th><th colspan="2">Intel® AMT Network Interface</th><th>LAN Type</th></tr> </thead> <tbody> <tr> <td><input checked="" type="checkbox"/> Desktop</td><td><input checked="" type="checkbox"/> Workstation</td><td><input checked="" type="checkbox"/> Standard</td><td><input type="checkbox"/> LAN</td><td><input checked="" type="checkbox"/> Either Used</td><td><input checked="" type="checkbox"/> Integrated LAN</td></tr> <tr> <td><input checked="" type="checkbox"/> Mobile</td><td></td><td><input checked="" type="checkbox"/> Modern Standby or InstantGo*</td><td><input type="checkbox"/> WLAN</td><td><input type="checkbox"/> Not Used</td><td><input type="checkbox"/> Discrete LAN</td></tr> <tr> <td></td><td></td><td></td><td></td><td></td><td><input type="checkbox"/> TBT Dock LAN</td></tr> </tbody> </table>					Form Factor		System Power Model	Intel® AMT Network Interface		LAN Type	<input checked="" type="checkbox"/> Desktop	<input checked="" type="checkbox"/> Workstation	<input checked="" type="checkbox"/> Standard	<input type="checkbox"/> LAN	<input checked="" type="checkbox"/> Either Used	<input checked="" type="checkbox"/> Integrated LAN	<input checked="" type="checkbox"/> Mobile		<input checked="" type="checkbox"/> Modern Standby or InstantGo*	<input type="checkbox"/> WLAN	<input type="checkbox"/> Not Used	<input type="checkbox"/> Discrete LAN						<input type="checkbox"/> TBT Dock LAN
Form Factor		System Power Model	Intel® AMT Network Interface		LAN Type																								
<input checked="" type="checkbox"/> Desktop	<input checked="" type="checkbox"/> Workstation	<input checked="" type="checkbox"/> Standard	<input type="checkbox"/> LAN	<input checked="" type="checkbox"/> Either Used	<input checked="" type="checkbox"/> Integrated LAN																								
<input checked="" type="checkbox"/> Mobile		<input checked="" type="checkbox"/> Modern Standby or InstantGo*	<input type="checkbox"/> WLAN	<input type="checkbox"/> Not Used	<input type="checkbox"/> Discrete LAN																								
					<input type="checkbox"/> TBT Dock LAN																								
Method:	Automated by Intel® PETS with test operator interaction																												
Description:	When the BIOS executes (before OS boot) the BIOS must read the boot options from the Intel® ME by means of the Get Boot Options command. This test verifies that the BIOS reads and executes the sent options, and also clears the options for next boot.																												
Objective:	<p>Verify that the BIOS reads and executes boot options as specified by the remote console and then clears the options for next boot.</p> <p>Intel® AMT enables remote management of the platform, including providing capabilities to receive the boot options sent from a management console. Once the BIOS has successfully read the boot options, the BIOS must then reset/clear the sent boot options on the local Intel® AMT platform so as to return it to the default state for the next boot.</p>																												
Setup:	The initial state of the SUT should be S0/MeOn with Host OS running. Intel® AMT should be provisioned via manual mode. There should be only one bootable system drive attached to the SUT. Where attached, remove any additional bootable system drives from the SUT before testing.																												
Procedure:	<ol style="list-style-type: none"> Set the active power package on the SUT to Power Package 2 (Intel® ME on in S0, wake in Sx/AC). Set the Intel® AMT WLAN link policy on the SUT to Link Policy 3 (Enabled in S0, Sx/AC), if the WLAN network interface is used. Obtain the boot options available from the SUT via Intel® AMT. Some systems may not support all possible boot options like force boot to CD/DVD device. Display the boot options supported by the SUT and ask the test operator to select a special command, plus one or more system boot capabilities. <p>Special Commands:</p> <ul style="list-style-type: none"> No Operation Force PXE Boot Force Hard Drive Boot Force Diagnostic Boot BIOS Pause <p>System Boot Capabilities:</p> <ul style="list-style-type: none"> Lock Power Button Lock Reset Button Lock Keyboard Lock Sleep Button Safe Mode User Password Bypass Configuration Data Reset Firmware Verbosity (System Default, Quiet, Verbose, and Screen Blank) <p>Note: Boot options related to KVM and Storage Redirection, the boot Progress Events boot capability, the Force CD/DVD Boot capability, and the BIOS Setup boot capability would not be provided to the test operator. Testing related to those features are covered by other tests.</p>																												



ID:	AMT_010
Procedure: (continued)	5. Use Intel® AMT to apply the boot options, as specified by the test operator, to the SUT for the next boot. 6. Gracefully shutdown to S5/MeOn the SUT via the Host OS and then wait 10 seconds . 7. Perform a Remote Power-Up of the SUT via Intel® AMT. 8. Wait for the SUT to return to S0/MeOn. Note that depending on the boot option selected, it should not be possible for Intel® PETS to programmatically confirm the Host OS or final S0 system operational state (example: Force PXE Boot). 9. Request the test operator to verify that the boot was performed with selected boot options. 10. Request the test operator to gracefully shutdown the SUT. Note that depending on the boot option selected, it should not be possible for Intel® PETS to programmatically shut down the system gracefully in all cases. 11. Wait for the SUT to move to S5/MeOn. 12. Inform the test operator that a system boot is performed by Intel® PETS with no special options. 13. Perform a Remote Power-Up of the SUT via Intel® AMT. 14. Wait for the SUT to return to S0/MeOn with the Host OS running. 15. Request the test operator to verify that the boot, without any boot options applied, was performed correctly. 16. Display instructions describing to re-run this test as many times as is needed to cover all remaining untested boot options available on the SUT.
Pass Criteria:	The test passes if each of the specified boot options passes, and if the subsequent boot shows that the option was cleared.
References:	For details on the BIOS boot options, refer the <i>Intel® ME BIOS Specification</i> .

11.5.3 PET Boot Progress Event Support

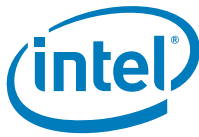
ID:	AMT_011			
Title:	Platform Event Trap (PET) Boot Progress Event Support			
Requirement:	Mandatory			
System:	Form Factor <input checked="" type="checkbox"/> Desktop <input checked="" type="checkbox"/> Workstation <input checked="" type="checkbox"/> Mobile	System Power Model <input checked="" type="checkbox"/> Standard <input checked="" type="checkbox"/> Modern Standby or InstantGo*	Intel® AMT Network Interface <input type="checkbox"/> LAN <input checked="" type="checkbox"/> Either Used <input type="checkbox"/> WLAN <input type="checkbox"/> Not Used	LAN Type <input checked="" type="checkbox"/> Integrated LAN <input type="checkbox"/> Discrete LAN <input type="checkbox"/> TBT Dock LAN
Method:	Automated by Intel® PETS with test operator interaction			
Description:	When the boot options sent remotely indicate FORCE PROGRESS EVENTS the BIOS sends at least one of the following progress messages as a PET event: <ul style="list-style-type: none"> • BIOS Present • MemInit • HddInit • BspInit • APInit • PciResConfig • VideoInit • KbcInit • OSBoot 			
Objective:	Verify that the defined boot progress message PET events are being sent by the BIOS under the appropriate conditions.			
Setup:	The initial state of the SUT should be S0/MeOn with Host OS running. Intel® AMT should be provisioned via manual mode.			



ID:	AMT_011
Procedure:	<ol style="list-style-type: none"> 1. Set the active power package on the SUT to Power Package 2 (Intel® ME on in S0, wake in Sx/AC). 2. Set the Intel® AMT WLAN link policy on the SUT to Link Policy 3 (Enabled in S0, Sx/AC), if the WLAN network interface is used. 3. Clear the Intel® AMT Event Manager log on the SUT. 4. Use Intel® AMT to set the FORCE PROGRESS EVENTS boot option on the SUT for the next boot. 5. Gracefully shutdown to S5/MeOn the SUT via the Host OS and then wait 10 seconds. 6. Perform a Remote Power-Up of the SUT via Intel® AMT. 7. Wait for the SUT to return to S0/MeOn with the Host OS running. 8. Dump the Event Manager log to a local file on the SUT. 9. Transfer the Event Manager log file from the SUT to the management console. 10. On the management console, parse the Event Manager log to verify that at least one boot progress message PET alert was sent. 11. Display from the Event Manager log all of the PET alerts received during the boot. 12. Request the test operator to inspect and confirm all of the PET alerts logged are accurate.
Limitations:	<p>Intel provides no direct test for the other PET events and error/warning messages that the BIOS might have in-full or in-part. As such, the following recommendation is provided:</p> <ol style="list-style-type: none"> 1. Test for PET alerts on all tests available for the SUT. 2. Conduct a BIOS code review for all PET events not tested. <p>It is up to the BIOS vendor to verify implementation of retransmission mechanism per the Intel® ME BIOS Specification recommendations.</p>
Pass Criteria:	The test passes when at least one of the progress message PET alerts are received, and code review shows that messages is sent in cases not tested.
References:	For details on boot progress PET events, refer the <i>Intel® ME BIOS Specification</i> .

11.5.4 BIOS Hardware Asset Table Update

ID:	AMT_013					
Title:	BIOS Hardware Asset Table Update					
Requirement:	Mandatory					
System:	Form Factor		System Power Model	Intel® AMT Network Interface		LAN Type
	<input checked="" type="checkbox"/> Desktop <input checked="" type="checkbox"/> Mobile	<input checked="" type="checkbox"/> Workstation	<input checked="" type="checkbox"/> Standard <input checked="" type="checkbox"/> Modern Standby or InstantGo*	<input type="checkbox"/> LAN <input type="checkbox"/> WLAN	<input checked="" type="checkbox"/> Either Used <input type="checkbox"/> Not Used	<input checked="" type="checkbox"/> Integrated LAN <input type="checkbox"/> Discrete LAN <input type="checkbox"/> TBT Dock LAN
Method:	Automated by Intel® PETS with test operator interaction					
Description:	An Intel® AMT compliant BIOS implements appropriate Hardware Asset management.					
Objective:	Verify that the BIOS reports add-on devices installed in the system.					
Setup:	The initial state of the SUT should be S0/MeOn with Host OS running. Intel® AMT should be provisioned via manual mode. Before running this test, ensure that Storage Redirection is enabled in the Intel® MEBX.					



ID:	AMT_013
Procedure:	<ol style="list-style-type: none">1. Set the active power package on the SUT to Power Package 2 (Intel® ME on in S0, wake in Sx/AC).2. Set the Intel® AMT WLAN link policy on the SUT to Link Policy 3 (Enabled in S0, Sx/AC), if the WLAN network interface is used.3. Retrieve the Hardware Asset information from the SUT via Intel® AMT.4. Ensure the TCP maximum data retransmission setting defined in the SUT profile is applied to both a) the management console, and b) the SUT via Intel® AMT, if the WLAN network interface is used. If the configuration on the management console is not already aligned to the SUT profile setting, the network stack on the management console need to be reset; leading to potential network connectivity loss for other applications on the system. Before synchronizing the setting on the management console, provide a warning to the test operator, with the option to proceed or cancel, indicating the TCP maximum data retransmission network setting is about to be changed and that it may be necessary to re-establish network connectivity for any other applications running on the management console. If the test operator chooses to cancel, the test step is marked as failed.5. Ensure the Intel® AMT redirection ports are enabled on the SUT.6. Cancel any existing Intel® AMT user consent session which may be active on the SUT.7. Ensure the Intel® AMT user consent opt-in setting is disabled on the SUT.8. Use Intel® AMT to set the boot options to Force Storage Redirection Boot on the SUT for the next boot.9. Inform the test operator that a system boot is performed by Intel® PETS requesting that the BIOS boot to a redirected ISO OS image (without Serial-Over-LAN).10. Gracefully shutdown to S5/MeOn the SUT via the Host OS and then wait 10 seconds.11. Open a Storage Redirection session with the SUT via Intel® AMT using an ISO OS image on the management console.12. Perform a Remote Power-Up of the SUT via Intel® AMT.13. Wait for the SUT to return to S0/MeOn.14. Retrieve the Hardware Asset information from the SUT via Intel® AMT.15. Close the Storage Redirection session with the SUT via Intel® AMT.16. Perform a Remote Power-Down of the SUT via Intel® AMT.
Procedure: (continued)	<ol style="list-style-type: none">17. Compare the Hardware Asset information collected at step 3 with the information collected at step 11, and confirm that there are no differences.18. Request the test operator to:<ol style="list-style-type: none">a. disconnect power to the SUT,b. insert an additional PCI add-in card,c. reconnect power to the SUT, andd. boot the SUT to Host OS.19. Wait for the SUT to return to S0/MeOn with the Host OS running.20. Retrieve the Hardware Asset information from the SUT via Intel® AMT.21. Compare the Hardware Asset information collected at step 3 with the information collected at step 17, and confirm that a PCI device was added to the hardware list.22. Gracefully shutdown to S5/MeOn the SUT via the Host OS and then wait 10 seconds.23. Request the test operator to:<ol style="list-style-type: none">a. disconnect power to the SUT,b. remove the additional PCI add-in card,c. reconnect power to the SUT, andd. boot the SUT to Host OS.24. Wait for the SUT to return to S0/MeOn with the Host OS running.25. Retrieve the Hardware Asset information from the SUT via Intel® AMT.26. Compare the Hardware Asset information collected at step 3 with the information collected at step 22, and confirm that there are no differences.
Pass Criteria:	The test passes if Intel® PETS detects a change in the Hardware Asset list when the PCI device is added, there is no change after removal (as compared to the configuration at the start of the test), and Storage Redirection session does not result in any change in the Hardware Asset list.
References:	For details on BIOS hardware asset tables sent to Intel® AMT, refer the <i>Intel® ME BIOS Specification</i> .

11.5.5 BAE PET Support

ID:	AMT_014
Title:	Boot Audit Entry (BAE) Platform Event Trap (PET) Support
Requirement:	Mandatory



ID:	AMT_014			
System:	Form Factor	System Power Model	Intel® AMT Network Interface	LAN Type
	<input checked="" type="checkbox"/> Desktop <input checked="" type="checkbox"/> Workstation <input checked="" type="checkbox"/> Mobile	<input checked="" type="checkbox"/> Standard <input checked="" type="checkbox"/> Modern Standby or InstantGo*	<input type="checkbox"/> LAN <input checked="" type="checkbox"/> Either Used <input type="checkbox"/> WLAN <input type="checkbox"/> Not Used	<input checked="" type="checkbox"/> Integrated LAN <input type="checkbox"/> Discrete LAN <input type="checkbox"/> TBT Dock LAN
Method:	Automated by Intel® PETS			
Description:	A Boot Audit Entry (BAE) Platform Event Trap (PET) alert must be sent when booting to the default hard drive before passing control to the OS.			
Objective:	Verify that a BAE PET alert indicating a normal boot is sent when the system boots from the local hard drive for the third time in a row.			
Setup:	The initial state of the SUT should be S0/MeOn with Host OS running. Intel® AMT should be provisioned via manual mode.			
Procedure:	<ol style="list-style-type: none"> Set the active power package on the SUT to Power Package 2 (Intel® ME on in S0, wake in Sx/AC). Set the Intel® AMT WLAN link policy on the SUT to Link Policy 3 (Enabled in S0, Sx/AC), if the WLAN network interface is used. Clear the Intel® AMT Event Manager log on the SUT. Gracefully shutdown to S5/MeOn the SUT via the Host OS and then wait 10 seconds. Perform a Remote Power-Up of the SUT via Intel® AMT. Wait for the SUT to return to S0/MeOn with the Host OS running. Repeat steps 3 through 5 each two more times. This yields a total of three boots to the hard drive. Dump the Event Manager log to a local file on the SUT. Transfer the Event Manager log file from the SUT to the management console. On the management console, parse the Event Manager log, and verify that the most recent BAE PET alert sent by the SUT indicates a normal boot with the following Event Data: <ul style="list-style-type: none"> Event Data 1 is set to 0x40 (Progress Event) Event Data 2 is set to 0x13 (System Boot) 			
Pass Criteria:	The test passes if all of the following are confirmed: <ul style="list-style-type: none"> The SUT boots to the hard drive each time a normal boot is performed. BAE PET alert indicating normal boot is sent when a normal boot is performed third time in a row (most BIOS implementations indicate via BAE PET alert that a normal boot occurred the second time the system is booted). 			
References:	For details on BAE PET events, refer the <i>Intel® ME BIOS Specification</i> .			

11.5.6 BAE PET Support with Alternate Boot Device

ID:	AMT_015			
Title:	Boot Audit Entry (BAE) Platform Event Trap (PET) Support with Alternate Boot Device			
Requirement:	Mandatory - exempt for systems that have no internal or removable CD/DVD drive support and can only boot via external USB-connected CD/DVD drive.			
System:	Form Factor	System Power Model	Intel® AMT Network Interface	LAN Type
	<input checked="" type="checkbox"/> Desktop <input checked="" type="checkbox"/> Workstation <input checked="" type="checkbox"/> Mobile	<input checked="" type="checkbox"/> Standard <input checked="" type="checkbox"/> Modern Standby or InstantGo*	<input type="checkbox"/> LAN <input checked="" type="checkbox"/> Either Used <input type="checkbox"/> WLAN <input type="checkbox"/> Not Used	<input checked="" type="checkbox"/> Integrated LAN <input type="checkbox"/> Discrete LAN <input type="checkbox"/> TBT Dock LAN
Method:	Automated by Intel® PETS with test operator interaction			
Description:	The BIOS must override the BBS (BIOS Boot Specification) table when boot options are set which designate a different boot device. A Boot Audit Entry (BAE) Platform Event Trap (PET) alert must be sent when a new boot device has been designated between boots, or a boot is performed from an alternate device.			
Objective:	Verify that the BIOS follows the specified boot option or defaults to the standard when no boot option is sent. Verify that a BAE PET alert is sent when the boot device is changed, or the SUT is booting from a removable device. Verify that a BAE PET alert indicating a normal boot is sent when the system boots from the local hard drive for the second time in a row.			
Setup:	The initial state of the SUT should be S0/MeOn with Host OS running. Intel® AMT should be provisioned via manual mode. This test checks multiple different boot flows to different devices including CD/DVD. Be sure to prepare a system which has a CD/DVD drive attached with bootable media inserted.			

ID:	AMT_015
Procedure:	<ol style="list-style-type: none"> 1. Set the active power package on the SUT to Power Package 2 (Intel® ME on in S0, wake in Sx/AC). 2. Set the Intel® AMT WLAN link policy on the SUT to Link Policy 3 (Enabled in S0, Sx/AC), if the WLAN network interface is used. 3. Clear the Intel® AMT Event Manager log on the SUT. 4. Gracefully shutdown to S5/MeOn the SUT via the Host OS and then wait 10 seconds. 5. Use Intel® AMT to set the boot option to Force CD/DVD Boot on the SUT for the next boot. 6. Inform the test operator that a system boot is performed by Intel® PETS requesting that the BIOS boot to the CD/DVD device. 7. Perform a Remote Power-Up of the SUT via Intel® AMT. 8. Wait for the SUT to return to S0/MeOn. Note that it is not possible for Intel® PETS to programmatically confirm that the SUT actually booted to CD/DVD. 9. Request the test operator to: <ol style="list-style-type: none"> a. confirm that system booted to the CD/DVD, b. gracefully shutdown the SUT 10. Wait for the SUT to move to S5/MeOn.
Procedure: (continued)	<ol style="list-style-type: none"> 11. Use Intel® AMT to set the boot option to Force CD/DVD Boot on the SUT for the next boot again. 12. Inform the test operator that a system boot is performed by Intel® PETS requesting that the BIOS boot to the CD/DVD device. 13. Perform a Remote Power-Up of the SUT via Intel® AMT. 14. Wait for the SUT to return to S0/MeOn. Note that it is not possible for Intel® PETS to programmatically confirm that the SUT actually booted to CD/DVD. 15. Request the test operator to: <ol style="list-style-type: none"> a. confirm that system booted to the CD/DVD, b. gracefully shutdown the SUT, and c. boot the SUT to Host OS. 16. Wait for the SUT to return to S0/MeOn with the Host OS running. 17. Dump the Event Manager log to a local file on the SUT. 18. Transfer the Event Manager log file from the SUT to the management console. 19. On the management console, parse the Event Manager log, and verify that the most recent BAE PET alert sent by the SUT indicates a 'unusual event' boot with the following Event Data: <ul style="list-style-type: none"> — Event Data 1 is set to 0xAA (OEM Specific) — Event Data 2 is set to 0x13 (System Boot) — Event Data 3 is set to 0x02 (Most Recent BAE: Boot to hard drive) — Event Data 4 is set to 0x03 (Next Most Recent BAE: Boot to removable device) — Event Data 5 is set to 0x03 (Oldest BAE: Boot to removable device)
Pass Criteria:	<p>The test passes if all of the following are confirmed:</p> <ul style="list-style-type: none"> • The SUT boots to CD/DVD when the boot option is set, and to the hard drive when a normal boot is performed. • BAE PET alert indicating new/removable device sent whenever the boot device is changed, or boot performed from a removable device.
References:	For details on BAE PET events, refer the <i>Intel® ME BIOS Specification</i> .

11.6 Remote Power Control

The section serves as a checklist for the environment setup and covers integration testing of the Remote Power Control feature in Intel® AMT.

11.6.1 Test Environment

The System Under Test (SUT) is to be configured with Intel® AMT set in manual provisioning mode with static IP address or DHCP. The management console may be a laptop or a desktop with a version of Microsoft Windows* supported by Intel® PETS, and the SUT should have a version of Microsoft Windows* supported by Intel® PETS as well. The test network is comprised of a hub/switch and network cables. The SUT should have only one system drive attached.

Tools for Testing:



- Intel® PETS: The latest version of the tool from the Intel® CSME Compliance and Debug kit release. Refer the Intel® PETS User Guide for exact instructions on how to load and setup the Intel® PETS software.
- Intel® Automated Power Switch (Intel® APS): The SUT should be connected to an Intel® APS 3 unit. In case an Intel® APS 3 is not available, select the Manual configuration in the Intel® PETS SUT profile configuration menu.
- Intel® PETS Local Agent: The local agent must be installed on the SUT.

Where applicable, the wireless LAN interface on Intel® AMT must be on a different network/subnet than the wired LAN interface. For details on how to enter the network interface details into Intel® PETS, consult the Intel® PETS User Guide.

If the firmware image or the SUT configuration does not support some features, Intel® PETS show those features as failing when tested. Intel® PETS cannot determine in all cases which features have been deactivated and should thus be skipped during testing.

11.6.2 Remote Power Control via Intel® AMT LAN Network Interface for Mobile Systems

ID:	AMT_020			
Title:	Remote Power Control via Intel® AMT LAN Network Interface for Mobile Systems			
Requirement:	Mandatory			
System:	Form Factor <input type="checkbox"/> Desktop <input type="checkbox"/> Workstation <input checked="" type="checkbox"/> Mobile	System Power Model <input checked="" type="checkbox"/> Standard <input checked="" type="checkbox"/> Modern Standby or InstantGo*	Intel® AMT Network Interface <input checked="" type="checkbox"/> LAN <input type="checkbox"/> Either Used <input type="checkbox"/> WLAN <input type="checkbox"/> Not Used	LAN Type <input checked="" type="checkbox"/> Integrated LAN <input type="checkbox"/> Discrete LAN <input type="checkbox"/> TBT Dock LAN
Method:	Automated by Intel® PETS			
Description:	An Intel® AMT compliant system supports the following remote control operations: <ul style="list-style-type: none"> • Reset • Power-Up • Power-Down • Power-Cycle 			
Objective:	Verify that the remote control management features of the Intel® AMT platform meet the requirements. Intel® AMT enables remote management of the platform, including the capability to control platform power states (reset, power-on/off/cycle). This test verifies that the BIOS has been properly enabled to support these usage models.			
Setup:	The initial state of the SUT should be S0/MeOn with Host OS running. Intel® AMT should be provisioned via manual mode.			

ID:	AMT_020																									
Procedure:	<div><div><div>1. Ensure the system power configuration is set to AC/DC.</div><div>2. Set the active power package on the SUT to Power Package 1 (Intel® ME on in S0).</div><div>3. Perform the following remote control operations across the given power states:</div></div><table><tr><th>SUT Initial state</th><th>Reset</th><th>Power-Cycle</th><th>Power-Up</th><th>Power-Down</th></tr><tr><td>S0-></td><td>S0</td><td>S0</td><td>N/A</td><td>S5/DS5[†]</td></tr><tr><td>S3-></td><td>N/A</td><td>N/A</td><td>N/A</td><td>N/A</td></tr><tr><td>S4-></td><td>N/A</td><td>N/A</td><td>N/A</td><td>N/A</td></tr><tr><td>S5-></td><td>N/A</td><td>N/A</td><td>N/A</td><td>N/A</td></tr></table><div><div>Each flow in the table above is executed as if they are part of an independent sub-test.</div><div>4. Verify that the relevant power flow operation succeeded for each flow in the table above. Additionally, for applicable Reset, Power-Cycle, and Power-Down flows, perform the following additional sub-steps for two (2) cycles each after the remote control operation has completed:</div><div><div>a. If shutdown, briefly press the Power Button on the SUT.</div><div>b. Verify that the Host OS on the SUT is available.</div><div>c. Record the Host OS last boot time on the SUT (to verify successful restart).</div><div>d. Perform a graceful restart of the SUT via Host OS.</div><div>e. Verify that the SUT is in S0/MeOn (CM0,CM0-PG).</div><div>f. Verify the Host OS last boot time on the SUT does not match the boot time recorded before the restart.</div></div><div><div>If a failure occurs at any point during the flow above (including during any additional applicable sub-steps), the remainder of the steps related to the sub-test, may be skipped.</div><div>Regardless of the prior sub-test overall results, before beginning the next sub-test, attempt to bring the SUT to a base state via the following:</div><div><div>a. Verify that the SUT is in S0/MeOn (CM0,CM0-PG).</div><div>b. Verify that the Host OS on the SUT is available.</div><div>c. Verify that Intel® AMT on the SUT responds to version queries via the LAN network interface.</div></div><div><div>If any of base state verification steps above fail, perform the following as an attempt to recover the SUT before attempting the base state verification steps above one last time:</div><div><div>a. Bring the system to G3 and wait 10 seconds.</div><div>b. Set system power configuration to AC/DC and wait another 10 seconds.</div><div>c. Briefly press the Power Button on the SUT.</div></div></div></div></div></div>	SUT Initial state	Reset	Power-Cycle	Power-Up	Power-Down	S0->	S0	S0	N/A	S5/DS5 [†]	S3->	N/A	N/A	N/A	N/A	S4->	N/A	N/A	N/A	N/A	S5->	N/A	N/A	N/A	N/A
	SUT Initial state	Reset	Power-Cycle	Power-Up	Power-Down																					
	S0->	S0	S0	N/A	S5/DS5 [†]																					
	S3->	N/A	N/A	N/A	N/A																					
	S4->	N/A	N/A	N/A	N/A																					
	S5->	N/A	N/A	N/A	N/A																					



ID:	AMT_020																									
Procedure: (continued)	5. Set the active power package on the SUT to Power Package 2 (Intel® ME on in S0, wake in Sx/AC).																									
	6. Perform the following remote control operations across the given power states:																									
	<table><tr><th>SUT Initial state</th><th>Reset</th><th>Power-Cycle</th><th>Power-Up</th><th>Power-Down</th></tr><tr><td>S0-></td><td>S0</td><td>S0</td><td>N/A</td><td>S5</td></tr><tr><td>S3-></td><td>N/A</td><td>S0</td><td>S0</td><td>S5</td></tr><tr><td>S4-></td><td>N/A</td><td>N/A</td><td>S0</td><td>N/A</td></tr><tr><td>S5-></td><td>N/A</td><td>N/A</td><td>S0</td><td>N/A</td></tr></table>	SUT Initial state	Reset	Power-Cycle	Power-Up	Power-Down	S0->	S0	S0	N/A	S5	S3->	N/A	S0	S0	S5	S4->	N/A	N/A	S0	N/A	S5->	N/A	N/A	S0	N/A
	SUT Initial state	Reset	Power-Cycle	Power-Up	Power-Down																					
	S0->	S0	S0	N/A	S5																					
	S3->	N/A	S0	S0	S5																					
	S4->	N/A	N/A	S0	N/A																					
	S5->	N/A	N/A	S0	N/A																					
	Each flow in the table above is executed as if they are part of an independent sub-test. In the case of Modern Standby or Microsoft Windows* InstantGo* mode, the S3 test flows is skipped.																									
	7. Verify that the relevant power flow operation succeeded for each flow in the table above. Additionally, for applicable Reset, Power-Cycle, and Power-Down flows in the chart above, perform the following additional sub-steps for two (2) cycles each after the remote control operation has completed:																									
a. If shutdown, briefly press the Power Button on the SUT.																										
b. Verify that the Host OS on the SUT is available.																										
c. Record the Host OS last boot time on the SUT (to verify successful restart).																										
d. Perform a graceful restart of the SUT via Host OS.																										
e. Verify that the SUT is in S0/MeOn (CM0,CM0-PG).																										
f. Verify the Host OS last boot time on the SUT does not match the boot time recorded before the restart.																										
If a failure occurs at any point during the flow above (including during any additional applicable sub-steps), the remainder of the steps related to the sub-test, may be skipped.																										
Regardless of the prior sub-test overall results, before beginning the next sub-test, attempt to bring the SUT to a base state via the following:																										
a. Verify that the SUT is in S0/MeOn (CM0,CM0-PG).																										
b. Verify that the Host OS on the SUT is available.																										
c. Verify that Intel® AMT on the SUT responds to version queries via the LAN network interface.																										
If any of base state verification steps above fail, perform the following as an attempt to recover the SUT before attempting the base state verification steps above one last time.																										
a. Bring the system to G3 and wait 10 seconds.																										
b. Set system power configuration to AC/DC and wait another 10 seconds.																										
c. Briefly press the Power Button on the SUT.																										
8. Set the SUT to DC-only power and repeat steps 2 through 7. Verify that the relevant power flow operations match the table in both steps 3 and 6 for both Power Package 1 and Power Package 2 using their associated verification methods in steps 4 and 7 respectively.																										
† In the case of Power Package 1 configuration or DC-only power configuration testing, the SUT enters the relative Deep Sx state when the BIOS has enabled Deep Sx.																										
Pass Criteria:	The test passes if Intel® PETS confirms each test step succeeded.																									
References:	For details on Remote Control Operations, refer the Intel® ME BIOS Specification.																									

11.6.3 Remote Power Control via Intel® AMT WLAN Network Interface for Mobile Systems

ID:	AMT_021			
Title:	Remote Power Control via Intel® AMT WLAN Network Interface for Mobile Systems			
Requirement:	Mandatory			
System:	Form Factor <input type="checkbox"/> Desktop <input type="checkbox"/> Workstation <input checked="" type="checkbox"/> Mobile	System Power Model <input checked="" type="checkbox"/> Standard <input checked="" type="checkbox"/> Modern Standby or InstantGo*	Intel® AMT Network Interface <input type="checkbox"/> LAN <input type="checkbox"/> Either Used <input checked="" type="checkbox"/> WLAN <input type="checkbox"/> Not Used	LAN Type <input type="checkbox"/> Integrated LAN <input type="checkbox"/> Discrete LAN <input type="checkbox"/> TBT Dock LAN
Method:	Automated by Intel® PETS			



ID:	AMT_021																									
Description:	An Intel® AMT compliant system supports the following remote control operations: <ul style="list-style-type: none">ResetPower-UpPower-DownPower-Cycle																									
Objective:	Verify that the remote control management features of the Intel® AMT platform meet the requirements. Intel® AMT enables remote management of the platform, including the capability to control platform power states (reset, power-on/off/cycle). This test verifies that the BIOS has been properly enabled to support these usage models.																									
Setup:	The initial state of the SUT should be S0/MeOn with Host OS running. Intel® AMT should be provisioned via manual mode.																									
Procedure:	<div>1. Ensure the system power configuration is set to AC/DC.</div> <div>2. Set the active power package on the SUT to Power Package 1 (Intel® ME on in S0).</div> <div>3. Set the Intel® AMT WLAN link policy on the SUT to Link Policy 2 (Enabled in S0).</div> <div>4. Ensure the Host OS Wake on Wireless LAN is disabled.</div> <div>5. Verify that Intel® AMT is available via WLAN by requesting its version.</div> <div>6. Perform the following remote control operations across the given power states:</div> <table><thead><tr><th>SUT Initial state</th><th>Reset</th><th>Power-Cycle</th><th>Power-Up</th><th>Power-Down</th></tr></thead><tbody><tr><td>S0-></td><td>S0</td><td>S0</td><td>N/A</td><td>S5/DS5†</td></tr><tr><td>S3-></td><td>N/A</td><td>N/A</td><td>N/A</td><td>N/A</td></tr><tr><td>S4-></td><td>N/A</td><td>N/A</td><td>N/A</td><td>N/A</td></tr><tr><td>S5-></td><td>N/A</td><td>N/A</td><td>N/A</td><td>N/A</td></tr></tbody></table> <div>Each flow in the table above is executed as if they are part of an independent sub-test.</div> <div>7. Verify that the relevant power flow operation succeeded for each flow in the table above. Additionally, for applicable Reset, Power-Cycle, and Power-Down flows, perform the following additional sub-steps for two (2) cycles each after the remote control operation has completed:<div><div>a. If shutdown, briefly press the Power Button on the SUT.</div><div>b. Verify that the Host OS on the SUT is available.</div><div>c. Record the Host OS last boot time on the SUT (to verify successful restart).</div><div>d. Perform a graceful restart of the SUT via Host OS.</div><div>e. Verify that the SUT is in S0/MeOn (CM0,CM0-PG).</div><div>f. Verify the Host OS last boot time on the SUT does not match the boot time recorded before the restart.</div></div></div> <div>If a failure occurs at any point during the flow above (including during any additional applicable sub-steps), the remainder of the steps related to the sub-test, may be skipped.</div> <div>Regardless of the prior sub-test overall results, before beginning the next sub-test, attempt to bring the SUT to a base state via the following:<div><div>a. Verify that the SUT is in S0/MeOn (CM0,CM0-PG).</div><div>b. Verify that the Host OS on the SUT is available.</div><div>c. Verify that Intel® AMT on the SUT responds to version queries via the WLAN network interface.</div></div></div> <div>If any of base state verification steps above fail, perform the following as an attempt to recover the SUT before attempting the base state verification steps above one last time:<div><div>a. Bring the system to G3 and wait 10 seconds.</div><div>b. Set system power configuration to AC/DC and wait another 10 seconds.</div><div>c. Briefly press the Power Button on the SUT.</div></div></div>	SUT Initial state	Reset	Power-Cycle	Power-Up	Power-Down	S0->	S0	S0	N/A	S5/DS5†	S3->	N/A	N/A	N/A	N/A	S4->	N/A	N/A	N/A	N/A	S5->	N/A	N/A	N/A	N/A
	SUT Initial state	Reset	Power-Cycle	Power-Up	Power-Down																					
	S0->	S0	S0	N/A	S5/DS5†																					
	S3->	N/A	N/A	N/A	N/A																					
	S4->	N/A	N/A	N/A	N/A																					
	S5->	N/A	N/A	N/A	N/A																					



ID:	AMT_021																									
Procedure: (continued)	8. Set the active power package on the SUT to Power Package 2 (Intel® ME on in S0, wake in Sx/AC).																									
	9. Set the Intel® AMT WLAN link policy on the SUT to Link Policy 3 (Enabled in S0, Sx/AC).																									
	10. Perform the following remote control operations across the given power states:																									
	<table><tr><th>SUT Initial state</th><th>Reset</th><th>Power-Cycle</th><th>Power-Up</th><th>Power-Down</th></tr><tr><td>S0-></td><td>S0</td><td>S0</td><td>N/A</td><td>S5</td></tr><tr><td>S3-></td><td>N/A</td><td>S0</td><td>S0</td><td>S5</td></tr><tr><td>S4-></td><td>N/A</td><td>N/A</td><td>S0</td><td>N/A</td></tr><tr><td>S5-></td><td>N/A</td><td>N/A</td><td>S0</td><td>N/A</td></tr></table>	SUT Initial state	Reset	Power-Cycle	Power-Up	Power-Down	S0->	S0	S0	N/A	S5	S3->	N/A	S0	S0	S5	S4->	N/A	N/A	S0	N/A	S5->	N/A	N/A	S0	N/A
	SUT Initial state	Reset	Power-Cycle	Power-Up	Power-Down																					
	S0->	S0	S0	N/A	S5																					
	S3->	N/A	S0	S0	S5																					
	S4->	N/A	N/A	S0	N/A																					
	S5->	N/A	N/A	S0	N/A																					
	Each flow in the table above is executed as if they are part of an independent sub-test. In the case of Modern Standby or Microsoft Windows* InstantGo* mode, the S3 test flows are skipped.																									
11. Verify that the relevant power flow operation succeeded for each flow in the table above. Additionally, for applicable Reset, Power-Cycle, and Power-Down flows in the chart above, perform the following additional sub-steps for two (2) cycles each after the remote control operation has completed:																										
a. If shutdown, briefly press the Power Button on the SUT.																										
b. Verify that the Host OS on the SUT is available.																										
c. Record the Host OS last boot time on the SUT (to verify successful restart).																										
d. Perform a graceful restart of the SUT via Host OS.																										
e. Verify that the SUT is in S0/MeOn (CM0,CM0-PG).																										
f. Verify the Host OS last boot time on the SUT does not match the boot time recorded before the restart.																										
If a failure occurs at any point during the flow above (including during any additional applicable sub-steps), the remainder of the steps related to the sub-test, may be skipped.																										
Regardless of the prior sub-test overall results, before beginning the next sub-test, attempt to bring the SUT to a base state via the following:																										
a. Verify that the SUT is in S0/MeOn (CM0,CM0-PG).																										
b. Verify that the Host OS on the SUT is available.																										
c. Verify that Intel® AMT on the SUT responds to version queries via the WLAN network interface.																										
If any of base state verification steps above fail, perform the following as an attempt to recover the SUT before attempting the base state verification steps above one last time.																										
a. Bring the system to G3 and wait 10 seconds.																										
b. Set system power configuration to AC/DC and wait another 10 seconds.																										
c. Briefly press the Power Button on the SUT.																										
12. Set the SUT to DC-only power and repeat steps 2 through 11. Verify that the relevant power flow operations match the table in step 6 for both Power Package 1 (Link Policy 2) and Power Package 2 (Link Policy 3) respectively.																										
† In the case of Power Package 1 configuration or DC-only power configuration testing, the SUT enters the relative Deep Sx state when the BIOS has enabled Deep Sx.																										
Pass Criteria:	The test passes if Intel® PETS confirms each test step succeeded.																									
References:	For details on Remote Control Operations, refer the <i>Intel® ME BIOS Specification</i> .																									

11.6.4 Remote Power Control via Intel® AMT LAN Network Interface for Non-Mobile Systems

ID:	AMT_022			
Title:	Remote Power Control via Intel® AMT LAN Network Interface for Non-Mobile Systems			
Requirement:	Mandatory			
System:	Form Factor	System Power Model	Intel® AMT Network Interface	LAN Type
	<input checked="" type="checkbox"/> Desktop <input checked="" type="checkbox"/> Workstation <input type="checkbox"/> Mobile	<input checked="" type="checkbox"/> Standard <input type="checkbox"/> Modern Standby or InstantGo*	<input checked="" type="checkbox"/> LAN <input type="checkbox"/> Either Used <input type="checkbox"/> WLAN <input type="checkbox"/> Not Used	<input checked="" type="checkbox"/> Integrated LAN <input type="checkbox"/> Discrete LAN <input type="checkbox"/> TBT Dock LAN



ID:	AMT_022																													
Method:	Automated by Intel® PETS																													
Description:	An Intel® AMT compliant system supports the following remote control operations: <ul style="list-style-type: none">• Reset• Power-Up• Power-Down• Power-Cycle																													
Objective:	Verify that the remote control management features of the Intel® AMT platform meet the requirements. Intel® AMT enables remote management of the platform, including the capability to control platform power states (reset, power-on/off/cycle). This test verifies that the BIOS has been properly enabled to support these usage models.																													
Setup:	The initial state of the SUT should be S0/MeOn with Host OS running. Intel® AMT should be provisioned via manual mode.																													
Procedure:	1. Set the active power package on the SUT to Power Package 1 (Intel® ME on in S0).																													
	2. Perform the following remote control operations across the given power states:																													
	<table><tr><td>SUT Initial state</td><td>Reset</td><td>Power-Cycle</td><td>Power-Up</td><td>Power-Down</td></tr><tr><td>S0-></td><td>S0</td><td>S0</td><td>N/A</td><td>S5/DS5[†]</td></tr><tr><td>S3-></td><td>N/A</td><td>N/A</td><td>N/A</td><td>N/A</td></tr><tr><td>S4-></td><td>N/A</td><td>N/A</td><td>N/A</td><td>N/A</td></tr><tr><td>S5-></td><td>N/A</td><td>N/A</td><td>N/A</td><td>N/A</td></tr></table>					SUT Initial state	Reset	Power-Cycle	Power-Up	Power-Down	S0->	S0	S0	N/A	S5/DS5 [†]	S3->	N/A	N/A	N/A	N/A	S4->	N/A	N/A	N/A	N/A	S5->	N/A	N/A	N/A	N/A
	SUT Initial state	Reset	Power-Cycle	Power-Up	Power-Down																									
	S0->	S0	S0	N/A	S5/DS5 [†]																									
	S3->	N/A	N/A	N/A	N/A																									
	S4->	N/A	N/A	N/A	N/A																									
	S5->	N/A	N/A	N/A	N/A																									
	Each flow in the table above is executed as if they are part of an independent sub-test.																													
	3. Verify that the relevant power flow operation succeeded for each flow in the table above. Additionally, for applicable Reset, Power-Cycle, and Power-Down flows, perform the following additional sub-steps for two (2) cycles each after the remote control operation has completed:																													
a. If shutdown, briefly press the Power Button on the SUT.																														
b. Verify that the Host OS on the SUT is available.																														
c. Record the Host OS last boot time on the SUT (to verify successful restart).																														
d. Perform a graceful restart of the SUT via Host OS.																														
e. Verify that the SUT is in S0/MeOn (CM0,CM0-PG).																														
f. Verify the Host OS last boot time on the SUT does not match the boot time recorded before the restart.																														
If a failure occurs at any point during the flow above (including during any additional applicable sub-steps), the remainder of the steps related to the sub-test, may be skipped.																														
Regardless of the prior sub-test overall results, before beginning the next sub-test, attempt to bring the SUT to a base state via the following:																														
a. Verify that the SUT is in S0/MeOn (CM0,CM0-PG).																														
b. Verify that the Host OS on the SUT is available.																														
c. Verify that Intel® AMT on the SUT responds to version queries via the LAN network interface.																														
If any of base state verification steps above fail, perform the following as an attempt to recover the SUT before attempting the base state verification steps above one last time:																														
a. Bring the system to G3 and wait 10 seconds.																														
b. Set system power configuration to AC/DC and wait another 10 seconds.																														
c. Briefly press the Power Button on the SUT.																														



ID:	AMT_022																									
Procedure: (continued)	4. Set the active power package on the SUT to Power Package 2 (Intel® ME on in S0, wake in Sx/AC).																									
	5. Perform the following remote control operations across the given power states:																									
	<table><tr><th>SUT Initial state</th><th>Reset</th><th>Power-Cycle</th><th>Power-Up</th><th>Power-Down</th></tr><tr><td>S0-></td><td>S0</td><td>S0</td><td>N/A</td><td>S5</td></tr><tr><td>S3-></td><td>N/A</td><td>S0</td><td>S0</td><td>S5</td></tr><tr><td>S4-></td><td>N/A</td><td>N/A</td><td>S0</td><td>N/A</td></tr><tr><td>S5-></td><td>N/A</td><td>N/A</td><td>S0</td><td>N/A</td></tr></table>	SUT Initial state	Reset	Power-Cycle	Power-Up	Power-Down	S0->	S0	S0	N/A	S5	S3->	N/A	S0	S0	S5	S4->	N/A	N/A	S0	N/A	S5->	N/A	N/A	S0	N/A
	SUT Initial state	Reset	Power-Cycle	Power-Up	Power-Down																					
	S0->	S0	S0	N/A	S5																					
	S3->	N/A	S0	S0	S5																					
	S4->	N/A	N/A	S0	N/A																					
	S5->	N/A	N/A	S0	N/A																					
	Each flow in the table above is executed as if they are part of an independent sub-test. For desktop systems with Intel® RMT support, ensure that Intel® RMT is disabled before running S3 test flows.																									
	6. Verify that the relevant power flow operation succeeded for each flow in the table above. Additionally, for applicable Reset, Power-Cycle, and Power-Down flows in the chart above, perform the following additional sub-steps for two (2) cycles each after the remote control operation has completed:																									
a. If shutdown, briefly press the Power Button on the SUT.																										
b. Verify that the Host OS on the SUT is available.																										
c. Record the Host OS last boot time on the SUT (to verify successful restart).																										
d. Perform a graceful restart of the SUT via Host OS.																										
e. Verify that the SUT is in S0/MeOn (CM0,CM0-PG).																										
f. Verify the Host OS last boot time on the SUT does not match the boot time recorded before the restart.																										
If a failure occurs at any point during the flow above (including during any additional applicable sub-steps), the remainder of the steps related to the sub-test, may be skipped.																										
Regardless of the prior sub-test overall results, before beginning the next sub-test, attempt to bring the SUT to a base state via the following:																										
a. Verify that the SUT is in S0/MeOn (CM0,CM0-PG).																										
b. Verify that the Host OS on the SUT is available.																										
c. Verify that Intel® AMT on the SUT responds to version queries via the LAN network interface.																										
If any of base state verification steps above fail, perform the following as an attempt to recover the SUT before attempting the base state verification steps above one last time																										
a. Bring the system to G3 and wait 10 seconds.																										
b. Set system power configuration to AC/DC and wait another 10 seconds.																										
c. Briefly press the Power Button on the SUT.																										
† In the case of Power Package 1 configuration testing, the SUT enter the relative Deep Sx state when the BIOS has enabled Deep Sx.																										
Pass Criteria:	The test passes if Intel® PETS confirms each test step succeeded.																									
References:	For details on Remote Control Operations, refer the <i>Intel® ME BIOS Specification</i> .																									

11.6.5 Remote Power Control via Intel® AMT WLAN Network Interface for Non-Mobile Systems

ID:	AMT_023			
Title:	Remote Power Control via Intel® AMT WLAN Network Interface for Non-Mobile Systems			
Requirement:	Mandatory			
System:	Form Factor <input checked="" type="checkbox"/> Desktop <input checked="" type="checkbox"/> Workstation <input type="checkbox"/> Mobile	System Power Model <input checked="" type="checkbox"/> Standard <input type="checkbox"/> Modern Standby or InstantGo*	Intel® AMT Network Interface <input type="checkbox"/> LAN <input type="checkbox"/> Either Used <input checked="" type="checkbox"/> WLAN <input type="checkbox"/> Not Used	LAN Type <input type="checkbox"/> Integrated LAN <input type="checkbox"/> Discrete LAN <input type="checkbox"/> TBT Dock LAN
Method:	Automated by Intel® PETS			

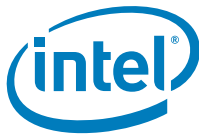
ID:	AMT_023																									
Description:	An Intel® AMT compliant system supports the following remote control operations: <ul style="list-style-type: none">ResetPower-UpPower-DownPower-Cycle																									
Objective:	Verify that the remote control management features of the Intel® AMT platform meet the requirements. Intel® AMT enables remote management of the platform, including the capability to control platform power states (reset, power-on/off/cycle). This test verifies that the BIOS has been properly enabled to support these usage models.																									
Setup:	The initial state of the SUT should be S0/MeOn with Host OS running. Intel® AMT should be provisioned via manual mode.																									
Procedure:	<div><div><div>1. Set the active power package on the SUT to Power Package 1 (Intel® ME on in S0).</div><div>2. Set the Intel® AMT WLAN link policy on the SUT to Link Policy 2 (Enabled in S0).</div><div>3. Ensure the Host OS Wake on Wireless LAN is disabled.</div><div>4. Verify that Intel® AMT is available via WLAN by requesting its version.</div><div>5. Perform the following remote control operations across the given power states:</div></div><table><thead><tr><th>SUT Initial state</th><th>Reset</th><th>Power-Cycle</th><th>Power-Up</th><th>Power-Down</th></tr></thead><tbody><tr><td>S0-></td><td>S0</td><td>S0</td><td>N/A</td><td>S5/DS5[†]</td></tr><tr><td>S3-></td><td>N/A</td><td>N/A</td><td>N/A</td><td>N/A</td></tr><tr><td>S4-></td><td>N/A</td><td>N/A</td><td>N/A</td><td>N/A</td></tr><tr><td>S5-></td><td>N/A</td><td>N/A</td><td>N/A</td><td>N/A</td></tr></tbody></table><div><p>Each flow in the table above is executed as if they are part of an independent sub-test.</p><div>6. Verify that the relevant power flow operation succeeded for each flow in the table above. Additionally, for applicable Reset, Power-Cycle, and Power-Down flows, perform the following additional sub-steps for two (2) cycles each after the remote control operation has completed:</div><div><div>a. If shutdown, briefly press the Power Button on the SUT.</div><div>b. Verify that the Host OS on the SUT is available.</div><div>c. Record the Host OS last boot time on the SUT (to verify successful restart).</div><div>d. Perform a graceful restart of the SUT via Host OS.</div><div>e. Verify that the SUT is in S0/MeOn (CM0,CM0-PG).</div><div>f. Verify the Host OS last boot time on the SUT does not match the boot time recorded before the restart.</div></div><p>If a failure occurs at any point during the flow above (including during any additional applicable sub-steps), the remainder of the steps related to the sub-test, may be skipped.</p><p>Regardless of the prior sub-test overall results, before beginning the next sub-test, attempt to bring the SUT to a base state via the following:</p><div><div>a. Verify that the SUT is in S0/MeOn (CM0,CM0-PG).</div><div>b. Verify that the Host OS on the SUT is available.</div><div>c. Verify that Intel® AMT on the SUT responds to version queries via the WLAN network interface.</div></div><p>If any of base state verification steps above fail, perform the following as an attempt to recover the SUT before attempting the base state verification steps above one last time:</p><div><div>a. Bring the system to G3 and wait 10 seconds.</div><div>b. Set system power configuration to AC/DC and wait another 10 seconds.</div><div>c. Briefly press the Power Button on the SUT.</div></div></div></div>	SUT Initial state	Reset	Power-Cycle	Power-Up	Power-Down	S0->	S0	S0	N/A	S5/DS5 [†]	S3->	N/A	N/A	N/A	N/A	S4->	N/A	N/A	N/A	N/A	S5->	N/A	N/A	N/A	N/A
SUT Initial state	Reset	Power-Cycle	Power-Up	Power-Down																						
S0->	S0	S0	N/A	S5/DS5 [†]																						
S3->	N/A	N/A	N/A	N/A																						
S4->	N/A	N/A	N/A	N/A																						
S5->	N/A	N/A	N/A	N/A																						



ID:	AMT_023																									
Procedure: (continued)	7. Set the active power package on the SUT to Power Package 2 (Intel® ME on in S0, wake in Sx/AC).																									
	8. Set the Intel® AMT WLAN link policy on the SUT to Link Policy 3 (Enabled in S0, Sx/AC).																									
	9. Perform the following remote control operations across the given power states:																									
	<table><tr><th>SUT Initial state</th><th>Reset</th><th>Power-Cycle</th><th>Power-Up</th><th>Power-Down</th></tr><tr><td>S0-></td><td>S0</td><td>S0</td><td>N/A</td><td>S5</td></tr><tr><td>S3-></td><td>N/A</td><td>S0</td><td>S0</td><td>S5</td></tr><tr><td>S4-></td><td>N/A</td><td>N/A</td><td>S0</td><td>N/A</td></tr><tr><td>S5-></td><td>N/A</td><td>N/A</td><td>S0</td><td>N/A</td></tr></table>	SUT Initial state	Reset	Power-Cycle	Power-Up	Power-Down	S0->	S0	S0	N/A	S5	S3->	N/A	S0	S0	S5	S4->	N/A	N/A	S0	N/A	S5->	N/A	N/A	S0	N/A
	SUT Initial state	Reset	Power-Cycle	Power-Up	Power-Down																					
	S0->	S0	S0	N/A	S5																					
	S3->	N/A	S0	S0	S5																					
	S4->	N/A	N/A	S0	N/A																					
	S5->	N/A	N/A	S0	N/A																					
	Each flow in the table above is executed as if they are part of an independent sub-test. For desktop systems with Intel® RMT support, ensure that Intel® RMT is disabled before running S3 test flows.																									
10. Verify that the relevant power flow operation succeeded for each flow in the table above. Additionally, for applicable Reset, Power-Cycle, and Power-Down flows in the chart above, perform the following additional sub-steps for two (2) cycles each after the remote control operation has completed:																										
<ul style="list-style-type: none">a. If shutdown, briefly press the Power Button on the SUT.b. Verify that the Host OS on the SUT is available.c. Record the Host OS last boot time on the SUT (to verify successful restart).d. Perform a graceful restart of the SUT via Host OS.e. Verify that the SUT is in S0/MeOn (CM0,CM0-PG).f. Verify the Host OS last boot time on the SUT does not match the boot time recorded before the restart.																										
If a failure occurs at any point during the flow above (including during any additional applicable sub-steps), the remainder of the steps related to the sub-test, may be skipped.																										
Regardless of the prior sub-test overall results, before beginning the next sub-test, attempt to bring the SUT to a base state via the following:																										
<ul style="list-style-type: none">a. Verify that the SUT is in S0/MeOn (CM0,CM0-PG).b. Verify that the Host OS on the SUT is available.c. Verify that Intel® AMT on the SUT responds to version queries via the WLAN network interface.																										
If any of base state verification steps above fail, perform the following as an attempt to recover the SUT before attempting the base state verification steps above one last time																										
<ul style="list-style-type: none">a. Bring the system to G3 and wait 10 seconds.b. Set system power configuration to AC/DC and wait another 10 seconds.c. Briefly press the Power Button on the SUT.																										
+ In the case of Power Package 1 configuration testing, the SUT enter the relative Deep Sx state when the BIOS has enabled Deep Sx.																										
Pass Criteria:	The test passes if Intel® PETS confirms each test step succeeded.																									
References:	For details on Remote Control Operations, refer the Intel® ME BIOS Specification.																									

11.6.6 Remote Power Control in S0 Low Power Idle State via Intel® AMT LAN Network Interface

ID:	AMT_024				
Title:	Remote Power Control with S0 Low Power Idle state, as with Modern Standby or Microsoft Windows* InstantGo* mode, via Intel® AMT LAN Network Interface				
System:	Form Factor	System Power Model	Intel® AMT Network Interface		LAN Type
	<input checked="" type="checkbox"/> Desktop <input type="checkbox"/> Workstation <input checked="" type="checkbox"/> Mobile	<input type="checkbox"/> Standard <input checked="" type="checkbox"/> Modern Standby or InstantGo*	<input checked="" type="checkbox"/> LAN <input type="checkbox"/> Either Used <input type="checkbox"/> WLAN <input type="checkbox"/> Not Used	<input checked="" type="checkbox"/> Integrated LAN <input type="checkbox"/> Discrete LAN <input type="checkbox"/> TBT Dock LAN	
Method:	Automated by Intel® PETS with test operator interaction				
Description:	Ensure that an Intel® AMT complaint system responds to RCO power command after the Host OS switches to S0 Low Power Idle state.				



ID:	AMT_024
Objective:	Verify that Intel® AMT responds in S0 Low Power Idle state to Remote Power Control commands.
Setup:	The initial state of the SUT should be S0/MeOn with Host OS running. Intel® AMT should be provisioned via manual mode. The SUT must be configured to work in Modern Standby or Microsoft Windows* InstantGo* mode. NOTE: In order to fully implement RCO wake, the host BIOS must implement Intel® Proprietary Wake . Also, HID Event Filter Driver must be installed. Failure to properly implement the above may result in failures for this test.
Procedure:	<ol style="list-style-type: none">1. Set the active power package on the SUT to Power Package 2 (Intel® ME on in S0, wake in Sx/AC).2. Request the test operator to manually place the SUT into S0 Low Power Idle state.3. Verify that the SUT has moved into S0 Low Power Idle state.4. Inform the test operator that a graceful system shutdown is performed by Intel® PETS and to acknowledge the forthcoming shutdown prompt which appear on the SUT.5. Perform a Remote Graceful Shutdown to S5/MeOn of the SUT via Intel® AMT and then wait 10 seconds.6. Perform a Remote Power-Up of the SUT via Intel® AMT.7. Wait for the SUT to return to S0/MeOn with the Host OS running.8. Request the test operator to manually place the SUT into S0 Low Power Idle state.9. Verify that the SUT has moved into S0 Low Power Idle state.
Pass Criteria:	The test passes if Intel® AMT is able perform Remote Power Command from S0 Low Power Idle state, and the system can be booted back to, and enter into S0 Low Power Idle state again.
References:	For details on Remote Control Operations, refer the <i>Intel® ME BIOS Specification</i> . For details on Intel® Proprietary Wake, refer HID Event Filter in <i>BIOS Enabling Guide for Windows* 10</i> .

11.6.7 Remote Power Control with S0 Low Power Idle via Intel® AMT WLAN Network Interface

ID:	AMT_025				
Title:	Remote Power Control with S0 Low Power Idle state, as with Modern Standby or Microsoft Windows* InstantGo* mode, via Intel® AMT WLAN Network Interface				
System:	Form Factor	System Power Model	Intel® AMT Network Interface		LAN Type
	<input checked="" type="checkbox"/> Desktop <input type="checkbox"/> Workstation <input checked="" type="checkbox"/> Mobile	<input type="checkbox"/> Standard <input checked="" type="checkbox"/> Modern Standby or InstantGo*	<input type="checkbox"/> LAN <input checked="" type="checkbox"/> WLAN	<input type="checkbox"/> Either Used <input type="checkbox"/> Not Used	<input type="checkbox"/> Integrated LAN <input type="checkbox"/> Discrete LAN <input type="checkbox"/> TBT Dock LAN
Method:	Automated by Intel® PETS with test operator interaction				
Description:	Ensure that an Intel® AMT complaint system responds to RCO power command after the Host OS switches to S0 Low Power Idle state.				
Objective:	Verify that Intel® AMT responds in S0 Low Power Idle state to Remote Power Control commands.				
Setup:	The initial state of the SUT should be S0/MeOn with Host OS running. Intel® AMT should be provisioned via manual mode. The SUT must be configured to work in Modern Standby or Microsoft Windows* InstantGo* mode.				
Procedure:	<ol style="list-style-type: none">1. Set the active power package on the SUT to Power Package 2 (Intel® ME on in S0, wake in Sx/AC).2. Set the Intel® AMT WLAN link policy on the SUT to Link Policy 3 (Enabled in S0, Sx/AC).3. Request the test operator to manually place the SUT into S0 Low Power Idle state.4. Verify that the SUT has moved into S0 Low Power Idle state.5. Inform the test operator that a graceful system shutdown is performed by Intel® PETS and to acknowledge the forthcoming shutdown prompt which appear on the SUT.6. Perform a Remote Graceful Shutdown to S5/MeOn of the SUT via Intel® AMT and then wait 10 seconds.7. Verify that Intel® AMT is available via WLAN by requesting its version.8. Perform a Remote Power-Up of the SUT via Intel® AMT.9. Wait for the SUT to return to S0/MeOn with the Host OS running.10. Request the test operator to manually place the SUT into S0 Low Power Idle state.11. Verify that the SUT has moved into S0 Low Power Idle state.				



ID:	AMT_025
Pass Criteria:	The test passes if Intel® AMT is able perform Remote Power Command from S0 Low Power Idle state, and the system can be booted back to, and enter into S0 Low Power Idle state again.
References:	For details on Remote Control Operations, refer the <i>Intel® ME BIOS Specification</i> .

11.6.8 Remote Power Control via Intel® AMT WLAN Network Interface for Mobile Systems Supporting Wake On Wireless LAN

ID:	AMT_026			
Title:	Remote Power Control via Intel® AMT WLAN Network Interface for Mobile Systems supporting Wake on Wireless LAN			
Requirement:	Mandatory - exempt for systems that do not support Wake on Wireless LAN			
System:	Form Factor <input type="checkbox"/> Desktop <input type="checkbox"/> Workstation <input checked="" type="checkbox"/> Mobile	System Power Model <input checked="" type="checkbox"/> Standard <input type="checkbox"/> Modern Standby or InstantGo*	Intel® AMT Network Interface <input type="checkbox"/> LAN <input type="checkbox"/> Either Used <input checked="" type="checkbox"/> WLAN <input type="checkbox"/> Not Used	LAN Type <input type="checkbox"/> Integrated LAN <input type="checkbox"/> Discrete LAN <input type="checkbox"/> TBT Dock LAN
Method:	Automated by Intel® PETS			
Description:	An Intel® AMT compliant system supports the following remote control operations: <ul style="list-style-type: none"> • Reset • Power-Up • Power-Down • Power-Cycle 			
Objective:	Verify that the remote control management features of the Intel® AMT platform meet the requirements. Intel® AMT enables remote management of the platform, including the capability to control platform power states (reset, power-on/off/cycle). This test verifies that the BIOS has been properly enabled to support these usage models.			
Setup:	The initial state of the SUT should be S0/MeOn with Host OS running. Intel® AMT should be provisioned via manual mode. NOTE: In order to fully implement Wake on Wireless LAN (WoWLAN) in Sx states, the host BIOS must set HOST_WLAN_PP_EN. For more further details, refer the PCH <i>External Design Specification (EDS)</i> and the PCH <i>Platform Design Guide (PDG)</i> . Failure to properly set the HOST_WLAN_PP_EN bit may result in failures for this test.			



ID:	AMT_026																									
Procedure:	<div>1. Ensure the system power configuration is set to AC/DC.</div> <div>2. Set the active power package on the SUT to Power Package 1 (Intel® ME on in S0).</div> <div>3. Set the Intel® AMT WLAN link policy on the SUT to Link Policy 2 (Enabled in S0).</div> <div>4. Ensure the Host OS Wake on Wireless LAN is enabled.</div> <div>5. Verify that Intel® AMT is available via WLAN by requesting its version.</div> <div>6. Perform the following remote control operations across the given power states:</div> <table><tr><th>SUT Initial state</th><th>Reset</th><th>Power-Cycle</th><th>Power-Up</th><th>Power-Down</th></tr><tr><td>S0-></td><td>S0</td><td>S0</td><td>N/A</td><td>S5/DS5[†]</td></tr><tr><td>S3-></td><td>N/A</td><td>S0</td><td>S0</td><td>S5/DS5[†]</td></tr><tr><td>S4-></td><td>N/A</td><td>N/A</td><td>N/A</td><td>N/A</td></tr><tr><td>S5-></td><td>N/A</td><td>N/A</td><td>N/A</td><td>N/A</td></tr></table> <div>Each flow in the table above is executed as if they are part of an independent sub-test.</div> <div>7. Verify that the relevant power flow operation succeeded for each flow in the table above. Additionally, for applicable Reset, Power-Cycle, and Power-Down flows, perform the following additional sub-steps for two (2) cycles each after the remote control operation has completed:</div> <div><div>a. If shutdown, briefly press the Power Button on the SUT.</div><div>b. Verify that the Host OS on the SUT is available.</div><div>c. Record the Host OS last boot time on the SUT (to verify successful restart).</div><div>d. Perform a graceful restart of the SUT via Host OS.</div><div>e. Verify that the SUT is in S0/MeOn (CM0,CM0-PG).</div><div>f. Verify the Host OS last boot time on the SUT does not match the boot time recorded before the restart.</div></div> <div>If a failure occurs at any point during the flow above (including during any additional applicable sub-steps), the remainder of the steps related to the sub-test, may be skipped.</div> <div>Regardless of the prior sub-test overall results, before beginning the next sub-test, attempt to bring the SUT to a base state via the following:</div> <div><div>a. Verify that the SUT is in S0/MeOn (CM0,CM0-PG).</div><div>b. Verify that the Host OS on the SUT is available.</div><div>c. Verify that Intel® AMT on the SUT responds to version queries via the WLAN network interface.</div></div> <div>If any of base state verification steps above fail, perform the following as an attempt to recover the SUT before attempting the base state verification steps above one last time:</div> <div><div>a. Bring the system to G3 and wait 10 seconds.</div><div>b. Set system power configuration to AC/DC and wait another 10 seconds.</div><div>c. Briefly press the Power Button on the SUT.</div></div>	SUT Initial state	Reset	Power-Cycle	Power-Up	Power-Down	S0->	S0	S0	N/A	S5/DS5 [†]	S3->	N/A	S0	S0	S5/DS5 [†]	S4->	N/A	N/A	N/A	N/A	S5->	N/A	N/A	N/A	N/A
	SUT Initial state	Reset	Power-Cycle	Power-Up	Power-Down																					
	S0->	S0	S0	N/A	S5/DS5 [†]																					
	S3->	N/A	S0	S0	S5/DS5 [†]																					
	S4->	N/A	N/A	N/A	N/A																					
	S5->	N/A	N/A	N/A	N/A																					



ID:	AMT_026																									
Procedure: (continued)	8. Set the active power package on the SUT to Power Package 2 (Intel® ME on in S0, wake in Sx/AC).																									
	9. Set the Intel® AMT WLAN link policy on the SUT to Link Policy 3 (Enabled in S0, Sx/AC).																									
	10. Perform the following remote control operations across the given power states:																									
	<table><tr><th>SUT Initial state</th><th>Reset</th><th>Power-Cycle</th><th>Power-Up</th><th>Power-Down</th></tr><tr><td>S0-></td><td>S0</td><td>S0</td><td>N/A</td><td>S5</td></tr><tr><td>S3-></td><td>N/A</td><td>S0</td><td>S0</td><td>S5</td></tr><tr><td>S4-></td><td>N/A</td><td>N/A</td><td>S0</td><td>N/A</td></tr><tr><td>S5-></td><td>N/A</td><td>N/A</td><td>S0</td><td>N/A</td></tr></table>	SUT Initial state	Reset	Power-Cycle	Power-Up	Power-Down	S0->	S0	S0	N/A	S5	S3->	N/A	S0	S0	S5	S4->	N/A	N/A	S0	N/A	S5->	N/A	N/A	S0	N/A
	SUT Initial state	Reset	Power-Cycle	Power-Up	Power-Down																					
	S0->	S0	S0	N/A	S5																					
	S3->	N/A	S0	S0	S5																					
	S4->	N/A	N/A	S0	N/A																					
	S5->	N/A	N/A	S0	N/A																					
	Each flow in the table above is executed as if they are part of an independent sub-test.																									
11. Verify that the relevant power flow operation succeeded for each flow in the table above. Additionally, for applicable Reset, Power-Cycle, and Power-Down flows in the chart above, perform the following additional sub-steps for two (2) cycles each after the remote control operation has completed:																										
a. If shutdown, briefly press the Power Button on the SUT.																										
b. Verify that the Host OS on the SUT is available.																										
c. Record the Host OS last boot time on the SUT (to verify successful restart).																										
d. Perform a graceful restart of the SUT via Host OS.																										
e. Verify that the SUT is in S0/MeOn (CM0,CM0-PG).																										
f. Verify the Host OS last boot time on the SUT does not match the boot time recorded before the restart.																										
If a failure occurs at any point during the flow above (including during any additional applicable sub-steps), the remainder of the steps related to the sub-test, may be skipped.																										
Regardless of the prior sub-test overall results, before beginning the next sub-test, attempt to bring the SUT to a base state via the following:																										
a. Verify that the SUT is in S0/MeOn (CM0,CM0-PG).																										
b. Verify that the Host OS on the SUT is available.																										
c. Verify that Intel® AMT on the SUT responds to version queries via the WLAN network interface.																										
If any of base state verification steps above fail, perform the following as an attempt to recover the SUT before attempting the base state verification steps above one last time.																										
a. Bring the system to G3 and wait 10 seconds.																										
b. Set system power configuration to AC/DC and wait another 10 seconds.																										
c. Briefly press the Power Button on the SUT.																										
12. Set the SUT to DC-only power and repeat steps 2 through 11. Verify that the relevant power flow operations match the table in step 6 for both Power Package 1 (Link Policy 2) and Power Package 2 (Link Policy 3) respectively.																										
† In the case of Power Package 1 configuration or DC-only power configuration testing, the SUT enter the relative Deep Sx state when the BIOS has enabled Deep Sx.																										
Pass Criteria:	The test passes if Intel® PETS confirms each test step succeeded.																									
References:	For details on Remote Control Operations, refer the <i>Intel® ME BIOS Specification</i> as well as the <i>Intel® AMT and Wake On Wireless LAN Coexistence</i> feature overview.																									

11.6.9 Remote Power Control via Intel® AMT WLAN Network Interface for Non-Mobile Systems Supporting Wake On Wireless LAN

ID:	AMT_027					
Title:	Remote Power Control via Intel® AMT WLAN Network Interface for Non-Mobile Systems supporting Wake on Wireless LAN					
Requirement:	Mandatory - exempt for systems that do not support Wake on Wireless LAN					
System:	Form Factor		System Power Model	Intel® AMT Network Interface		LAN Type
	<input checked="" type="checkbox"/> Desktop <input type="checkbox"/> Mobile	<input checked="" type="checkbox"/> Workstation	<input checked="" type="checkbox"/> Standard <input type="checkbox"/> Modern Standby or InstantGo*	<input type="checkbox"/> LAN <input checked="" type="checkbox"/> WLAN	<input type="checkbox"/> Either Used <input type="checkbox"/> Not Used	<input type="checkbox"/> Integrated LAN <input type="checkbox"/> Discrete LAN <input type="checkbox"/> TBT Dock LAN



ID:	AMT_027																									
Method:	Automated by Intel® PETS																									
Description:	An Intel® AMT compliant system supports the following remote control operations: <ul style="list-style-type: none">• Reset• Power-Up• Power-Down• Power-Cycle																									
Objective:	Verify that the remote control management features of the Intel® AMT platform meet the requirements. Intel® AMT enables remote management of the platform, including the capability to control platform power states (reset, power-on/off/cycle). This test verifies that the BIOS has been properly enabled to support these usage models.																									
Setup:	The initial state of the SUT should be S0/MeOn with Host OS running. Intel® AMT should be provisioned via manual mode. NOTE: In order to fully implement Wake on Wireless LAN (WoWLAN) in Sx states, the host BIOS must set HOST_WLAN_PP_EN. For more further details, refer the PCH <i>External Design Specification (EDS)</i> and the PCH <i>Platform Design Guide (PDG)</i> . Failure to properly set the HOST_WLAN_PP_EN bit may result in failures for this test.																									
Procedure:	<div><div><div>1. Set the active power package on the SUT to Power Package 1 (Intel® ME on in S0).</div><div>2. Set the Intel® AMT WLAN link policy on the SUT to Link Policy 2 (Enabled in S0).</div><div>3. Ensure the Host OS Wake on Wireless LAN is enabled.</div><div>4. Verify that Intel® AMT is available via WLAN by requesting its version.</div><div>5. Perform the following remote control operations across the given power states:</div></div><table><tr><th>SUT Initial state</th><th>Reset</th><th>Power-Cycle</th><th>Power-Up</th><th>Power-Down</th></tr><tr><td>S0-></td><td>S0</td><td>S0</td><td>N/A</td><td>S5/DS5[†]</td></tr><tr><td>S3-></td><td>N/A</td><td>S0</td><td>S0</td><td>S5/DS5[†]</td></tr><tr><td>S4-></td><td>N/A</td><td>N/A</td><td>N/A</td><td>N/A</td></tr><tr><td>S5-></td><td>N/A</td><td>N/A</td><td>N/A</td><td>N/A</td></tr></table><div><div>Each flow in the table above is executed as if they are part of an independent sub-test.</div><div>6. Verify that the relevant power flow operation succeeded for each flow in the table above. Additionally, for applicable Reset, Power-Cycle, and Power-Down flows, perform the following additional sub-steps for two (2) cycles each after the remote control operation has completed:<ul style="list-style-type: none">a. If shutdown, briefly press the Power Button on the SUT.b. Verify that the Host OS on the SUT is available.c. Record the Host OS last boot time on the SUT (to verify successful restart).d. Perform a graceful restart of the SUT via Host OS.e. Verify that the SUT is in S0/MeOn (CM0,CM0-PG).f. Verify the Host OS last boot time on the SUT does not match the boot time recorded before the restart.</div><div>If a failure occurs at any point during the flow above (including during any additional applicable sub-steps), the remainder of the steps related to the sub-test, may be skipped.</div><div>Regardless of the prior sub-test overall results, before beginning the next sub-test, attempt to bring the SUT to a base state via the following:<ul style="list-style-type: none">a. Verify that the SUT is in S0/MeOn (CM0,CM0-PG).b. Verify that the Host OS on the SUT is available.c. Verify that Intel® AMT on the SUT responds to version queries via the WLAN network interface.</div><div>If any of base state verification steps above fail, perform the following as an attempt to recover the SUT before attempting the base state verification steps above one last time:<ul style="list-style-type: none">a. Bring the system to G3 and wait 10 seconds.b. Set system power configuration to AC/DC and wait another 10 seconds.c. Briefly press the Power Button on the SUT.</div></div></div>	SUT Initial state	Reset	Power-Cycle	Power-Up	Power-Down	S0->	S0	S0	N/A	S5/DS5 [†]	S3->	N/A	S0	S0	S5/DS5 [†]	S4->	N/A	N/A	N/A	N/A	S5->	N/A	N/A	N/A	N/A
SUT Initial state	Reset	Power-Cycle	Power-Up	Power-Down																						
S0->	S0	S0	N/A	S5/DS5 [†]																						
S3->	N/A	S0	S0	S5/DS5 [†]																						
S4->	N/A	N/A	N/A	N/A																						
S5->	N/A	N/A	N/A	N/A																						



ID:	AMT_027																									
Procedure: (continued)	7. Set the active power package on the SUT to Power Package 2 (Intel® ME on in S0, wake in Sx/AC).																									
	8. Set the Intel® AMT WLAN link policy on the SUT to Link Policy 3 (Enabled in S0, Sx/AC).																									
	9. Perform the following remote control operations across the given power states:																									
	<table><tr><th>SUT Initial state</th><th>Reset</th><th>Power-Cycle</th><th>Power-Up</th><th>Power-Down</th></tr><tr><td>S0-></td><td>S0</td><td>S0</td><td>N/A</td><td>S5</td></tr><tr><td>S3-></td><td>N/A</td><td>S0</td><td>S0</td><td>S5</td></tr><tr><td>S4-></td><td>N/A</td><td>N/A</td><td>S0</td><td>N/A</td></tr><tr><td>S5-></td><td>N/A</td><td>N/A</td><td>S0</td><td>N/A</td></tr></table>	SUT Initial state	Reset	Power-Cycle	Power-Up	Power-Down	S0->	S0	S0	N/A	S5	S3->	N/A	S0	S0	S5	S4->	N/A	N/A	S0	N/A	S5->	N/A	N/A	S0	N/A
	SUT Initial state	Reset	Power-Cycle	Power-Up	Power-Down																					
	S0->	S0	S0	N/A	S5																					
	S3->	N/A	S0	S0	S5																					
	S4->	N/A	N/A	S0	N/A																					
	S5->	N/A	N/A	S0	N/A																					
	Each flow in the table above is executed as if they are part of an independent sub-test.																									
10. Verify that the relevant power flow operation succeeded for each flow in the table above. Additionally, for applicable Reset, Power-Cycle, and Power-Down flows in the chart above, perform the following additional sub-steps for two (2) cycles each after the remote control operation has completed:																										
a. If shutdown, briefly press the Power Button on the SUT.																										
b. Verify that the Host OS on the SUT is available.																										
c. Record the Host OS last boot time on the SUT (to verify successful restart).																										
d. Perform a graceful restart of the SUT via Host OS.																										
e. Verify that the SUT is in S0/MeOn (CM0,CM0-PG).																										
f. Verify the Host OS last boot time on the SUT does not match the boot time recorded before the restart.																										
If a failure occurs at any point during the flow above (including during any additional applicable sub-steps), the remainder of the steps related to the sub-test, may be skipped.																										
Regardless of the prior sub-test overall results, before beginning the next sub-test, attempt to bring the SUT to a base state via the following:																										
a. Verify that the SUT is in S0/MeOn (CM0,CM0-PG).																										
b. Verify that the Host OS on the SUT is available.																										
c. Verify that Intel® AMT on the SUT responds to version queries via the WLAN network interface.																										
If any of base state verification steps above fail, perform the following as an attempt to recover the SUT before attempting the base state verification steps above one last time.																										
a. Bring the system to G3 and wait 10 seconds.																										
b. Set system power configuration to AC/DC and wait another 10 seconds.																										
c. Briefly press the Power Button on the SUT.																										
† In the case of Power Package 1 configuration testing, the SUT enter the relative Deep Sx state when the BIOS has enabled Deep Sx.																										
Pass Criteria:	The test passes if Intel® PETS confirms each test step succeeded.																									
References:	For details on Remote Control Operations, refer the Intel® ME BIOS Specification as well as the Intel® AMT and Wake On Wireless LAN Coexistence feature overview.																									

11.6.10 Remote Power Control with Host OS Interaction via Intel® AMT LAN Network Interface

ID:	AMT_028			
Title:	Remote Power Control with Host OS interaction via Intel® AMT LAN Network Interface			
Requirement:	Mandatory			
System:	Form Factor	System Power Model	Intel® AMT Network Interface	LAN Type
	<input checked="" type="checkbox"/> Desktop <input checked="" type="checkbox"/> Workstation <input checked="" type="checkbox"/> Mobile	<input checked="" type="checkbox"/> Standard <input checked="" type="checkbox"/> Modern Standby or InstantGo*	<input checked="" type="checkbox"/> LAN <input type="checkbox"/> Either Used <input type="checkbox"/> WLAN <input type="checkbox"/> Not Used	<input checked="" type="checkbox"/> Integrated LAN <input type="checkbox"/> Discrete LAN <input type="checkbox"/> TBT Dock LAN
Method:	Automated by Intel® PETS			



ID:	AMT_028																									
Description:	An Intel® AMT compliant system supports the following remote control operations: <ul style="list-style-type: none">• Sleep• Hibernate• Graceful Power-Down• Graceful Power-Cycle																									
Objective:	Verify that the remote control management features of the Intel® AMT platform meet the requirements. Intel® AMT enables remote management of the platform, including the capability to control platform power states (Sleep, Hibernate, and graceful power-on/off/cycle). This test verifies that the system has been properly enabled to support these usage models.																									
Setup:	The initial state of the SUT should be S0/MeOn with Host OS running. Intel® AMT should be provisioned via manual mode. The Local Manageability Service (LMS), included with the Intel® ME software package, must be installed and running on the SUT.																									
Procedure:	<div><div><div>1. Ensure the system power configuration is set to AC/DC or AC-only.</div><div>2. Set the active power package on the SUT to Power Package 1 (Intel® ME on in S0).</div><div>3. Perform the following remote control operations across the given power states:</div></div><table><tr><th>SUT Initial state</th><th>Sleep</th><th>Hibernate</th><th>Graceful Power- Down</th><th>Graceful Power-Reset</th></tr><tr><td>S0-></td><td>S3</td><td>S4/DS4[†]</td><td>S5/DS5[†]</td><td>S0</td></tr><tr><td>S3-></td><td>N/A</td><td>N/A</td><td>N/A</td><td>N/A</td></tr><tr><td>S4-></td><td>N/A</td><td>N/A</td><td>N/A</td><td>N/A</td></tr><tr><td>S5-></td><td>N/A</td><td>N/A</td><td>N/A</td><td>N/A</td></tr></table><div><p>Each flow in the table above is executed as if they are part of an independent sub-test. In each independent sub-test, before issuing the remote control operation, query Intel® AMT on the SUT for up to 4 minutes at 30 second intervals to ensure that the intended graceful remote power state is available. In the case of Modern Standby or Microsoft Windows* InstantGo* mode, the Sleep test flows are skipped.</p><div><div>4. Verify that the relevant power flow operation succeeded for each flow in the table above.</div><div>If a failure occurs at any point during the flow above (including during any additional applicable sub-steps), the remainder of the steps related to the sub-test, may be skipped.</div><div>Regardless of the prior sub-test overall results, before beginning the next sub-test, attempt to bring the SUT to a base state via the following:</div><div><div>a. Verify that the SUT is in S0/MeOn (CM0,CM0-PG).</div><div>b. Verify that the Host OS on the SUT is available.</div><div>c. Verify that Intel® AMT on the SUT responds to version queries via the LAN network interface.</div></div><div>If any of base state verification steps above fail, perform the following as an attempt to recover the SUT before attempting the base state verification steps above one last time:</div><div><div>a. Bring the system to G3 and wait 10 seconds.</div><div>b. Set system power configuration to AC/DC and wait another 10 seconds.</div><div>c. Briefly press the Power Button on the SUT.</div></div></div></div></div>	SUT Initial state	Sleep	Hibernate	Graceful Power- Down	Graceful Power-Reset	S0->	S3	S4/DS4 [†]	S5/DS5 [†]	S0	S3->	N/A	N/A	N/A	N/A	S4->	N/A	N/A	N/A	N/A	S5->	N/A	N/A	N/A	N/A
SUT Initial state	Sleep	Hibernate	Graceful Power- Down	Graceful Power-Reset																						
S0->	S3	S4/DS4 [†]	S5/DS5 [†]	S0																						
S3->	N/A	N/A	N/A	N/A																						
S4->	N/A	N/A	N/A	N/A																						
S5->	N/A	N/A	N/A	N/A																						



ID:	AMT_028																									
<div>Procedure:</div> <div>(continued)</div>	<div>5. Set the active power package on the SUT to Power Package 2 (Intel® ME on in S0, wake in Sx/AC).</div> <div>6. Perform the following remote control operations across the given power states:</div> <table><tr><th>SUT Initial state</th><th>Sleep</th><th>Hibernate</th><th>Graceful Power- Down</th><th>Graceful Power-Reset</th></tr><tr><td>S0-></td><td>S3</td><td>S4</td><td>S5</td><td>S0</td></tr><tr><td>S3-></td><td>N/A</td><td>N/A</td><td>N/A</td><td>N/A</td></tr><tr><td>S4-></td><td>N/A</td><td>N/A</td><td>N/A</td><td>N/A</td></tr><tr><td>S5-></td><td>N/A</td><td>N/A</td><td>N/A</td><td>N/A</td></tr></table> <div>Each flow in the table above is executed as if they are part of an independent sub-test. In each independent sub-test, before issuing the remote control operation, query Intel® AMT on the SUT for up to 4 minutes at 30 second intervals to ensure that the intended graceful remote power state is available. In the case of Modern Standby or Microsoft Windows* InstantGo* mode, the Sleep test flows are skipped.</div> <div>7. Verify that the relevant power flow operation succeeded for each flow in the table above</div> <div>If a failure occurs at any point during the flow above (including during any additional applicable sub-steps), the remainder of the steps related to the sub-test, may be skipped.</div> <div>Regardless of the prior sub-test overall results, before beginning the next sub-test, attempt to bring the SUT to a base state via the following:</div> <div><div>a. Verify that the SUT is in S0/MeOn (CM0,CM0-PG).</div><div>b. Verify that the Host OS on the SUT is available.</div><div>c. Verify that Intel® AMT on the SUT responds to version queries via the LAN network interface.</div></div> <div>If any of base state verification steps above fail, perform the following as an attempt to recover the SUT before attempting the base state verification steps above one last time.</div> <div><div>a. Bring the system to G3 and wait 10 seconds.</div><div>b. Set system power configuration to AC/DC and wait another 10 seconds.</div><div>c. Briefly press the Power Button on the SUT.</div></div> <div>† In the case of Power Package 1 configuration testing, the SUT enter the relative Deep Sx state when the BIOS has enabled Deep Sx.</div>	SUT Initial state	Sleep	Hibernate	Graceful Power- Down	Graceful Power-Reset	S0->	S3	S4	S5	S0	S3->	N/A	N/A	N/A	N/A	S4->	N/A	N/A	N/A	N/A	S5->	N/A	N/A	N/A	N/A
	SUT Initial state	Sleep	Hibernate	Graceful Power- Down	Graceful Power-Reset																					
	S0->	S3	S4	S5	S0																					
	S3->	N/A	N/A	N/A	N/A																					
	S4->	N/A	N/A	N/A	N/A																					
S5->	N/A	N/A	N/A	N/A																						
Pass Criteria:	The test passes if Intel® PETS confirms each test step succeeded.																									
References:	For details on Remote Control Operations, refer the Intel® ME BIOS Specification.																									

11.6.11 Remote Power Control with Host OS Interaction via Intel® AMT WLAN Network Interface

ID:	AMT_029					
Title:	Remote Power Control with Host OS interaction via Intel® AMT WLAN Network Interface					
Requirement:	Mandatory					
System:	Form Factor		System Power Model	Intel® AMT Network Interface		LAN Type
	<input checked="" type="checkbox"/> Desktop <input checked="" type="checkbox"/> Workstation <input checked="" type="checkbox"/> Mobile	<input checked="" type="checkbox"/> Standard <input checked="" type="checkbox"/> Modern Standby or InstantGo*	<input type="checkbox"/> LAN <input checked="" type="checkbox"/> WLAN	<input type="checkbox"/> Either Used <input type="checkbox"/> Not Used	<input type="checkbox"/> Integrated LAN <input type="checkbox"/> Discrete LAN <input type="checkbox"/> TBT Dock LAN	
Method:	Automated by Intel® PETS					
Description:	An Intel® AMT compliant system supports the following remote control operations: <ul style="list-style-type: none">• Sleep• Hibernate• Graceful Power-Down• Graceful Power-Cycle					
Objective:	Verify that the remote control management features of the Intel® AMT platform meet the requirements. Intel® AMT enables remote management of the platform, including the capability to control platform power states (Sleep, Hibernate, and graceful power-on/off/cycle). This test verifies that the system has been properly enabled to support these usage models.					



ID:	AMT_029																									
Setup:	The initial state of the SUT should be S0/MeOn with Host OS running. Intel® AMT should be provisioned via manual mode. The Local Manageability Service (LMS), included with the Intel® ME software package, must be installed and running on the SUT.																									
Procedure:	<div><div><div>1. Ensure the system power configuration is set to AC/DC or AC-only.</div><div>2. Set the active power package on the SUT to Power Package 1 (Intel® ME on in S0).</div><div>3. Set the Intel® AMT WLAN link policy on the SUT to Link Policy 2 (Enabled in S0).</div><div>4. Ensure the Host OS Wake on Wireless LAN is disabled.</div><div>5. Verify that Intel® AMT is available via WLAN by requesting its version.</div><div>6. Perform the following remote control operations across the given power states:</div></div><table><tr><th>SUT Initial state</th><th>Sleep</th><th>Hibernate</th><th>Graceful Power- Down</th><th>Graceful Power-Reset</th></tr><tr><td>S0-></td><td>S3</td><td>S4/DS4[†]</td><td>S5/DS5[†]</td><td>S0</td></tr><tr><td>S3-></td><td>N/A</td><td>N/A</td><td>N/A</td><td>N/A</td></tr><tr><td>S4-></td><td>N/A</td><td>N/A</td><td>N/A</td><td>N/A</td></tr><tr><td>S5-></td><td>N/A</td><td>N/A</td><td>N/A</td><td>N/A</td></tr></table><div><p>Each flow in the table above is executed as if they are part of an independent sub-test. In each independent sub-test, before issuing the remote control operation, query Intel® AMT on the SUT for up to 4 minutes at 30 second intervals to ensure that the intended graceful remote power state is available. In the case of Modern Standby or Microsoft Windows* InstantGo* mode, the Sleep test flows are skipped.</p><div><div>7. Verify that the relevant power flow operation succeeded for each flow in the table above.</div><div><p>If a failure occurs at any point during the flow above (including during any additional applicable sub-steps), the remainder of the steps related to the sub-test, may be skipped.</p><p>Regardless of the prior sub-test overall results, before beginning the next sub-test, attempt to bring the SUT to a base state via the following:</p><div><div>a. Verify that the SUT is in S0/MeOn (CM0,CM0-PG).</div><div>b. Verify that the Host OS on the SUT is available.</div><div>c. Verify that Intel® AMT on the SUT responds to version queries via the WLAN network interface.</div></div><p>If any of base state verification steps above fail, perform the following as an attempt to recover the SUT before attempting the base state verification steps above one last time:</p><div><div>a. Bring the system to G3 and wait 10 seconds.</div><div>b. Set system power configuration to AC/DC and wait another 10 seconds.</div><div>c. Briefly press the Power Button on the SUT.</div></div></div></div></div></div>	SUT Initial state	Sleep	Hibernate	Graceful Power- Down	Graceful Power-Reset	S0->	S3	S4/DS4 [†]	S5/DS5 [†]	S0	S3->	N/A	N/A	N/A	N/A	S4->	N/A	N/A	N/A	N/A	S5->	N/A	N/A	N/A	N/A
	SUT Initial state	Sleep	Hibernate	Graceful Power- Down	Graceful Power-Reset																					
	S0->	S3	S4/DS4 [†]	S5/DS5 [†]	S0																					
	S3->	N/A	N/A	N/A	N/A																					
	S4->	N/A	N/A	N/A	N/A																					
	S5->	N/A	N/A	N/A	N/A																					



ID:	AMT_029																									
Procedure: (continued)	8. Set the active power package on the SUT to Power Package 2 (Intel® ME on in S0, wake in Sx/AC).																									
	9. Set the Intel® AMT WLAN link policy on the SUT to Link Policy 3 (Enabled in S0, Sx/AC).																									
	10. Perform the following remote control operations across the given power states:																									
	<table><tr><th>SUT Initial state</th><th>Sleep</th><th>Hibernate</th><th>Graceful Power- Down</th><th>Graceful Power-Reset</th></tr><tr><td>S0-></td><td>S3</td><td>S4</td><td>S5</td><td>S0</td></tr><tr><td>S3-></td><td>N/A</td><td>N/A</td><td>N/A</td><td>N/A</td></tr><tr><td>S4-></td><td>N/A</td><td>N/A</td><td>N/A</td><td>N/A</td></tr><tr><td>S5-></td><td>N/A</td><td>N/A</td><td>N/A</td><td>N/A</td></tr></table>	SUT Initial state	Sleep	Hibernate	Graceful Power- Down	Graceful Power-Reset	S0->	S3	S4	S5	S0	S3->	N/A	N/A	N/A	N/A	S4->	N/A	N/A	N/A	N/A	S5->	N/A	N/A	N/A	N/A
	SUT Initial state	Sleep	Hibernate	Graceful Power- Down	Graceful Power-Reset																					
S0->	S3	S4	S5	S0																						
S3->	N/A	N/A	N/A	N/A																						
S4->	N/A	N/A	N/A	N/A																						
S5->	N/A	N/A	N/A	N/A																						
Each flow in the table above is executed as if they are part of an independent sub-test. In each independent sub-test, before issuing the remote control operation, query Intel® AMT on the SUT for up to 4 minutes at 30 second intervals to ensure that the intended graceful remote power state is available. In the case of Modern Standby or Microsoft Windows* InstantGo* mode, the Sleep test flows are kipped.																										
11. Verify that the relevant power flow operation succeeded for each flow in the table above.																										
If a failure occurs at any point during the flow above (including during any additional applicable sub-steps), the remainder of the steps related to the sub-test, may be skipped.																										
Regardless of the prior sub-test overall results, before beginning the next sub-test, attempt to bring the SUT to a base state via the following:																										
a. Verify that the SUT is in S0/MeOn (CM0,CM0-PG).																										
b. Verify that the Host OS on the SUT is available.																										
c. Verify that Intel® AMT on the SUT responds to version queries via the WLAN network interface.																										
If any of base state verification steps above fail, perform the following as an attempt to recover the SUT before attempting the base state verification steps above one last time.																										
a. Bring the system to G3 and wait 10 seconds.																										
b. Set system power configuration to AC/DC and wait another 10 seconds.																										
c. Briefly press the Power Button on the SUT.																										
† In the case of Power Package 1 configuration testing, the SUT enter the relative Deep Sx state when the BIOS has enabled Deep Sx.																										
Pass Criteria:	The test passes if Intel® PETS confirms each test step succeeded.																									
References:	For details on Remote Control Operations, refer the Intel® ME BIOS Specification.																									

11.7 Serial-Over-LAN and Storage Redirection

The section serves as a checklist for the environment setup and covers integration testing of the Serial-Over-LAN and Storage Redirection features in Intel® AMT.

11.7.1 Test Environment

The System Under Test (SUT) is to be configured with Intel® AMT set in manual provisioning mode with static IP address or DHCP. The management console may be a laptop or a desktop with a version of Microsoft Windows* supported by Intel® PETS, and the SUT should have a version of Microsoft Windows* supported by Intel® PETS as well. The test network is comprised of a hub/switch and network cables.

Tools for testing:

- Intel® PETS: The latest version of the tool from the Intel® CSME Compliancy and Debug kit release. Refer the Intel® PETS User Guide for exact instructions on how to load and setup the Intel® PETS software.
- Intel® Automated Power Switch (Intel® APS): The SUT should be connected to an Intel® APS 3 unit. In case an Intel® APS 3 is not available, select the Manual configuration in the Intel® PETS SUT profile configuration menu.
- Intel® PETS Local Agent: The local agent must be installed on the SUT.



In order for Intel® PETS to work properly, ensure the following:

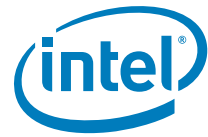
- the SUT has a valid System UUID. This can be checked by confirming a non-zero value is reported by the Intel® MEInfo tool.
- the firmware image is configured to **not** require user consent on redirection. This can be done by checking the following value of the SPI image via the Intel® FIT tool in the 'Intel(R) AMT' tab: 'Redirection Configuration' | 'Redirection Privacy / Security Level' set to "Default".

Where applicable, the wireless LAN interface on Intel® AMT must be on a different network/subnet than the wired LAN interface. For details on how to enter the network interface details into Intel® PETS, consult the Intel® PETS User Guide.

If the firmware image or the SUT configuration does not support some features, Intel® PETS show those features as failing when tested. Intel® PETS cannot determine in all cases which features have been deactivated and should thus be skipped during testing.

11.7.2 SOL Redirection and BIOS Setup Boot Option over Intel® AMT LAN

ID:	AMT_030				
Title:	Serial-Over-LAN (SOL) Redirection and BIOS Setup Boot Option over Intel® AMT LAN Network Interface				
Requirement:	Mandatory - exempt for systems that do not support the BIOS Setup boot option				
System:	<div><div>Form Factor</div><div><input checked="" type="checkbox"/> Desktop <input checked="" type="checkbox"/> Workstation <input checked="" type="checkbox"/> Mobile</div></div>	<div><div>System Power Model</div><div><input checked="" type="checkbox"/> Standard <input checked="" type="checkbox"/> Modern Standby or InstantGo*</div></div>	<div><div>Intel® AMT Network Interface</div><div><input checked="" type="checkbox"/> LAN <input type="checkbox"/> Either Used <input type="checkbox"/> WLAN <input type="checkbox"/> Not Used</div></div>	<div><div>LAN Type</div><div><input checked="" type="checkbox"/> Integrated LAN <input type="checkbox"/> Discrete LAN <input type="checkbox"/> TBT Dock LAN</div></div>	
Method:	Automated by Intel® PETS with test operator interaction				
Description:	An Intel® AMT compliant system implements BIOS boot screen redirection according to the boot options received from the GetBootOptions command.				
Objective:	<p>Verify that the BIOS detects, and executes, a request (by means of boot options) to redirect text to the management console via SOL.</p> <p>Intel® AMT enables remote management of the platform, including providing capabilities to read the boot options sent from the management console. These boot options can include commands to send display text from the Intel® AMT platform to the remote console by means of Serial-Over-LAN functionality. Testing described in this section verify that BIOS has been properly enabled to support these usage models.</p>				
Setup:	<p>The initial state of the SUT should be S0/MeOn with Host OS running. Intel® AMT should be provisioned via manual mode. Before running this test, ensure that SOL is enabled in the Intel® MEBX.</p> <p>The default number of rows shown in the Putty terminal window may differ from the number of rows displayed by the BIOS. When this occurs, the Putty terminal display incur line wrapping problems. To avoid this problem, change the settings of the Putty application to align with the BIOS via the following steps:</p> <ol style="list-style-type: none">1. Open the ".\Intel(R) Platform Enablement Test Suite\Plugins\Me\Redirection\bin\" directory.2. Start putty.exe, and in the Category section:<ol style="list-style-type: none">a. Select Window, and change the Rows value to the required number of rows.b. Select Session, then select <i>Default Settings</i>, and finally click the Save button.3. Close the Putty Configuration window.4. To confirm, start putty.exe again, and make sure Row number is set to the new value.				



ID:	AMT_030
Procedure:	<ol style="list-style-type: none"> 1. Set the active power package on the SUT to Power Package 2 (Intel® ME on in S0, wake in Sx/AC). 2. Check that the SUT supports booting into BIOS by querying the Intel® AMT and checking the boot capabilities. <ol style="list-style-type: none"> a. If supported, use Intel® AMT to set the BIOS Setup boot option on the SUT for the next boot. b. If not supported, end the test and request the test operator to confirm the BIOS support of 'BIOS Setup' OEMCapabilities1 setting provided to the Intel® ME via the SMBIOS Type 130 table. 3. Ensure the Intel® AMT redirection ports are enabled on the SUT. 4. Cancel any existing Intel® AMT user consent session which may be active on the SUT. 5. Ensure the Intel® AMT user consent opt-in setting is disabled on the SUT. 6. Use Intel® AMT to set the SUT boot options to use SOL Redirection on the next boot.
Procedure: (continued)	<ol style="list-style-type: none"> 7. Close any open SOL Redirection session with the SUT via Intel® AMT. The remaining steps within this block is executed as if they are part of an independent sub-test. If a failure occurs at any point during the flow below, the remainder of the steps related to the sub-test, may be skipped. 8. Inform the test operator that a system boot is performed by Intel® PETS requesting that the BIOS boot into the BIOS setup menu. 9. Gracefully shutdown to S5/MeOn the SUT via the Host OS and then wait 10 seconds. 10. Open a SOL Redirection session with the SUT via Intel® AMT using the Putty terminal program on the management console. 11. Perform a Remote Power-Up of the SUT via Intel® AMT. 12. Request the test operator to: <ol style="list-style-type: none"> a. confirm that the BIOS setup screen of the SUT is displayed in the Putty window. b. confirm that remote keyboard is working properly.
Procedure: (continued)	<ol style="list-style-type: none"> 13. Close any open SOL Redirection session with the SUT via Intel® AMT. 14. Close any Putty terminal window which may still be open. 15. Perform a Remote Reset of the SUT via Intel® AMT.
Pass Criteria:	The test passes if Intel® PETS indicates all steps have passed successfully.
References:	For details on SOL and ASF Boot Options, refer the <i>Intel® ME BIOS Specification</i> .

11.7.3 SOL Redirection and BIOS Setup Boot Option over Intel® AMT WLAN Network Interface

ID:	AMT_031			
Title:	Serial-Over-LAN (SOL) Redirection and BIOS Setup Boot Option over Intel® AMT WLAN Network Interface			
Requirement:	Mandatory - exempt for systems that do not support the BIOS Setup boot option			
System:	Form Factor	System Power Model	Intel® AMT Network Interface	LAN Type
	<input checked="" type="checkbox"/> Desktop <input checked="" type="checkbox"/> Workstation <input checked="" type="checkbox"/> Mobile	<input checked="" type="checkbox"/> Standard <input checked="" type="checkbox"/> Modern Standby or InstantGo*	<input type="checkbox"/> LAN <input type="checkbox"/> Either Used <input checked="" type="checkbox"/> WLAN <input type="checkbox"/> Not Used	<input type="checkbox"/> Integrated LAN <input type="checkbox"/> Discrete LAN <input type="checkbox"/> TBT Dock LAN
Method:	Automated by Intel® PETS with test operator interaction			
Description:	An Intel® AMT compliant system implements BIOS boot screen redirection according to the boot options received from the GetBootOptions command.			
Objective:	Verify that the BIOS detects, and executes, a request (by means of boot options) to redirect text to the management console (SOL). Before running this test, ensure that SOL is enabled in the Intel® MEBX. Intel® AMT enables remote management of the platform, including providing capabilities to read the boot options sent from the management console. These boot options can include commands to send display text from the Intel® AMT platform to the remote console by means of Serial-Over-LAN functionality. Testing described in this section verify that BIOS has been properly enabled to support these usage models.			

ID:	AMT_031
Setup:	<p>The initial state of the SUT should be S0/MeOn with Host OS running. Intel® AMT should be provisioned via manual mode.</p> <p>The default number of rows shown in the Putty terminal window may differ from the number of rows displayed by the BIOS. When this occurs, the Putty terminal display incur line wrapping problems. To avoid this problem, change the settings of the Putty application to align with the BIOS via the following steps:</p> <ol style="list-style-type: none"> 1. Open the ".\Intel(R) Platform Enablement Test Suite\Plugins\Me\Redirection\bin\" directory. 2. Start putty.exe, and in the Category section: <ol style="list-style-type: none"> a. Select Window, and change the Rows value to the required number of rows. b. Select Session, then select <i>Default Settings</i>, and finally click the Save button. 3. Close the Putty Configuration window. 4. To confirm, start putty.exe again, and make sure Row number is set to the new value.
Procedure:	<ol style="list-style-type: none"> 1. Set the active power package on the SUT to Power Package 2 (Intel® ME on in S0, wake in Sx/AC). 2. Check that the SUT supports booting into BIOS by querying the Intel® AMT and checking the boot capabilities. <ol style="list-style-type: none"> a. If supported, use Intel® AMT to set the BIOS Setup boot option on the SUT for the next boot. b. If not supported, end the test and request the test operator to confirm the BIOS support of 'BIOS Setup' OEMCapabilities1 setting provided to the Intel® ME via the SMBIOS Type 130 table. 3. Set the Intel® AMT WLAN link policy on the SUT to Link Policy 3 (Enabled in S0, Sx/AC). 4. Ensure the TCP maximum data retransmission setting defined in the SUT profile is applied to both a) the management console, and b) the SUT via Intel® AMT. <p>If the configuration on the management console is not already aligned to the SUT profile setting, the network stack on the management console need to be reset; leading to potential network connectivity loss for other applications on the system.</p> <p>Before synchronizing the setting on the management console, provide a warning to the test operator, with the option to proceed or cancel, indicating the TCP maximum data retransmission network setting is about to be changed and that it may be necessary to re-establish network connectivity for any other applications running on the management console. If the test operator chooses to cancel, the test step is marked as failed.</p> 5. Ensure the Intel® AMT redirection ports are enabled on the SUT. 6. Cancel any existing Intel® AMT user consent session which may be active on the SUT. 7. Ensure the Intel® AMT user consent opt-in setting is disabled on the SUT. 8. Use Intel® AMT to set the SUT boot options to use SOL Redirection on the next boot.
Procedure: (continued)	<ol style="list-style-type: none"> 9. Close any open SOL Redirection session with the SUT via Intel® AMT. <p>The remaining steps within this block is executed as if they are part of an independent sub-test. If a failure occurs at any point during the flow below, the remainder of the steps related to the sub-test, may be skipped.</p> 10. Inform the test operator that a system boot is performed by Intel® PETS requesting that the BIOS boot into the BIOS setup menu. 11. Gracefully shutdown to S5/MeOn the SUT via the Host OS and then wait 10 seconds. 12. Verify that Intel® AMT is available via WLAN by requesting its version. 13. Open a SOL Redirection session with the SUT via Intel® AMT using the Putty terminal program on the management console. 14. Perform a Remote Power-Up of the SUT via Intel® AMT. 15. Request the test operator to: <ol style="list-style-type: none"> a. confirm that the BIOS setup screen of the SUT is displayed in the Putty window. b. confirm that remote keyboard is working properly.
Procedure: (continued)	<ol style="list-style-type: none"> 16. Close any open SOL Redirection session with the SUT via Intel® AMT. 17. Close any Putty terminal window which may still be open. 18. Perform a Remote Reset of the SUT via Intel® AMT.
Pass Criteria:	The test passes if Intel® PETS indicates all steps have passed successfully.
References:	For details on SOL and ASF Boot Options, refer the <i>Intel® ME BIOS Specification</i> .

11.7.4 SOL and Storage Redirection over Intel® AMT LAN Network Interface

ID:	AMT_032
Title:	Serial-Over-LAN (SOL) and Storage Redirection over Intel® AMT LAN Network Interface



ID:	AMT_032			
Requirement:	Mandatory			
System:	Form Factor <input checked="" type="checkbox"/> Desktop <input checked="" type="checkbox"/> Workstation <input checked="" type="checkbox"/> Mobile	System Power Model <input checked="" type="checkbox"/> Standard <input checked="" type="checkbox"/> Modern Standby or InstantGo*	Intel® AMT Network Interface <input checked="" type="checkbox"/> LAN <input type="checkbox"/> Either Used <input type="checkbox"/> WLAN <input type="checkbox"/> Not Used	LAN Type <input checked="" type="checkbox"/> Integrated LAN <input type="checkbox"/> Discrete LAN <input type="checkbox"/> TBT Dock LAN
Method:	Automated by Intel® PETS with test operator interaction			
Description:	An Intel® AMT compliant system implements SOL and Storage Redirection according to the boot options received from the GetBootOptions command.			
Objective:	<p>Verify that the BIOS detects, and executes, a request (by means of boot options) to redirect text to the management console via SOL and perform Storage Redirection to an ISO OS image.</p> <p>Intel® AMT enables remote management of the platform, including providing capabilities to read the boot options sent from the management console. These boot options can include commands to send display text from the Intel® AMT platform to the remote console by means of SOL functionality and to redirect the default platform boot device via Storage Redirection. Testing described in this section verify that BIOS has been properly enabled to support these usage models.</p>			
Setup:	The initial state of the SUT should be S0/MeOn with Host OS running. Intel® AMT should be provisioned via manual mode. Before running this test, ensure that SOL and Storage Redirection are enabled in the Intel® MEBX.			
Procedure:	<ol style="list-style-type: none"> 1. Set the active power package on the SUT to Power Package 2 (Intel® ME on in S0, wake in Sx/AC). 2. Ensure the Intel® AMT redirection ports are enabled on the SUT. 3. Cancel any existing Intel® AMT user consent session which may be active on the SUT. 4. Ensure the Intel® AMT user consent opt-in setting is disabled on the SUT. 5. Use Intel® AMT to set the SUT boot options to use SOL and Storage Redirection Boot on the next boot. 			
Procedure: (continued)	<ol style="list-style-type: none"> 6. Close any open SOL and Storage Redirection session(s) with the SUT via Intel® AMT. The remaining steps within this block is executed as if they are part of an independent sub-test. If a failure occurs at any point during the flow below, the remainder of the steps related to the sub-test, may be skipped. 7. Inform the test operator that a system boot is performed by Intel® PETS requesting that the BIOS boot to a redirected ISO OS image via Serial-Over-LAN. 8. Gracefully shutdown to S5/MeOn the SUT via the Host OS and then wait 10 seconds. 9. Open a SOL Redirection session with the SUT via Intel® AMT using the Putty terminal program on the management console. 10. Open a Storage Redirection session with the SUT via Intel® AMT using an ISO OS image on the management console. 11. Perform a Remote Power-Up of the SUT via Intel® AMT. 12. Request the test operator to confirm that SUT boots from redirected ISO OS image. 			
Procedure: (continued)	<ol style="list-style-type: none"> 13. Close any open SOL and Storage Redirection session(s) with the SUT via Intel® AMT. 14. Close any Putty terminal window which may still be open. 15. Request the test operator to: <ol style="list-style-type: none"> a. gracefully reboot the SUT, b. enter the Intel® MEBX on the SUT and disable both SOL and Storage Redirection, and c. boot the SUT to Host OS. 16. Gracefully shutdown to S5/MeOn the SUT via the Host OS and then wait 10 seconds. 17. Attempt to open a SOL Redirection session with the SUT via Intel® AMT using the Putty terminal program on the management console. Note that failure to open the session by error indicating the SOL interface is disabled indicates success for the test step, otherwise the test step fails. 18. Attempt to open a Storage Redirection session with the SUT via Intel® AMT using an ISO OS image on the management console. Note that failure to open the session by error indicating the Storage Redirection interface is disabled indicates success for the test step, otherwise the test step fails. 19. Request the test operator to: <ol style="list-style-type: none"> a. boot the SUT, b. enter the Intel® MEBX on the SUT and enable both SOL and Storage Redirection, and c. boot the SUT to Host OS. 			
Pass Criteria:	The test passes if Intel® PETS indicates all steps have passed successfully.			
References:	For details on SOL and Storage Redirection, refer the <i>Intel® ME BIOS Specification</i> .			



11.7.5 SOL and Storage Redirection over Intel® AMT WLAN Network Interface

ID:	AMT_033			
Title:	Serial-Over-LAN (SOL) and Storage Redirection over Intel® AMT WLAN Network Interface			
Requirement:	Mandatory			
System:	Form Factor <input checked="" type="checkbox"/> Desktop <input checked="" type="checkbox"/> Workstation <input checked="" type="checkbox"/> Mobile	System Power Model <input checked="" type="checkbox"/> Standard <input checked="" type="checkbox"/> Modern Standby or InstantGo*	Intel® AMT Network Interface <input type="checkbox"/> LAN <input type="checkbox"/> Either Used <input checked="" type="checkbox"/> WLAN <input type="checkbox"/> Not Used	LAN Type <input type="checkbox"/> Integrated LAN <input type="checkbox"/> Discrete LAN <input type="checkbox"/> TBT Dock LAN
Method:	Automated by Intel® PETS with test operator interaction			
Description:	An Intel® AMT compliant system implements SOL and Storage Redirection according to the boot options received from the GetBootOptions command.			
Objective:	<p>Verify that the BIOS detects, and executes, a request (by means of boot options) to redirect text to the management console via SOL and perform Storage Redirection to an ISO OS image.</p> <p>Intel® AMT enables remote management of the platform, including providing capabilities to read the boot options sent from the management console. These boot options can include commands to send display text from the Intel® AMT platform to the remote console by means of SOL functionality and to redirect the default platform boot device via Storage Redirection. Testing described in this section verify that BIOS has been properly enabled to support these usage models.</p>			
Setup:	The initial state of the SUT should be S0/MeOn with Host OS running. Intel® AMT should be provisioned via manual mode. Before running this test, ensure that SOL and Storage Redirection are enabled in the Intel® MEBX.			
Procedure:	<ol style="list-style-type: none"> Set the active power package on the SUT to Power Package 2 (Intel® ME on in S0, wake in Sx/AC). Set the Intel® AMT WLAN link policy on the SUT to Link Policy 3 (Enabled in S0, Sx/AC). Ensure the TCP maximum data retransmission setting defined in the SUT profile is applied to both a) the management console, and b) the SUT via Intel® AMT. If the configuration on the management console is not already aligned to the SUT profile setting, the network stack on the management console need to be reset; leading to potential network connectivity loss for other applications on the system. Before synchronizing the setting on the management console, provide a warning to the test operator, with the option to proceed or cancel, indicating the TCP maximum data retransmission network setting is about to be changed and that it may be necessary to re-establish network connectivity for any other applications running on the management console. If the test operator chooses to cancel, the test step is marked as failed. Ensure the Intel® AMT redirection ports are enabled on the SUT. Cancel any existing Intel® AMT user consent session which may be active on the SUT. Ensure the Intel® AMT user consent opt-in setting is disabled on the SUT. Use Intel® AMT to set the SUT boot options to use SOL and Storage Redirection Boot on the next boot. 			
Procedure: (continued)	<ol style="list-style-type: none"> Close any open SOL and Storage Redirection session(s) with the SUT via Intel® AMT. The remaining steps within this block is executed as if they are part of an independent sub-test. If a failure occurs at any point during the flow below, the remainder of the steps related to the sub-test, may be skipped. Inform the test operator that a system boot is performed by Intel® PETS requesting that the BIOS boot to a redirected ISO OS image via Serial-Over-LAN. Gracefully shutdown to S5/MeOn the SUT via the Host OS and then wait 10 seconds. Verify that Intel® AMT is available via WLAN by requesting its version. Open a SOL Redirection session with the SUT via Intel® AMT using the Putty terminal program on the management console. Open a Storage Redirection session with the SUT via Intel® AMT using an ISO OS image on the management console. Perform a Remote Power-Up of the SUT via Intel® AMT. Request the test operator to confirm that SUT boots from redirected ISO OS image. 			



ID:	AMT_033
Procedure: (continued)	<p>16. Close any open SOL and Storage Redirection session(s) with the SUT via Intel® AMT.</p> <p>17. Close any Putty terminal window which may still be open.</p> <p>18. Request the test operator to:</p> <ol style="list-style-type: none"> gracefully reboot the SUT, enter the Intel® MEBX on the SUT and disable both SOL and Storage Redirection, and boot the SUT to Host OS. <p>19. Gracefully shutdown to S5/MeOn the SUT via the Host OS and then wait 10 seconds.</p> <p>20. Verify that Intel® AMT is available via WLAN by requesting its version.</p> <p>21. Attempt to open a SOL Redirection session with the SUT via Intel® AMT using the Putty terminal program on the management console. Note that failure to open the session by error indicating the SOL interface is disabled indicates success for the test step, otherwise the test step fails.</p> <p>22. Attempt to open a Storage Redirection session with the SUT via Intel® AMT using an ISO OS image on the management console. Note that failure to open the session by error indicating the Storage Redirection interface is disabled indicates success for the test step, otherwise the test step fails.</p> <p>23. Request the test operator to:</p> <ol style="list-style-type: none"> boot the SUT, enter the Intel® MEBX on the SUT and enable both SOL and Storage Redirection, and boot the SUT to Host OS.
Pass Criteria:	The test passes if Intel® PETS confirms each test step succeeded.
References:	For details on SOL and Storage Redirection, refer the <i>Intel® ME BIOS Specification</i> .

11.7.6 SOL and Storage Redirection over Intel® AMT LAN Network Interface with User Consent Enabled

ID:	AMT_034			
Title:	Serial-Over-LAN (SOL) and Storage Redirection over Intel® AMT LAN Network Interface with User Consent Enabled			
Requirement:	Mandatory			
System:	Form Factor <input checked="" type="checkbox"/> Desktop <input checked="" type="checkbox"/> Workstation <input checked="" type="checkbox"/> Mobile	System Power Model <input checked="" type="checkbox"/> Standard <input checked="" type="checkbox"/> Modern Standby or InstantGo*	Intel® AMT Network Interface <input checked="" type="checkbox"/> LAN <input type="checkbox"/> Either Used <input type="checkbox"/> WLAN <input type="checkbox"/> Not Used	LAN Type <input checked="" type="checkbox"/> Integrated LAN <input type="checkbox"/> Discrete LAN <input type="checkbox"/> TBT Dock LAN
	NOTE: Applies to systems with discrete graphics and also those with integrated graphics.			
Method:	Automated by Intel® PETS with test operator interaction			
Description:	An Intel® AMT compliant system implements SOL and Storage Redirection according to the boot options received from the GetBootOptions command. When user consent is enabled, a redirection session is allowed only after the user consent code is accepted by Intel® AMT.			
Objective:	<p>Verify that the BIOS detects, and executes, a request (by means of boot options) to redirect text to the management console via SOL and perform Storage Redirection to an ISO OS image.</p> <p>Intel® AMT enables remote management of the platform, including providing capabilities to read the boot options sent from the management console. These boot options can include commands to send display text from the Intel® AMT platform to the remote console by means of SOL functionality and to redirect the default platform boot device via Storage Redirection. Testing described in this section verify that BIOS has been properly enabled to support these usage models.</p>			
Setup:	The initial state of the SUT should be S0/MeOn with Host OS running. Intel® AMT should be provisioned via manual mode. Before running this test, ensure that SOL and Storage Redirection are enabled in the Intel® MEBX.			



ID:	AMT_034
Procedure:	<ol style="list-style-type: none"> 1. Set the active power package on the SUT to Power Package 2 (Intel® ME on in S0, wake in Sx/AC). 2. Ensure the Intel® AMT redirection ports are enabled on the SUT. 3. Cancel any existing Intel® AMT user consent session which may be active on the SUT. 4. Ensure the Intel® AMT user consent opt-in setting is enabled on the SUT. 5. Initiate a new Intel® AMT user consent session with the SUT. 6. In the case of integrated graphics: <ol style="list-style-type: none"> a. A user consent code is displayed on the SUT screen. b. Verify via Intel® AMT that the user consent opt-in state on the SUT is "Displayed". c. Request the test operator to enter the user consent code to the text box on the management console. d. Forward the user consent code to the SUT via Intel® AMT. In the case of discrete graphics: <ol style="list-style-type: none"> a. Perform a graceful restart of the SUT via Host OS. The SUT boot and halt in Intel® MEBX to display the user consent code. b. Verify via Intel® AMT that the user consent opt-in state on the SUT is "Displayed". c. Request the test operator to enter the user consent code to the text box on the management console. d. Forward the user consent code to the SUT via Intel® AMT. e. The SUT continue to boot to the Host OS. Note: It may be necessary to press ESC on the SUT to continue the boot process. f. Wait for the SUT to return to S0/MeOn with the Host OS running. 7. Use Intel® AMT to set the SUT boot options to use SOL and Storage Redirection Boot on the next boot.
Procedure: (continued)	<ol style="list-style-type: none"> 8. Close any open SOL and Storage Redirection session(s) with the SUT via Intel® AMT. The remaining steps within this block is executed as if they are part of an independent sub-test. If a failure occurs at any point during the flow below, the remainder of the steps related to the sub-test, may be skipped. 9. Inform the test operator that a system boot is performed by Intel® PETS requesting that the BIOS boot to a redirected ISO OS image via Serial-Over-LAN. 10. Gracefully shutdown to S5/MeOn the SUT via the Host OS and then wait 10 seconds. 11. Open a SOL Redirection session with the SUT via Intel® AMT using the Putty terminal program on the management console. 12. Open a Storage Redirection session with the SUT via Intel® AMT using an ISO OS image on the management console. 13. Perform a Remote Power-Up of the SUT via Intel® AMT. 14. Request the test operator to confirm that SUT boots from redirected ISO OS image.
Procedure: (continued)	<ol style="list-style-type: none"> 15. Close any open SOL and Storage Redirection session(s) with the SUT via Intel® AMT. 16. Close any Putty terminal window which may still be open. 17. Cancel any existing Intel® AMT user consent session which may be active on the SUT. 18. Perform a Remote Reset of the SUT via Intel® AMT.
Pass Criteria:	The test passes if Intel® PETS confirms each test step succeeded.
References:	For details on SOL and Storage Redirection, refer the <i>Intel® ME BIOS Specification</i> .

11.7.7 SOL and Storage Redirection over Intel® AMT WLAN Network Interface with User Consent Enabled

ID:	AMT_035			
Title:	Serial-Over-LAN (SOL) and Storage Redirection over Intel® AMT WLAN Network Interface with User Consent Enabled			
Requirement:	Mandatory			
System:	<div> <div>Form Factor</div> <div> <input checked="" type="checkbox"/> Desktop <input checked="" type="checkbox"/> Workstation <input checked="" type="checkbox"/> Mobile </div> </div>	<div> <div>System Power Model</div> <div> <input checked="" type="checkbox"/> Standard <input checked="" type="checkbox"/> Modern Standby or InstantGo* </div> </div>	<div> <div>Intel® AMT Network Interface</div> <div> <input type="checkbox"/> LAN <input type="checkbox"/> Either Used <input checked="" type="checkbox"/> WLAN <input type="checkbox"/> Not Used </div> </div>	<div> <div>LAN Type</div> <div> <input type="checkbox"/> Integrated LAN <input type="checkbox"/> Discrete LAN <input type="checkbox"/> TBT Dock LAN </div> </div>
	NOTE: Applies to systems with discrete graphics and also those with integrated graphics.			
Method:	Automated by Intel® PETS with test operator interaction.			



ID:	AMT_035
Description:	An Intel® AMT compliant system implements SOL and Storage Redirection according to the boot options received from the GetBootOptions command. When user consent is enabled, a redirection session is allowed only after the user consent code is accepted by Intel® AMT.
Objective:	<p>Verify that the BIOS detects, and executes, a request (by means of boot options) to redirect text to the management console via SOL and perform Storage Redirection to an ISO OS image.</p> <p>Intel® AMT enables remote management of the platform, including providing capabilities to read the boot options sent from the management console. These boot options can include commands to send display text from the Intel® AMT platform to the remote console by means of SOL functionality and to redirect the default platform boot device via Storage Redirection. Testing described in this section verify that BIOS has been properly enabled to support these usage models.</p>
Setup:	The initial state of the SUT should be S0/MeOn with Host OS running. Intel® AMT should be provisioned via manual mode. Before running this test, ensure that SOL and Storage Redirection are enabled in the Intel® MEBX.
Procedure:	<ol style="list-style-type: none"> Set the active power package on the SUT to Power Package 2 (Intel® ME on in S0, wake in Sx/AC). Set the Intel® AMT WLAN link policy on the SUT to Link Policy 3 (Enabled in S0, Sx/AC). Ensure the TCP maximum data retransmission setting defined in the SUT profile is applied to both a) the management console, and b) the SUT via Intel® AMT. If the configuration on the management console is not already aligned to the SUT profile setting, the network stack on the management console need to be reset; leading to potential network connectivity loss for other applications on the system. Before synchronizing the setting on the management console, provide a warning to the test operator, with the option to proceed or cancel, indicating the TCP maximum data retransmission network setting is about to be changed and that it may be necessary to re-establish network connectivity for any other applications running on the management console. If the test operator chooses to cancel, the test step is marked as failed. Ensure the Intel® AMT redirection ports are enabled on the SUT. Cancel any existing Intel® AMT user consent session which may be active on the SUT. Ensure the Intel® AMT user consent opt-in setting is enabled on the SUT. Initiate a new Intel® AMT user consent session with the SUT. In the case of integrated graphics: <ol style="list-style-type: none"> A user consent code is displayed on the SUT screen. Verify via Intel® AMT that the user consent opt-in state on the SUT is "Displayed". Request the test operator to enter the user consent code to the text box on the management console. Forward the user consent code to the SUT via Intel® AMT. In the case of discrete graphics: <ol style="list-style-type: none"> Perform a graceful restart of the SUT via Host OS. The SUT boot and halt in Intel® MEBX to display the user consent code. Verify via Intel® AMT that the user consent opt-in state on the SUT is "Displayed". Request the test operator to enter the user consent code to the text box on the management console. Forward the user consent code to the SUT via Intel® AMT. The SUT continues to boot to the Host OS. Note: It may be necessary to press ESC on the SUT to continue the boot process. Wait for the SUT to return to S0/MeOn with the Host OS running. Use Intel® AMT to set the SUT boot options to use SOL and Storage Redirection Boot on the next boot.
Procedure: (continued)	<ol style="list-style-type: none"> Close any open SOL and Storage Redirection session(s) with the SUT via Intel® AMT. The remaining steps within this block is executed as if they are part of an independent sub-test. If a failure occurs at any point during the flow below, the remainder of the steps related to the sub-test, may be skipped. Inform the test operator that a system boot is performed by Intel® PETS requesting that the BIOS boot to a redirected ISO OS image via Serial-Over-LAN. Gracefully shutdown to S5/MeOn the SUT via the Host OS and then wait 10 seconds. Verify that Intel® AMT is available via WLAN by requesting its version. Open a SOL Redirection session with the SUT via Intel® AMT using the Putty terminal program on the management console. Open a Storage Redirection session with the SUT via Intel® AMT using an ISO OS image on the management console. Perform a Remote Power-Up of the SUT via Intel® AMT. Request the test operator to confirm that SUT boots from redirected ISO OS image.
Procedure: (continued)	<ol style="list-style-type: none"> Close any open SOL and Storage Redirection session(s) with the SUT via Intel® AMT. Close any Putty terminal window which may still be open. Cancel any existing Intel® AMT user consent session which may be active on the SUT. Perform a Remote Reset of the SUT via Intel® AMT.



ID:	AMT_035
Pass Criteria:	The test passes if Intel® PETS confirms each test step succeeded.
References:	For details on SOL and Storage Redirection, refer the <i>Intel® ME BIOS Specification</i> .

11.7.8 SOL and Storage Redirection with Secure Boot

ID:	AMT_036								
Title:	Serial-Over-LAN (SOL) and Storage Redirection with Secure Boot								
Requirement:	Mandatory - exempt for systems that do not support the Secure Boot BIOS boot option								
System:	<table><tr><th>Form Factor</th><th>System Power Model</th><th>Intel® AMT Network Interface</th><th>LAN Type</th></tr><tr><td><input checked="" type="checkbox"/> Desktop <input checked="" type="checkbox"/> Workstation <input checked="" type="checkbox"/> Mobile</td><td><input checked="" type="checkbox"/> Standard <input checked="" type="checkbox"/> Modern Standby or InstantGo*</td><td><input type="checkbox"/> LAN <input checked="" type="checkbox"/> Either Used <input type="checkbox"/> WLAN <input type="checkbox"/> Not Used</td><td><input checked="" type="checkbox"/> Integrated LAN <input type="checkbox"/> Discrete LAN <input type="checkbox"/> TBT Dock LAN</td></tr></table>	Form Factor	System Power Model	Intel® AMT Network Interface	LAN Type	<input checked="" type="checkbox"/> Desktop <input checked="" type="checkbox"/> Workstation <input checked="" type="checkbox"/> Mobile	<input checked="" type="checkbox"/> Standard <input checked="" type="checkbox"/> Modern Standby or InstantGo*	<input type="checkbox"/> LAN <input checked="" type="checkbox"/> Either Used <input type="checkbox"/> WLAN <input type="checkbox"/> Not Used	<input checked="" type="checkbox"/> Integrated LAN <input type="checkbox"/> Discrete LAN <input type="checkbox"/> TBT Dock LAN
Form Factor	System Power Model	Intel® AMT Network Interface	LAN Type						
<input checked="" type="checkbox"/> Desktop <input checked="" type="checkbox"/> Workstation <input checked="" type="checkbox"/> Mobile	<input checked="" type="checkbox"/> Standard <input checked="" type="checkbox"/> Modern Standby or InstantGo*	<input type="checkbox"/> LAN <input checked="" type="checkbox"/> Either Used <input type="checkbox"/> WLAN <input type="checkbox"/> Not Used	<input checked="" type="checkbox"/> Integrated LAN <input type="checkbox"/> Discrete LAN <input type="checkbox"/> TBT Dock LAN						
Method:	Automated by Intel® PETS with test operator interaction								
Description:	An Intel® AMT compliant system supporting Secure Boot supports Storage Redirection operations with non-secure images. It also supports a boot option to enforce the secure boot even during the Storage Redirection boot flow.								
Objective:	Verify that the BIOS by default disables the secure boot feature when performing a Storage Redirection boot. Additionally, verify that when the flag to enforce secure boot during Storage Redirection is set, BIOS does not disable the secure boot feature when performing the Storage Redirection boot of an ISO OS image. Furthermore, it fail to boot with an insecure ISO OS image, but succeed to boot with a secured ISO OS image.								
Setup:	The initial state of the SUT should be S0/MeOn with Host OS running. Intel® AMT should be provisioned via manual mode. Before running this test, ensure that SOL and Storage Redirection are enabled in the Intel® MEBX. The SUT must have a UEFI BIOS and CSM disabled to allow Secure Boot testing. A secured ISO OS image must be created and placed on the management console hard drive; Intel® PETS does not include such an image.								
Procedure:	<div><div><div>1. Set the active power package on the SUT to Power Package 2 (Intel® ME on in S0, wake in Sx/AC).</div><div>2. Set the Intel® AMT WLAN link policy on the SUT to Link Policy 3 (Enabled in S0, Sx/AC), if the WLAN network interface is used.</div><div>3. Ensure the TCP maximum data retransmission setting defined in the SUT profile is applied to both a) the management console, and b) the SUT via Intel® AMT, if the WLAN network interface is used.</div></div><div>If the configuration on the management console is not already aligned to the SUT profile setting, the network stack on the management console need to be reset; leading to potential network connectivity loss for other applications on the system.</div><div>Before synchronizing the setting on the management console, provide a warning to the test operator, with the option to proceed or cancel, indicating the TCP maximum data retransmission network setting is about to be changed and that it may be necessary to re-establish network connectivity for any other applications running on the management console. If the test operator chooses to cancel, the test step is marked as failed.</div><div><div>4. Ensure the Intel® AMT redirection ports are enabled on the SUT.</div><div>5. Cancel any existing Intel® AMT user consent session which may be active on the SUT.</div><div>6. Ensure the Intel® AMT user consent opt-in setting is disabled on the SUT.</div><div>7. Request the test operator to:<div><div> a. gracefully reboot the SUT,</div><div> b. set the BIOS to disable Secure Boot, and</div><div> c. boot the SUT to Host OS.</div></div></div><div><div>8. Verify that the SUT is in S0/MeOn (CM0,CM0-PG).</div><div>9. Verify that the Host OS on the SUT is available.</div><div>10. Verify that Intel® AMT on the SUT responds to version queries.</div></div></div></div>								



ID:	AMT_036
Procedure: (continued)	<p>The steps within this block is executed as if they are part of an independent sub-test. If a failure occurs at any point during the flow below, the remainder of the steps related to the sub-test, may be skipped.</p> <ol style="list-style-type: none"> Gracefully shutdown to S5/MeOn the SUT via the Host OS and then wait 10 seconds. Use Intel® AMT to set the SUT boot options to use SOL and Storage Redirection Boot on the next boot. Inform the test operator that a system boot is performed by Intel® PETS requesting that the BIOS boot to a redirected un-secured ISO OS image via Serial-Over-LAN. Open a SOL Redirection session with the SUT via Intel® AMT using the Putty terminal program on the management console. Open a Storage Redirection session with the SUT via Intel® AMT using an un-secured ISO OS image on the management console. Perform a Remote Power-Up of the SUT via Intel® AMT. Request the test operator to confirm that SUT boots from redirected un-secured ISO OS image.
Procedure: (continued)	<ol style="list-style-type: none"> Close any open SOL and Storage Redirection session(s) with the SUT via Intel® AMT. Close any Putty terminal window which may still be open. <p>The remaining steps within this block is executed as if they are part of an independent sub-test. If a failure occurs at any point during the flow below, the remainder of the steps related to the sub-test, may be skipped.</p> <ol style="list-style-type: none"> Request the test operator to: <ol style="list-style-type: none"> Gracefully reboot the SUT, Set the BIOS to enable Secure Boot, and Boot the SUT to Host OS. Perform a Remote Power-Down of the SUT via Intel® AMT. Use Intel® AMT to set the boot options to use SOL and Force Secure Storage Redirection Boot on the SUT for the next boot. Inform the test operator that a system boot is performed by Intel® PETS requesting that the BIOS securely boot to a redirected un-secured ISO OS image via Serial-Over-LAN. Open a SOL Redirection session with the SUT via Intel® AMT using the Putty terminal program on the management console. Open a Storage Redirection session with the SUT via Intel® AMT using an un-secured ISO OS image on the management console. Perform a Remote Power-Up of the SUT via Intel® AMT. Request the test operator to confirm that the redirected un-secured ISO OS image did not boot.
Procedure: (continued)	<ol style="list-style-type: none"> Close any open SOL and Storage Redirection session(s) with the SUT via Intel® AMT. Close any Putty terminal window which may still be open. <p>The remaining steps within this block is executed as if they are part of an independent sub-test. If a failure occurs at any point during the flow below, the remainder of the steps related to the sub-test, may be skipped.</p> <ol style="list-style-type: none"> Perform a Remote Power-Down of the SUT via Intel® AMT. Use Intel® AMT to set the boot options to use SOL and Force Secure Storage Redirection Boot on the SUT for the next boot. Inform the test operator that a system boot is performed by Intel® PETS requesting that the BIOS securely boot to a redirected secured ISO OS image via Serial-Over-LAN. Request the test operator to select a secure ISO OS image on the management console hard drive for Intel® PETS to use on the next boot. Open a SOL Redirection session with the SUT via Intel® AMT using the Putty terminal program on the management console. Open a Storage Redirection session with the SUT via Intel® AMT using a the secured ISO OS image selected by the test operator on the management console. Perform a Remote Power-Up of the SUT via Intel® AMT. Request the test operator to confirm that the redirected secured ISO OS image boot screen is displayed in the Putty window.
Procedure: (continued)	<ol style="list-style-type: none"> Close any open SOL and Storage Redirection session(s) with the SUT via Intel® AMT. Close any Putty terminal window which may still be open. Perform a Remote Reset of the SUT via Intel® AMT.
Pass Criteria:	The test passes if Intel® PETS confirms each test step succeeded.
References:	For details on Storage Redirection and Secure Boot, refer the <i>Intel® ME BIOS Specification</i> .



11.7.9 SOL Character Interpretation

ID:	AMT_037			
Title:	Serial-Over-LAN (SOL) Character Interpretation			
Requirement:	Mandatory - exempt for systems that do not support the BIOS Setup boot option			
System:	Form Factor <input checked="" type="checkbox"/> Desktop <input checked="" type="checkbox"/> Workstation <input checked="" type="checkbox"/> Mobile	System Power Model <input checked="" type="checkbox"/> Standard <input checked="" type="checkbox"/> Modern Standby or InstantGo*	Intel® AMT Network Interface <input type="checkbox"/> LAN <input checked="" type="checkbox"/> Either Used <input type="checkbox"/> WLAN <input type="checkbox"/> Not Used	LAN Type <input checked="" type="checkbox"/> Integrated LAN <input type="checkbox"/> Discrete LAN <input type="checkbox"/> TBT Dock LAN
Method:	Automated by Intel® PETS with test operator interaction			
Description:	An Intel® AMT compliant system have its BIOS interpret Serial-Over-LAN (SOL) characters input by means of a management console as ASCII characters.			
Objective:	Verify that the BIOS correctly handles and processes characters input by means of the management console via SOL as ASCII characters, and not as keystrokes, or any other interpretation.			
Setup:	<p>The initial state of the SUT should be S0/MeOn with Host OS running. Intel® AMT should be provisioned via manual mode. Before running this test, ensure that SOL is enabled in the Intel® MEBX.</p> <p>The default number of rows shown in the Putty terminal window may differ from the number of rows displayed by the BIOS. When this occurs, the Putty terminal display incur line wrapping problems. To avoid this problem, change the settings of the Putty application to align with the BIOS via the following steps:</p> <ol style="list-style-type: none"> 1. Open the ".\Intel(R) Platform Enablement Test Suite\Plugins\Me\Redirection\bin\" directory. 2. Start putty.exe, and in the Category section: <ol style="list-style-type: none"> a. Select Window, and change the Rows value to the required number of rows. b. Select Session, then select <i>Default Settings</i>, and finally click the <i>Save</i> button. 3. Close the Putty Configuration window. 4. To confirm, start putty.exe again, and make sure Row number is set to the new value. 			
Procedure:	<ol style="list-style-type: none"> 1. Set the active power package on the SUT to Power Package 2 (Intel® ME on in S0, wake in Sx/AC). 2. Set the Intel® AMT WLAN link policy on the SUT to Link Policy 3 (Enabled in S0, Sx/AC), if the WLAN network interface is used. 3. Ensure the TCP maximum data retransmission setting defined in the SUT profile is applied to both a) the management console, and b) the SUT via Intel® AMT, if the WLAN network interface is used. <p>If the configuration on the management console is not already aligned to the SUT profile setting, the network stack on the management console need to be reset; leading to potential network connectivity loss for other applications on the system.</p> <p>Before synchronizing the setting on the management console, provide a warning to the test operator, with the option to proceed or cancel, indicating the TCP maximum data retransmission network setting is about to be changed and that it may be necessary to re-establish network connectivity for any other applications running on the management console. If the test operator chooses to cancel, the test step is marked as failed.</p> <ol style="list-style-type: none"> 4. Check that the SUT supports booting into BIOS by querying the Intel® AMT and checking the boot capabilities. If not supported, end the test and request the test operator to confirm the BIOS support of 'BIOS Setup' OEMCapabilities1 setting provided to the Intel® ME via the SMBIOS Type 130 table. 5. Request the test operator to: <ol style="list-style-type: none"> a. gracefully reboot the SUT, b. enter the BIOS menu and set a strong password (a combination of lower case, upper case, alphanumeric characters, as well as punctuation characters) for BIOS menu access, and c. boot the SUT to Host OS. 6. Wait for the SUT to return to S0/MeOn with the Host OS running. 7. Ensure the Intel® AMT redirection ports are enabled on the SUT. 8. Cancel any existing Intel® AMT user consent session which may be active on the SUT. 9. Ensure the Intel® AMT user consent opt-in setting is disabled on the SUT. 10. Use Intel® AMT to set the BIOS Setup boot option on the SUT for the next boot. 11. Use Intel® AMT to set the SUT boot options to use SOL Redirection on the next boot. 			



ID:	AMT_037
Procedure: (continued)	<p>12. Close any open SOL Redirection session with the SUT via Intel® AMT. The remaining steps within this block is executed as if they are part of an independent sub-test. If a failure occurs at any point during the flow below, the remainder of the steps related to the sub-test, may be skipped.</p> <p>13. Inform the test operator that a system boot is performed by Intel® PETS requesting that the BIOS boot into the BIOS setup menu.</p> <p>14. Gracefully shutdown to S5/MeOn the SUT via the Host OS and then wait 10 seconds.</p> <p>15. Open a SOL Redirection session with the SUT via Intel® AMT using the Putty terminal program on the management console.</p> <p>16. Perform a Remote Power-Up of the SUT via Intel® AMT.</p> <p>17. Request the test operator to:</p> <ol style="list-style-type: none"> confirm that the BIOS setup screen of the SUT is displayed in the Putty window. confirm that the strong password can be entered into the Putty window and that the BIOS accepts it.
Procedure: (continued)	<p>18. Close any open SOL session with the SUT via Intel® AMT.</p> <p>19. Close any Putty terminal window which may still be open.</p> <p>20. Perform a Remote Reset of the SUT via Intel® AMT.</p> <p>21. Request the test operator to:</p> <ol style="list-style-type: none"> Repeat test multiple times to ensure that all lower case and upper case alphanumeric and punctuation characters are correctly handled and interpreted by the BIOS. When final testing is complete, clear the BIOS password (if possible).
Pass Criteria:	The test passes if all attempted strong passwords can be sent to BIOS over SOL.
References:	For details on Terminal Emulation, refer the <i>Intel® ME BIOS Specification</i> .

11.7.10 SOL Redirection during System Restart

ID:	AMT_038			
Title:	Serial-Over-LAN (SOL) Redirection during System Restart			
Requirement:	Optional			
System:	Form Factor <input checked="" type="checkbox"/> Desktop <input checked="" type="checkbox"/> Workstation <input checked="" type="checkbox"/> Mobile	System Power Model <input checked="" type="checkbox"/> Standard <input checked="" type="checkbox"/> Modern Standby or InstantGo*	Intel® AMT Network Interface <input type="checkbox"/> LAN <input checked="" type="checkbox"/> Either Used <input type="checkbox"/> WLAN <input type="checkbox"/> Not Used	LAN Type <input checked="" type="checkbox"/> Integrated LAN <input type="checkbox"/> Discrete LAN <input type="checkbox"/> TBT Dock LAN
Method:	Automated by Intel® PETS with test operator interaction			
Description:	An Intel® AMT compliant system implements BIOS boot screen redirection according to the boot options received from the GetBootOptions command during system Restart.			
Objective:	<p>Verify that the BIOS detects, and executes, a request (by means of boot options) to redirect text to the management console via SOL.</p> <p>Intel® AMT enables remote management of the platform, including providing capabilities to read the boot options sent from the management console. These boot options can include commands to send display text from the Intel® AMT platform to the remote console by means of Serial-Over-LAN functionality. Testing described in this section verify that BIOS has been properly enabled to support these usage models.</p>			
Setup:	<p>The initial state of the SUT should be S0/MeOn with Host OS running. Intel® AMT should be provisioned via manual mode. Before running this test, ensure that SOL is enabled in the Intel® MEBX.</p> <p>The default number of rows shown in the Putty terminal window may differ from the number of rows displayed by the BIOS. When this occurs, the Putty terminal display incur line wrapping problems. To avoid this problem, change the settings of the Putty application to align with the BIOS via the following steps:</p> <ol style="list-style-type: none"> Open the ".\Intel(R) Platform Enablement Test Suite\Plugins\Me\Redirection\bin\" directory. Start putty.exe, and in the Category section: <ol style="list-style-type: none"> Select Window, and change the Rows value to the required number of rows. Select Session, then select <i>Default Settings</i>, and finally click the Save button. Close the Putty Configuration window. To confirm, start putty.exe again, and make sure Row number is set to the new value. 			

ID:	AMT_038
Procedure:	<ol style="list-style-type: none"> 1. Set the active power package on the SUT to Power Package 2 (Intel® ME on in S0, wake in Sx/AC). 2. Set the Intel® AMT WLAN link policy on the SUT to Link Policy 3 (Enabled in S0, Sx/AC), if the WLAN network interface is used. 3. Ensure the TCP maximum data retransmission setting defined in the SUT profile is applied to both a) the management console, and b) the SUT via Intel® AMT, if the WLAN network interface is used. If the configuration on the management console is not already aligned to the SUT profile setting, the network stack on the management console need to be reset; leading to potential network connectivity loss for other applications on the system. Before synchronizing the setting on the management console, provide a warning to the test operator, with the option to proceed or cancel, indicating the TCP maximum data retransmission network setting is about to be changed and that it may be necessary to re-establish network connectivity for any other applications running on the management console. If the test operator chooses to cancel, the test step is marked as failed. 4. Ensure the Intel® AMT redirection ports are enabled on the SUT. 5. Cancel any existing Intel® AMT user consent session which may be active on the SUT. 6. Ensure the Intel® AMT user consent opt-in setting is disabled on the SUT. 7. Use Intel® AMT to set the SUT boot options to use SOL Redirection on the next boot.
Procedure: (continued)	<ol style="list-style-type: none"> 8. Close any open SOL Redirection session with the SUT via Intel® AMT. The remaining steps within this block is executed as if they are part of an independent sub-test. If a failure occurs at any point during the flow below, the remainder of the steps related to the sub-test, may be skipped. 9. Inform the test operator that a system restart is performed by Intel® PETS requesting that the BIOS boot with text output redirected via Serial-Over-LAN. 10. Open a SOL Redirection session with the SUT via Intel® AMT using the Putty terminal program on the management console. 11. Gracefully restart the SUT via the Host OS. 12. Request the test operator to confirm that the redirected text from the BIOS boot flow was displayed in the Putty window.
Procedure: (continued)	<ol style="list-style-type: none"> 13. Close any open SOL session with the SUT via Intel® AMT. 14. Close any Putty terminal window which may still be open. 15. Perform a Remote Reset of the SUT via Intel® AMT.
Pass Criteria:	The test passes if Intel® PETS indicates all steps have passed successfully and BIOS boot screen is redirected to the Putty terminal on the management console via Serial-Over-LAN.
References:	For details on SOL and ASF Boot Options, refer the <i>Intel® ME BIOS Specification</i> .

11.8 Keyboard, Video, and Mouse (KVM) Redirection

The section serves as a checklist for the environment setup and covers integration testing of Keyboard, Video, and Mouse (KVM) Redirection in Intel® AMT.

11.8.1 Test Environment

The System Under Test (SUT) is to be configured with Intel® AMT set in manual provisioning mode with static IP address or DHCP. The management console may be a laptop or a desktop with a version of Microsoft Windows* supported by Intel® PETS, and the SUT should have a version of Microsoft Windows* supported by Intel® PETS as well. The test network is comprised of a hub/switch and network cables.

Tools for testing:

- Intel® PETS: The latest version of the tool from the Intel® CSME Compliance and Debug kit release. Refer the Intel® PETS User Guide for exact instructions on how to load and setup the Intel® PETS software.
- Intel® Automated Power Switch (Intel® APS): The SUT should be connected to an Intel® APS 3 unit. In case an Intel® APS 3 is not available, select the Manual configuration in the Intel® PETS SUT profile configuration menu.
- Intel® PETS Local Agent: The local agent must be installed on the SUT.



- USB Storage device (USB Key): Either USB 2.0 or USB 3.0 compliant, depending on what the SUT can support. If the SUT can support both USB 2.0 and USB 3.0, the USB Storage device used for testing should be the lower of the two (USB 2.0).

In order for Intel® PETS to work properly, ensure the following:

- the SUT has a valid System UUID. This can be checked by confirming a non-zero value is reported by the Intel® MEInfo tool.
- the firmware image is configured to **not** require user consent on redirection. This can be done by checking the following value of the SPI image via the Intel® FIT tool in the 'Intel(R) AMT' tab: 'Redirection Configuration' | 'Redirection Privacy / Security Level' set to "Default".
- the SUT should have integrated graphics. If it supports switchable graphics, graphics configuration should be set to **integrated** graphics.

Where applicable, the wireless LAN interface on Intel® AMT must be on a different network/subnet than the wired LAN interface. For details on how to enter the network interface details into Intel® PETS, consult the Intel® PETS User Guide.

If the firmware image or the SUT configuration does not support some features, Intel® PETS show those features as failing when tested. Intel® PETS cannot determine in all cases which features have been deactivated and should thus be skipped during testing.

All KVM tests conducted with Intel® PETS uses a default 8bpp (bits-per-pixel) color depth configuration when connecting to the Intel® AMT KVM server. Compliancy test PASS/FAIL conditions are based on connectivity and testing conducted at an 8bpp color depth configuration. To enable extended product testing where supported, the test operator may specify a 16bpp color depth configuration via Intel® PETS package configuration options.

Note:

Use of 16bpp color depth when connecting to an Intel® AMT KVM server may not be supported at ultra-high display resolutions and/or with some system configurations, and may result in connectivity errors. Use of 8bpp color depth when connecting to a Intel® AMT KVM server may also not be supported at screen resolutions beyond product specification. Refer the *Intel® AMT Product Requirements* document for further details about supported KVM resolutions and color depths.

When a KVM Redirection session is active, the SUT screen have a colored line displayed around its edges. An icon on the upper right corner of the screen also appear, indicating that a KVM Redirection session is now active on the SUT.

In S0, the CM0-PG and CM0 Intel® ME 'MeOn' states appear the same from Intel® APS measurement perspective. Follow the procedure below via the Host OS on the SUT to confirm if the Intel® ME is Power Gated (CM0-PG):

1. Get the PWRMBASE (32-bits) by reading the PCI configuration space B0:D31:F2 (Bus:Device:Function) at offset 48h. Information describing how to access this value may be found in either the PCH EDS or the PCH BIOS Specification.
2. Read 32-bits at PWRMBASE + 590h and verify that bits 31:24 equal F9h.
3. Read 32-bits at PWRMBASE + 594h and verify that bits 7:0 equal FFh.

11.8.2 KVM Redirection and BIOS Setup Boot Option over Intel® AMT LAN Network Interface

ID:	AMT_040
Title:	Keyboard, Video, and Mouse (KVM) Redirection and BIOS Setup Boot Option over Intel® AMT LAN Network Interface



ID:	AMT_040			
Requirement:	Mandatory - exempt for systems which do not support KVM or the BIOS Setup boot option			
System:	Form Factor <input checked="" type="checkbox"/> Desktop <input checked="" type="checkbox"/> Workstation <input checked="" type="checkbox"/> Mobile	System Power Model <input checked="" type="checkbox"/> Standard <input checked="" type="checkbox"/> Modern Standby or InstantGo*	Intel® AMT Network Interface <input checked="" type="checkbox"/> LAN <input type="checkbox"/> Either Used <input type="checkbox"/> WLAN <input type="checkbox"/> Not Used	LAN Type <input checked="" type="checkbox"/> Integrated LAN <input type="checkbox"/> Discrete LAN <input type="checkbox"/> TBT Dock LAN
Method:	Automated by Intel® PETS with test operator interaction			
Description:	Verify that a KVM Redirection session can be established and functions correctly in the pre-OS environment.			
Objective:	This test verify that a KVM Redirection session can be established, the remote screen is displayed correctly, and remote keyboard (and mouse where supported) are working when the system under test is booting into a Pre-OS environment.			
Setup:	The initial state of the SUT should be S0/MeOn with Host OS running. Intel® AMT should be provisioned via manual mode. Before running this test, ensure that KVM is enabled in the Intel® MEBX. If the SUT supports switchable graphics, graphics configuration should be set to integrated graphics.			
Procedure:	<ol style="list-style-type: none">1. Set the active power package on the SUT to Power Package 2 (Intel® ME on in S0, wake in Sx/AC).2. Check that the SUT supports booting into BIOS by querying the Intel® AMT and checking the boot capabilities.<ol style="list-style-type: none">a. If supported, use Intel® AMT to set the BIOS Setup boot option on the SUT for the next boot.b. If not supported, end the test and request the test operator to confirm the BIOS support of 'BIOS Setup' OEMCapabilities1 setting provided to the Intel® ME via the SMBIOS Type 130 table.3. Ensure the Intel® AMT redirection ports are enabled on the SUT.4. Cancel any existing Intel® AMT user consent session which may be active on the SUT.5. Ensure the Intel® AMT user consent opt-in setting is disabled on the SUT.6. Set the KVM password to 'Admin!98' on the SUT via Intel® AMT.7. Ensure that the VNC port 5900 is enabled on the SUT via Intel® AMT.			
Procedure: (continued)	<p>The steps within this block is executed as if they are part of an independent sub-test. If a failure occurs at any point during the flow below, the remainder of the steps related to the sub-test, may be skipped.</p> <ol style="list-style-type: none">8. Inform the test operator that the SUT soon be powered down and the VNC Viewer window open. When the SUT starts to boot, request the test operator to:<ol style="list-style-type: none">a. Verify that the BIOS setup menu appears on the SUT screen during boot.b. Try using the keyboard (and mouse where supported) to navigate the BIOS menus.9. Gracefully shutdown to S5/MeOn the SUT via the Host OS and then wait 10 seconds.10. Open a KVM Redirection session with the SUT via Intel® AMT using the VNC Viewer on the management console.11. Perform a Remote Power-Up of the SUT via Intel® AMT.12. Request the test operator to:<ol style="list-style-type: none">a. Confirm that the redirected BIOS setup screen from the SUT appears in the VNC Viewer.b. Confirm that the keyboard (and mouse where supported) can control the Host OS via the management console via the VNC Viewer.			
Procedure: (continued)	<ol style="list-style-type: none">13. Close any open KVM Redirection session with the SUT via Intel® AMT.14. Close any VNC Viewer window which may still be open.15. Perform a Remote Reset of the SUT via Intel® AMT.			
Pass Criteria:	The test passes if the BIOS Setup screen is redirected to management console and remote keyboard (and mouse where supported) are confirmed to be working properly.			
References:	For details on KVM Redirection and ASF Boot Options, refer the <i>Intel® ME BIOS Specification</i> .			

11.8.3 KVM Redirection and BIOS Setup Boot Option over Intel® AMT WLAN Network Interface

ID:	AMT_041
Title:	Keyboard, Video, and Mouse (KVM) Redirection and BIOS Setup Boot Option over Intel® AMT WLAN Network Interface
Requirement:	Mandatory - exempt for systems which do not support KVM or the BIOS Setup boot option



ID:	AMT_041			
System:	Form Factor	System Power Model	Intel® AMT Network Interface	LAN Type
	<input checked="" type="checkbox"/> Desktop <input checked="" type="checkbox"/> Workstation <input checked="" type="checkbox"/> Mobile	<input checked="" type="checkbox"/> Standard <input checked="" type="checkbox"/> Modern Standby or InstantGo*	<input type="checkbox"/> LAN <input type="checkbox"/> Either Used <input checked="" type="checkbox"/> WLAN <input type="checkbox"/> Not Used	<input type="checkbox"/> Integrated LAN <input type="checkbox"/> Discrete LAN <input type="checkbox"/> TBT Dock LAN
Method:	Automated by Intel® PETS with test operator interaction			
Description:	Verify that a KVM Redirection session can be established and functions correctly in the pre-OS environment.			
Objective:	This test verify that a KVM Redirection session can be established, the remote screen is displayed correctly, and remote keyboard (and mouse where supported) are working when the system under test is booting into a Pre-OS environment.			
Setup:	The initial state of the SUT should be S0/MeOn with Host OS running. Intel® AMT should be provisioned via manual mode. Before running this test, ensure that KVM is enabled in the Intel® MEBX. If the SUT supports switchable graphics, graphics configuration should be set to integrated graphics.			
Procedure:	<ol style="list-style-type: none"> Set the active power package on the SUT to Power Package 2 (Intel® ME on in S0, wake in Sx/AC). Check that the SUT supports booting into BIOS by querying the Intel® AMT and checking the boot capabilities. <ol style="list-style-type: none"> If supported, use Intel® AMT to set the BIOS Setup boot option on the SUT for the next boot. If not supported, end the test and request the test operator to confirm the BIOS support of 'BIOS Setup' OEMCapabilities1 setting provided to the Intel® ME via the SMBIOS Type 130 table. Set the Intel® AMT WLAN link policy on the SUT to Link Policy 3 (Enabled in S0, Sx/AC). Ensure the TCP maximum data retransmission setting defined in the SUT profile is applied to both a) the management console, and b) the SUT via Intel® AMT. If the configuration on the management console is not already aligned to the SUT profile setting, the network stack on the management console need to be reset; leading to potential network connectivity loss for other applications on the system. Before synchronizing the setting on the management console, provide a warning to the test operator, with the option to proceed or cancel, indicating the TCP maximum data retransmission network setting is about to be changed and that it may be necessary to re-establish network connectivity for any other applications running on the management console. If the test operator chooses to cancel, the test step is marked as failed. Ensure the Intel® AMT redirection ports are enabled on the SUT. Cancel any existing Intel® AMT user consent session which may be active on the SUT. Ensure the Intel® AMT user consent opt-in setting is disabled on the SUT. Set the KVM password to 'Admin!98' on the SUT via Intel® AMT. Ensure that the VNC port 5900 is enabled on the SUT via Intel® AMT. 			
Procedure: (continued)	<p>The steps within this block is executed as if they are part of an independent sub-test. If a failure occurs at any point during the flow below, the remainder of the steps related to the sub-test, may be skipped.</p> <ol style="list-style-type: none"> Inform the test operator that the SUT soon be powered down and the VNC Viewer window opens. When the SUT starts to boot, request the test operator to: <ol style="list-style-type: none"> Verify that the BIOS setup menu appears on the SUT screen during boot. Try using the keyboard (and mouse where supported) to navigate the BIOS menus. Gracefully shutdown to S5/MeOn the SUT via the Host OS and then wait 10 seconds. Verify that Intel® AMT is available via WLAN by requesting its version. Open a KVM Redirection session with the SUT via Intel® AMT using the VNC Viewer on the management console. Perform a Remote Power-Up of the SUT via Intel® AMT. Request the test operator to: <ol style="list-style-type: none"> Confirm that the redirected BIOS setup screen from the SUT appears in the VNC Viewer. Confirm that the keyboard (and mouse where supported) can control the Host OS via the management console via the VNC Viewer. 			
Procedure: (continued)	<ol style="list-style-type: none"> Close any open KVM Redirection session with the SUT via Intel® AMT. Close any VNC Viewer window which may still be open. Perform a Remote Reset of the SUT via Intel® AMT. 			
Pass Criteria:	The test passes if the BIOS Setup screen is redirected to management console and remote keyboard (and mouse where supported) are confirmed to be working properly.			
References:	For details on KVM Redirection and ASF Boot Options, refer the <i>Intel® ME BIOS Specification</i> .			



11.8.4 KVM Redirection over Intel® AMT LAN Network Interface

ID:	AMT_042			
Title:	Keyboard, Video, and Mouse (KVM) Redirection over Intel® AMT LAN Network Interface			
Requirement:	Mandatory - exempt for systems which do not support KVM with internal graphics			
System:	Form Factor <input checked="" type="checkbox"/> Desktop <input checked="" type="checkbox"/> Workstation <input checked="" type="checkbox"/> Mobile	System Power Model <input checked="" type="checkbox"/> Standard <input checked="" type="checkbox"/> Modern Standby or InstantGo*	Intel® AMT Network Interface <input checked="" type="checkbox"/> LAN <input type="checkbox"/> Either Used <input type="checkbox"/> WLAN <input type="checkbox"/> Not Used	LAN Type <input checked="" type="checkbox"/> Integrated LAN <input type="checkbox"/> Discrete LAN <input type="checkbox"/> TBT Dock LAN
Method:	Automated by Intel® PETS with test operator interaction			
Description:	An Intel® AMT compliant system implements KVM redirection support when the system is in Sx state and moves to S0 state.			
Objective:	This test checks that when the SUT moves from S3, S4 or S5, to S0 when KVM has been initiated, the BIOS would not halt and wait for the user to give consent for the KVM Redirection session, and the user consent opt-in option should not be displayed on the platform under test. In all cases, the SUT's screen is visible in the Virtual Network Computing (VNC) Viewer on the management console.			
Setup:	The initial state of the SUT should be S0/MeOn with Host OS running. Intel® AMT should be provisioned via manual mode. Before running this test, ensure that KVM is enabled in the Intel® MEBX. If the SUT supports switchable graphics, graphics configuration should be set to integrated graphics.			
Procedure:	<ol style="list-style-type: none"> Set the active power package on the SUT to Power Package 2 (Intel® ME on in S0, wake in Sx/AC). Ensure the Intel® AMT redirection ports are enabled on the SUT. Cancel any existing Intel® AMT user consent session which may be active on the SUT. Ensure the Intel® AMT user consent opt-in setting is disabled on the SUT. Set the KVM password to 'Admin!98' on the SUT via Intel® AMT. Ensure that the VNC port 5900 is enabled on the SUT via Intel® AMT. 			
Procedure: (continued) S5→S0 Flow	<p>The steps within this block is executed as if they are part of an independent sub-test. If a failure occurs at any point during the flow below, the remainder of the steps related to the sub-test, may be skipped.</p> <ol style="list-style-type: none"> Inform the test operator that the SUT soon be powered down and the VNC Viewer window opens. When the VNC Viewer window opens and the SUT starts to boot, request the test operator to: <ol style="list-style-type: none"> Verify that the Ctrl+P (or equivalent keystroke) Intel® MEBX prompt does not appear on the SUT screen during boot. Try using the keyboard and mouse to control the Host OS. Gracefully shutdown to S5/MeOn the SUT via the Host OS and then wait 10 seconds. Open a KVM Redirection session with the SUT via Intel® AMT using the VNC Viewer on the management console. Perform a Remote Power-Up of the SUT via Intel® AMT. Request the test operator to: <ol style="list-style-type: none"> Confirm that the redirected screen from the SUT appears in the VNC Viewer. Confirm that the keyboard and mouse can control the Host OS via the management console via the VNC Viewer. 			



ID:	AMT_042
<p>Procedure: (continued)</p> <p>S4→S0 Flow</p>	<p>12. Close any open KVM Redirection session with the SUT via Intel® AMT.</p> <p>13. Close any VNC Viewer window which may still be open.</p> <p>14. Attempt to bring the SUT to a base state via the following:</p> <ol style="list-style-type: none"> Verify that the SUT is in S0/MeOn (CM0,CM0-PG). Verify that the Host OS on the SUT is available. Verify that Intel® AMT on the SUT responds to version queries via the LAN network interface. <p>If any of base state verification steps above fail, perform the following as an attempt to recover the SUT before attempting the base state verification steps above one last time.</p> <ol style="list-style-type: none"> Bring the system to G3 and wait 10 seconds. Set system power configuration to AC/DC and wait another 10 seconds. Briefly press the Power Button on the SUT. <p>The remaining steps within this block is executed as if they are part of an independent sub-test. If a failure occurs at any point during the flow below, the remainder of the steps related to the sub-test, may be skipped.</p> <p>15. Inform the test operator that the SUT soon be sent into hibernation state and the VNC Viewer window opens. When the VNC Viewer window opens and the SUT starts to boot, request the test operator to:</p> <ol style="list-style-type: none"> verify that the Ctrl+P (or equivalent keystroke) Intel® MEBX prompt does not appear on the SUT screen during resume from hibernation. try using the keyboard and mouse to control the Host OS. <p>16. Hibernate to S4/MeOn the SUT via the Host OS and then wait 10 seconds.</p> <p>17. Open a KVM Redirection session with the SUT via Intel® AMT using the VNC Viewer on the management console.</p> <p>18. Perform a Remote Power-Up of the SUT via Intel® AMT.</p> <p>19. Request the test operator to:</p> <ol style="list-style-type: none"> confirm that the redirected screen from the SUT appears in the VNC Viewer. confirm that the keyboard and mouse can control the Host OS via the management console via the VNC Viewer.
<p>Procedure: (continued)</p> <p>S3→S0 Flow</p>	<p>20. Close any open KVM Redirection session with the SUT via Intel® AMT.</p> <p>21. Close any VNC Viewer window which may still be open.</p> <p>22. Attempt to bring the SUT to a base state via the following:</p> <ol style="list-style-type: none"> Verify that the SUT is in S0/MeOn (CM0,CM0-PG). Verify that the Host OS on the SUT is available. Verify that Intel® AMT on the SUT responds to version queries via the LAN network interface. <p>If any of base state verification steps above fail, perform the following as an attempt to recover the SUT before attempting the base state verification steps above one last time.</p> <ol style="list-style-type: none"> Bring the system to G3 and wait 10 seconds. Set system power configuration to AC/DC and wait another 10 seconds. Briefly press the Power Button on the SUT. <p>The remaining steps within this block is executed as if they are part of an independent sub-test. If a failure occurs at any point during the flow below, the remainder of the steps related to the sub-test, may be skipped.</p> <p>NOTE: In the case the SUT is operating in Modern Standby or Microsoft Windows* InstantGo* mode, the test automatically end here, and the results thus far reported to the test operator as the final test results. For desktop systems with Intel® RMT support, ensure that Intel® RMT is disabled before running S3 test flows.</p> <p>23. Inform the test operator that the SUT soon be sent into suspend state and the VNC Viewer window opens. When the VNC Viewer window opens and the SUT starts to boot, request the test operator to try using the keyboard and mouse to control the Host OS.</p> <p>24. Record the Host OS last boot time on the SUT (to verify successful suspend/resume).</p> <p>25. Suspend to S3/MeOn the SUT via the Host OS and then wait 10 seconds.</p> <p>26. Open a KVM Redirection session with the SUT via Intel® AMT using the VNC Viewer on the management console.</p> <p>27. Perform a Remote Power-Up of the SUT via Intel® AMT.</p> <p>28. Wait until system resumes back to the Host OS.</p> <p>29. Verify the Host OS last boot time on the SUT does match the boot time recorded before the suspend.</p> <p>30. Request the test operator to:</p> <ol style="list-style-type: none"> confirm that the redirected screen from the SUT appears in the VNC Viewer. confirm that the keyboard and mouse can control the Host OS via the management console via the VNC Viewer.



ID:	AMT_042
Procedure: (continued) Intel® MEBX Override Check	<p>31. Close any open KVM Redirection session with the SUT via Intel® AMT.</p> <p>32. Close any VNC Viewer window which may still be open.</p> <p>33. Attempt to bring the SUT to a base state via the following:</p> <ol style="list-style-type: none">Verify that the SUT is in S0/MeOn (CM0,CM0-PG).Verify that the Host OS on the SUT is available.Verify that Intel® AMT on the SUT responds to version queries via the LAN network interface. <p>If any of base state verification steps above fail, perform the following as an attempt to recover the SUT before attempting the base state verification steps above one last time.</p> <ol style="list-style-type: none">Bring the system to G3 and wait 10 seconds.Set system power configuration to AC/DC and wait another 10 seconds.Briefly press the Power Button on the SUT. <p>34. The remaining steps within this block is executed as if they are part of an independent sub-test. If a failure occurs at any point during the flow below, the remainder of the steps related to the sub-test, may be skipped.</p> <p>35. Request the test operator to:</p> <ol style="list-style-type: none">Gracefully reboot the SUT,Enter the Intel® MEBX on the SUT and disable KVM, andBoot the SUT to Host OS. <p>36. Gracefully shutdown to S5/MeOn the SUT via the Host OS and then wait 10 seconds.</p> <p>37. Attempt to open a KVM Redirection session with the SUT via Intel® AMT using the VNC Viewer on the management console. Note that failure to open the session by error indicating the KVM interface is disabled indicates success for the test step, otherwise the test step fails.</p> <p>38. Request the test operator to:</p> <ol style="list-style-type: none">Boot the SUT,Enter the Intel® MEBX on the SUT and enable KVM, andBoot the SUT to Host OS.
Procedure: (continued)	<p>39. Close any open KVM Redirection session with the SUT via Intel® AMT.</p> <p>40. Close any VNC Viewer window which may still be open.</p>
Pass Criteria:	The test passes if all attempted KVM Redirection sessions are viewed via VNC Viewer on the management console, and keyboard/mouse functionality is redirected to the Host OS on the SUT. During system boot or resume, the Intel® MEBX hot-key (Ctrl+P or other keystroke) prompt is not displayed on the SUT.
References:	For details on KVM Redirection, refer the <i>Intel® ME BIOS Specification</i> .

11.8.5 KVM Redirection over Intel® AMT WLAN Network Interface

ID:	AMT_043					
Title:	Keyboard, Video, and Mouse (KVM) Redirection over Intel® AMT WLAN Network Interface					
Requirement:	Mandatory - exempt for systems which do not support KVM with internal graphics					
System:	Form Factor		System Power Model	Intel® AMT Network Interface		LAN Type
	<input checked="" type="checkbox"/> Desktop <input checked="" type="checkbox"/> Mobile	<input checked="" type="checkbox"/> Workstation	<input checked="" type="checkbox"/> Standard <input checked="" type="checkbox"/> Modern Standby or InstantGo*	<input type="checkbox"/> LAN <input checked="" type="checkbox"/> WLAN	<input type="checkbox"/> Either Used <input type="checkbox"/> Not Used	<input type="checkbox"/> Integrated LAN <input type="checkbox"/> Discrete LAN <input type="checkbox"/> TBT Dock LAN
Method:	Automated by Intel® PETS with test operator interaction					
Description:	An Intel® AMT compliant system implements KVM redirection support when the system is in Sx state and moves to S0 state.					
Objective:	This test check that when the SUT moves from S3, S4 or S5, to S0 when KVM has been initiated, the BIOS would not halt and wait for the user to give consent for the KVM Redirection session, and the user consent opt-in option should not be displayed on the platform under test. In all cases, the SUT's screen is visible in the Virtual Network Computing (VNC) Viewer on the management console.					
Setup:	The initial state of the SUT should be S0/MeOn with Host OS running. Intel® AMT should be provisioned via manual mode. Before running this test, ensure that KVM is enabled in the Intel® MEBX. If the SUT supports switchable graphics, graphics configuration should be set to integrated graphics.					



ID:	AMT_043
Procedure:	<ol style="list-style-type: none"> 1. Set the active power package on the SUT to Power Package 2 (Intel® ME on in S0, wake in Sx/AC). 2. Set the Intel® AMT WLAN link policy on the SUT to Link Policy 3 (Enabled in S0, Sx/AC). 3. Ensure the Host OS Wake on Wireless LAN is disabled. 4. Ensure the TCP maximum data retransmission setting defined in the SUT profile is applied to both a) the management console, and b) the SUT via Intel® AMT. If the configuration on the management console is not already aligned to the SUT profile setting, the network stack on the management console need to be reset; leading to potential network connectivity loss for other applications on the system. Before synchronizing the setting on the management console, provide a warning to the test operator, with the option to proceed or cancel, indicating the TCP maximum data retransmission network setting is about to be changed and that it may be necessary to re-establish network connectivity for any other applications running on the management console. If the test operator chooses to cancel, the test step is marked as failed. 5. Ensure the Intel® AMT redirection ports are enabled on the SUT. 6. Cancel any existing Intel® AMT user consent session which may be active on the SUT. 7. Ensure the Intel® AMT user consent opt-in setting is disabled on the SUT. 8. Set the KVM password to 'Admin!98' on the SUT via Intel® AMT. 9. Ensure that the VNC port 5900 is enabled on the SUT via Intel® AMT.
Procedure: (continued) S5→S0 Flow	<p>The steps within this block is executed as if they are part of an independent sub-test. If a failure occurs at any point during the flow below, the remainder of the steps related to the sub-test, may be skipped.</p> <ol style="list-style-type: none"> 10. Inform the test operator that the SUT soon be powered down and the VNC Viewer window opens. When the VNC Viewer window opens and the SUT starts to boot, request the test operator to: <ol style="list-style-type: none"> a. Verify that the Ctrl+P (or equivalent keystroke) Intel® MEBX prompt does not appear on the SUT screen during boot. b. Try using the keyboard and mouse to control the Host OS. 11. Gracefully shutdown to S5/MeOn the SUT via the Host OS and then wait 10 seconds. 12. Verify that Intel® AMT is available via WLAN by requesting its version. 13. Open a KVM Redirection session with the SUT via Intel® AMT using the VNC Viewer on the management console. 14. Perform a Remote Power-Up of the SUT via Intel® AMT. 15. Request the test operator to: <ol style="list-style-type: none"> a. Confirm that the redirected screen from the SUT appears in the VNC Viewer. b. Confirm that the keyboard and mouse can control the Host OS via the management console via the VNC Viewer.
Procedure: (continued) S4→S0 Flow	<ol style="list-style-type: none"> 16. Close any open KVM Redirection session with the SUT via Intel® AMT. 17. Close any VNC Viewer window which may still be open. 18. Attempt to bring the SUT to a base state via the following: <ol style="list-style-type: none"> a. Verify that the SUT is in S0/MeOn (CM0,CM0-PG). b. Verify that the Host OS on the SUT is available. c. Verify that Intel® AMT on the SUT responds to version queries via the WLAN network interface. <p>If any of base state verification steps above fail, perform the following as an attempt to recover the SUT before attempting the base state verification steps above one last time.</p> <ol style="list-style-type: none"> a. Bring the system to G3 and wait 10 seconds. b. Set system power configuration to AC/DC and wait another 10 seconds. c. Briefly press the Power Button on the SUT. <p>The remaining steps within this block is executed as if they are part of an independent sub-test. If a failure occurs at any point during the flow below, the remainder of the steps related to the sub-test, may be skipped.</p> 19. Inform the test operator that the SUT soon be sent into hibernation state and the VNC Viewer window opens. When the VNC Viewer window opens and the SUT starts to boot, request the test operator to: <ol style="list-style-type: none"> a. Verify that the Ctrl+P (or equivalent keystroke) Intel® MEBX prompt does not appear on the SUT screen during resume from hibernation. b. Try using the keyboard and mouse to control the Host OS. 20. Hibernate to S4/MeOn the SUT via the Host OS and then wait 10 seconds. 21. Verify that Intel® AMT is available via WLAN by requesting its version. 22. Open a KVM Redirection session with the SUT via Intel® AMT using the VNC Viewer on the management console. 23. Perform a Remote Power-Up of the SUT via Intel® AMT. 24. Request the test operator to: <ol style="list-style-type: none"> a. Confirm that the redirected screen from the SUT appears in the VNC Viewer. b. Confirm that the keyboard and mouse can control the Host OS via the management console via the VNC Viewer.



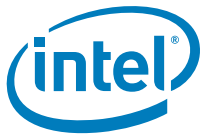
ID:	AMT_043
<p>Procedure: (continued)</p> <p>S3→S0 Flow</p>	<p>25. Close any open KVM Redirection session with the SUT via Intel® AMT.</p> <p>26. Close any VNC Viewer window which may still be open.</p> <p>27. Attempt to bring the SUT to a base state via the following:</p> <ol style="list-style-type: none"> Verify that the SUT is in S0/MeOn (CM0,CM0-PG). Verify that the Host OS on the SUT is available. Verify that the Intel® AMT on the SUT responds to version queries via the WLAN network interface. <p>If any of base state verification steps above fail, perform the following as an attempt to recover the SUT before attempting the base state verification steps above one last time.</p> <ol style="list-style-type: none"> Bring the system to G3 and wait 10 seconds. Set system power configuration to AC/DC and wait another 10 seconds. Briefly press the Power Button on the SUT. <p>The remaining steps within this block is executed as if they are part of an independent sub-test. If a failure occurs at any point during the flow below, the remainder of the steps related to the sub-test, may be skipped.</p> <p>NOTE: In the case the SUT is operating in Modern Standby or Microsoft Windows* InstantGo* mode, the test automatically end here, and the results thus far reported to the test operator as the final test results. For desktop systems with Intel® RMT support, ensure that Intel® RMT is disabled before running S3 test flows.</p> <p>28. Inform the test operator that the SUT soon be sent into suspend state and the VNC Viewer window opens. When the VNC Viewer window opens and the SUT starts to boot, request the test operator to try using the keyboard and mouse to control the Host OS.</p> <p>29. Record the Host OS last boot time on the SUT (to verify successful suspend/resume).</p> <p>30. Suspend to S3/MeOn the SUT via the Host OS and then wait 10 seconds.</p> <p>31. Verify that Intel® AMT is available via WLAN by requesting its version.</p> <p>32. Open a KVM Redirection session with the SUT via Intel® AMT using the VNC Viewer on the management console.</p> <p>33. Perform a Remote Power-Up of the SUT via Intel® AMT.</p> <p>34. Wait until system resumes back to the Host OS.</p> <p>35. Verify the Host OS last boot time on the SUT does match the boot time recorded before the suspend.</p> <p>36. Request the test operator to:</p> <ol style="list-style-type: none"> Confirm that the redirected screen from the SUT appears in the VNC Viewer. Confirm that the keyboard and mouse can control the Host OS via the management console via the VNC Viewer.
<p>Procedure: (continued)</p> <p>Intel® MEBX Override Check</p>	<p>37. Close any open KVM Redirection session with the SUT via Intel® AMT.</p> <p>38. Close any VNC Viewer window which may still be open.</p> <p>39. Attempt to bring the SUT to a base state via the following:</p> <ol style="list-style-type: none"> Verify that the SUT is in S0/MeOn (CM0,CM0-PG). Verify that the Host OS on the SUT is available. Verify that Intel® AMT on the SUT responds to version queries via the WLAN network interface. <p>If any of base state verification steps above fail, perform the following as an attempt to recover the SUT before attempting the base state verification steps above one last time.</p> <ol style="list-style-type: none"> Bring the system to G3 and wait 10 seconds. Set system power configuration to AC/DC and wait another 10 seconds. Briefly press the Power Button on the SUT. <p>40. The remaining steps within this block is executed as if they are part of an independent sub-test. If a failure occurs at any point during the flow below, the remainder of the steps related to the sub-test, may be skipped.</p> <p>41. Request the test operator to:</p> <ol style="list-style-type: none"> Gracefully reboot the SUT, Enter the Intel® MEBX on the SUT and disable KVM, and Boot the SUT to Host OS. <p>42. Gracefully shutdown to S5/MeOn the SUT via the Host OS and then wait 10 seconds.</p> <p>43. Attempt to open a KVM Redirection session with the SUT via Intel® AMT using the VNC Viewer on the management console. Note that failure to open the session by error indicating the KVM interface is disabled indicates success for the test step, otherwise the test step fails.</p> <p>44. Request the test operator to:</p> <ol style="list-style-type: none"> Boot the SUT, Enter the Intel® MEBX on the SUT and enable KVM, and Boot the SUT to Host OS.
<p>Procedure: (continued)</p>	<p>45. Close any open KVM Redirection session with the SUT via Intel® AMT.</p> <p>46. Close any VNC Viewer window which may still be open.</p>



ID:	AMT_043
Pass Criteria:	The test passes if all attempted KVM Redirection sessions are viewed via VNC Viewer on the management console, and keyboard/mouse functionality is redirected to the Host OS on the SUT. During system boot or resume, the Intel® MEBX hot-key (Ctrl+P or other keystroke) prompt is not displayed on the SUT.
References:	For details on KVM Redirection, refer the <i>Intel® ME BIOS Specification</i> .

11.8.6 KVM Redirection over Intel® AMT LAN Network Interface with User Consent Enabled

ID:	AMT_044			
Title:	Keyboard, Video, and Mouse (KVM) Redirection over Intel® AMT LAN Network Interface with User Consent Enabled			
Requirement:	Mandatory - exempt for systems which do not support KVM with internal graphics			
System:	Form Factor <input checked="" type="checkbox"/> Desktop <input checked="" type="checkbox"/> Workstation <input checked="" type="checkbox"/> Mobile	System Power Model <input checked="" type="checkbox"/> Standard <input checked="" type="checkbox"/> Modern Standby or InstantGo*	Intel® AMT Network Interface <input checked="" type="checkbox"/> LAN <input type="checkbox"/> Either Used <input type="checkbox"/> WLAN <input type="checkbox"/> Not Used	LAN Type <input checked="" type="checkbox"/> Integrated LAN <input type="checkbox"/> Discrete LAN <input type="checkbox"/> TBT Dock LAN
Method:	Automated by Intel® PETS with test operator interaction			
Description:	An Intel® AMT compliant system implements KVM redirection support when the system is in Sx state and moves to S0 state.			
Objective:	This test check that when the SUT moves from S3, S4 or S5, to S0 when KVM has been initiated, the BIOS halt and wait for the user to give consent for the KVM Redirection session, and the user consent opt-in option should be displayed on the platform under test. In all cases, the SUT's screen is visible in the Virtual Network Computing (VNC) Viewer on the management console.			
Setup:	The initial state of the SUT should be S0/MeOn with Host OS running. Intel® AMT should be provisioned via manual mode. Before running this test, ensure that KVM is enabled in the Intel® MEBX. If the SUT supports switchable graphics, graphics configuration should be set to integrated graphics.			
Procedure:	<ol style="list-style-type: none"> Set the active power package on the SUT to Power Package 2 (Intel® ME on in S0, wake in Sx/AC). Ensure the Intel® AMT redirection ports are enabled on the SUT. Cancel any existing Intel® AMT user consent session which may be active on the SUT. Ensure the Intel® AMT user consent opt-in setting is enabled on the SUT. Set the KVM password to 'Admin!98' on the SUT via Intel® AMT. Ensure that the VNC port 5900 is enabled on the SUT via Intel® AMT. 			
Procedure: (continued) S5→S0 Flow	<p>The remaining steps within this block is executed as if they are part of an independent sub-test. If a failure occurs at any point during the flow below, the remainder of the steps related to the sub-test, may be skipped.</p> <ol style="list-style-type: none"> Inform the test operator that the SUT soon be powered down and the VNC Viewer window opens. When the VNC Viewer window opens and the SUT starts to boot, request the test operator to: <ol style="list-style-type: none"> Verify that the Ctrl+P (or equivalent keystroke) Intel® MEBX prompt does not appear on the SUT screen during boot. Copy the user consent code from the SUT screen to the VNC Viewer. Try using the keyboard and mouse to control the Host OS. Gracefully shutdown to S5/MeOn the SUT via the Host OS and then wait 10 seconds. Open a KVM Redirection session with the SUT via Intel® AMT using the VNC Viewer on the management console. Perform a Remote Power-Up of the SUT via Intel® AMT. A user consent code is displayed on the SUT screen. Request the test operator to: <ol style="list-style-type: none"> Enter the user consent code into the VNC Viewer on the management console. Confirm that the redirected screen from the SUT appears in the VNC Viewer. Confirm that the keyboard and mouse can control the Host OS via the management console via the VNC Viewer. 			



ID:	AMT_044
<p>Procedure: (continued)</p> <p>S4→S0 Flow</p>	<p>12. Close any open KVM Redirection session with the SUT via Intel® AMT.</p> <p>13. Close any VNC Viewer window which may still be open.</p> <p>14. Cancel any existing Intel® AMT user consent session which may be active on the SUT.</p> <p>15. Attempt to bring the SUT to a base state via the following:</p> <ul style="list-style-type: none">a. Verify that the SUT is in S0/MeOn (CM0,CM0-PG).b. Verify that the Host OS on the SUT is available.c. Verify that Intel® AMT on the SUT responds to version queries via the LAN network interface. <p>If any of base state verification steps above fail, perform the following as an attempt to recover the SUT before attempting the base state verification steps above one last time.</p> <ul style="list-style-type: none">a. Bring the system to G3 and wait 10 seconds.b. Set system power configuration to AC/DC and wait another 10 seconds.c. Briefly press the Power Button on the SUT. <p>The remaining steps within this block is executed as if they are part of an independent sub-test. If a failure occurs at any point during the flow below, the remainder of the steps related to the sub-test, may be skipped.</p> <p>16. Inform the test operator that the SUT soon be sent into hibernation state and the VNC Viewer window opens. When the VNC Viewer window opens and the SUT starts to boot, request the test operator to:</p> <ul style="list-style-type: none">a. Verify that the Ctrl+P (or equivalent keystroke) Intel® MEBX prompt does not appear on the SUT screen during resume from hibernation.b. Copy the user consent code from the SUT screen to the VNC Viewer.c. Try using the keyboard and mouse to control the Host OS. <p>17. Hibernate to S4/MeOn the SUT via the Host OS and then wait 10 seconds.</p> <p>18. Open a KVM Redirection session with the SUT via Intel® AMT using the VNC Viewer on the management console.</p> <p>19. Perform a Remote Power-Up of the SUT via Intel® AMT. A user consent code is displayed on the SUT screen.</p> <p>20. Request the test operator to:</p> <ul style="list-style-type: none">a. Enter the user consent code into the VNC Viewer on the management console.b. Confirm that the redirected screen from the SUT appears in the VNC Viewer.c. Confirm that the keyboard and mouse can control the Host OS via the management console via the VNC Viewer.



ID:	AMT_044
Procedure: (continued) S3→S0 Flow	<p>21. Close any open KVM Redirection session with the SUT via Intel® AMT.</p> <p>22. Close any VNC Viewer window which may still be open.</p> <p>23. Cancel any existing Intel® AMT user consent session which may be active on the SUT.</p> <p>24. Attempt to bring the SUT to a base state via the following:</p> <ol style="list-style-type: none"> Verify that the SUT is in S0/MeOn (CM0,CM0-PG). Verify that the Host OS on the SUT is available. Verify that Intel® AMT on the SUT responds to version queries via the LAN network interface. <p>If any of base state verification steps above fail, perform the following as an attempt to recover the SUT before attempting the base state verification steps above one last time.</p> <ol style="list-style-type: none"> Bring the system to G3 and wait 10 seconds. Set system power configuration to AC/DC and wait another 10 seconds. Briefly press the Power Button on the SUT. <p>The remaining steps within this block is executed as if they are part of an independent sub-test. If a failure occurs at any point during the flow below, the remainder of the steps related to the sub-test, may be skipped</p> <p>NOTE: In the case the SUT is operating in Modern Standby or Microsoft Windows* InstantGo* mode, the test automatically end here, and the results thus far reported to the test operator as the final test results. For desktop systems with Intel® RMT support, ensure that Intel® RMT is disabled before running S3 test flows.</p> <p>25. Inform the test operator that the SUT soon be sent into suspend state and the VNC Viewer window opens. When the VNC Viewer window opens and the SUT starts to boot, request the test operator to:</p> <ol style="list-style-type: none"> Copy the user consent code from the SUT screen to the VNC Viewer. Try using the keyboard and mouse to control the Host OS. <p>26. Record the Host OS last boot time on the SUT (to verify successful suspend/resume).</p> <p>27. Suspend to S3/MeOn the SUT via the Host OS and then wait 10 seconds.</p> <p>28. Open a KVM Redirection session with the SUT via Intel® AMT using the VNC Viewer on the management console.</p> <p>29. Perform a Remote Power-Up of the SUT via Intel® AMT. A user consent code is displayed on the SUT screen.</p> <p>30. Wait until system resumes back to the Host OS.</p> <p>31. Verify the Host OS last boot time on the SUT does match the boot time recorded before the suspend.</p> <p>32. Request the test operator to:</p> <ol style="list-style-type: none"> Enter the user consent code into the VNC Viewer on the management console. Confirm that the redirected screen from the SUT appears in the VNC Viewer. Confirm that the keyboard and mouse can control the Host OS via the management console via the VNC Viewer.
Procedure: (continued)	<p>33. Close any open KVM Redirection session with the SUT via Intel® AMT.</p> <p>34. Close any VNC Viewer window which may still be open.</p> <p>35. Cancel any existing Intel® AMT user consent session which may be active on the SUT.</p>
Pass Criteria:	The test passes if all attempted KVM Redirection sessions are viewed via VNC Viewer on the management console, and keyboard/mouse functionality is redirected to the Host OS on the SUT. During system boot or resume, the Intel® MEBX hot-key (Ctrl+P or other keystroke) prompt is not displayed on the SUT. Additionally, no KVM redirection is permitted without first confirming the user consent code displayed on the SUT screen.
References:	For details on KVM Redirection, refer the <i>Intel® ME BIOS Specification</i> .

11.8.7 KVM Redirection over Intel® AMT WLAN Network Interface with User Consent Enabled

ID:	AMT_045			
Title:	Keyboard, Video, and Mouse (KVM) Redirection over Intel® AMT WLAN Network Interface with User Consent Enabled			
Requirement:	Mandatory - exempt for systems which do not support KVM with internal graphics			
System:	Form Factor	System Power Model	Intel® AMT Network Interface	LAN Type
	<input checked="" type="checkbox"/> Desktop <input checked="" type="checkbox"/> Workstation <input checked="" type="checkbox"/> Mobile	<input checked="" type="checkbox"/> Standard <input checked="" type="checkbox"/> Modern Standby or InstantGo*	<input type="checkbox"/> LAN <input type="checkbox"/> Either Used <input checked="" type="checkbox"/> WLAN <input type="checkbox"/> Not Used	<input type="checkbox"/> Integrated LAN <input type="checkbox"/> Discrete LAN <input type="checkbox"/> TBT Dock LAN



ID:	AMT_045
Method:	Automated by Intel® PETS with test operator interaction
Description:	An Intel® AMT compliant system implements KVM redirection support when the system is in Sx state and moves to S0 state.
Objective:	This test check that when the SUT moves from S3, S4 or S5, to S0 when KVM has been initiated, the BIOS halt and wait for the user to give consent for the KVM Redirection session, and the user consent opt-in option should be displayed on the platform under test. In all cases, the SUT's screen is visible in the Virtual Network Computing (VNC) Viewer on the management console.
Setup:	The initial state of the SUT should be S0/MeOn with Host OS running. Intel® AMT should be provisioned via manual mode. Before running this test, ensure that KVM is enabled in the Intel® MEBX. If the SUT supports switchable graphics, graphics configuration should be set to integrated graphics.
Procedure:	<ol style="list-style-type: none"> 1. Set the active power package on the SUT to Power Package 2 (Intel® ME on in S0, wake in Sx/AC). 2. Set the Intel® AMT WLAN link policy on the SUT to Link Policy 3 (Enabled in S0, Sx/AC). 3. Ensure the Host OS Wake on Wireless LAN is disabled. 4. Ensure the TCP maximum data retransmission setting defined in the SUT profile is applied to both a) the management console, and b) the SUT via Intel® AMT. If the configuration on the management console is not already aligned to the SUT profile setting, the network stack on the management console need to be reset; leading to potential network connectivity loss for other applications on the system. Before synchronizing the setting on the management console, provide a warning to the test operator, with the option to proceed or cancel, indicating the TCP maximum data retransmission network setting is about to be changed and that it may be necessary to re-establish network connectivity for any other applications running on the management console. If the test operator chooses to cancel, the test step is marked as failed. 5. Ensure the Intel® AMT redirection ports are enabled on the SUT. 6. Cancel any existing Intel® AMT user consent session which may be active on the SUT. 7. Ensure the Intel® AMT user consent opt-in setting is enabled on the SUT. 8. Set the KVM password to 'Admin!98' on the SUT via Intel® AMT. 9. Ensure that the VNC port 5900 is enabled on the SUT via Intel® AMT.
Procedure: (continued) S5→S0 Flow	<p>The remaining steps within this block is executed as if they are part of an independent sub-test. If a failure occurs at any point during the flow below, the remainder of the steps related to the sub-test, may be skipped.</p> <ol style="list-style-type: none"> 10. Inform the test operator that the SUT soon be powered down and the VNC Viewer window opens. When the VNC Viewer window opens and the SUT starts to boot, request the test operator to: <ol style="list-style-type: none"> a. Verify that the Ctrl+P (or equivalent keystroke) Intel® MEBX prompt does not appear on the SUT screen during boot. b. Copy the user consent code from the SUT screen to the VNC Viewer. c. Try using the keyboard and mouse to control the Host OS. 11. Gracefully shutdown to S5/MeOn the SUT via the Host OS and then wait 10 seconds. 12. Verify that Intel® AMT is available via WLAN by requesting its version. 13. Open a KVM Redirection session with the SUT via Intel® AMT using the VNC Viewer on the management console. 14. Perform a Remote Power-Up of the SUT via Intel® AMT. A user consent code is displayed on the SUT screen. 15. Request the test operator to: <ol style="list-style-type: none"> a. Enter the user consent code into the VNC Viewer on the management console. b. Confirm that the redirected screen from the SUT appears in the VNC Viewer. c. Confirm that the keyboard and mouse can control the Host OS via the management console via the VNC Viewer.



ID:	AMT_045
<p>Procedure: (continued) S4→S0 Flow</p>	<ol style="list-style-type: none"> 16. Close any open KVM Redirection session with the SUT via Intel® AMT. 17. Close any VNC Viewer window which may still be open. 18. Cancel any existing Intel® AMT user consent session which may be active on the SUT. 19. Attempt to bring the SUT to a base state via the following: <ol style="list-style-type: none"> a. Verify that the SUT is in S0/MeOn (CM0,CM0-PG). b. Verify that the Host OS on the SUT is available. c. Verify that Intel® AMT on the SUT responds to version queries via the WLAN network interface. <p>If any of base state verification steps above fail, perform the following as an attempt to recover the SUT before attempting the base state verification steps above one last time.</p> <ol style="list-style-type: none"> a. Bring the system to G3 and wait 10 seconds. b. Set system power configuration to AC/DC and wait another 10 seconds. c. Briefly press the Power Button on the SUT. <p>The remaining steps within this block is executed as if they are part of an independent sub-test. If a failure occurs at any point during the flow below, the remainder of the steps related to the sub-test, may be skipped.</p> 20. Inform the test operator that the SUT soon be sent into hibernation state and the VNC Viewer window opens. When the VNC Viewer window opens and the SUT starts to boot, request the test operator to: <ol style="list-style-type: none"> a. Verify that the Ctrl+P (or equivalent keystroke) Intel® MEBX prompt does not appear on the SUT screen during resume from hibernation. b. Copy the user consent code from the SUT screen to the VNC Viewer. c. Try using the keyboard and mouse to control the Host OS. 21. Hibernate to S4/MeOn the SUT via the Host OS and then wait 10 seconds. 22. Verify that Intel® AMT is available via WLAN by requesting its version. 23. Open a KVM Redirection session with the SUT via Intel® AMT using the VNC Viewer on the management console. 24. Perform a Remote Power-Up of the SUT via Intel® AMT. A user consent code is displayed on the SUT screen. 25. Request the test operator to: <ol style="list-style-type: none"> a. Enter the user consent code into the VNC Viewer on the management console. b. Confirm that the redirected screen from the SUT appears in the VNC Viewer. c. Confirm that the keyboard and mouse can control the Host OS via the management console via the VNC Viewer.

ID:	AMT_045
Procedure: (continued) S3→S0 Flow	<p>26. Close any open KVM Redirection session with the SUT via Intel® AMT.</p> <p>27. Close any VNC Viewer window which may still be open.</p> <p>28. Cancel any existing Intel® AMT user consent session which may be active on the SUT.</p> <p>29. Attempt to bring the SUT to a base state via the following:</p> <ol style="list-style-type: none"> Verify that the SUT is in S0/MeOn (CM0,CM0-PG). Verify that the Host OS on the SUT is available. Verify that Intel® AMT on the SUT responds to version queries via the WLAN network interface. <p>If any of base state verification steps above fail, perform the following as an attempt to recover the SUT before attempting the base state verification steps above one last time.</p> <ol style="list-style-type: none"> Bring the system to G3 and wait 10 seconds. Set system power configuration to AC/DC and wait another 10 seconds. Briefly press the Power Button on the SUT. <p>The remaining steps within this block is executed as if they are part of an independent sub-test. If a failure occurs at any point during the flow below, the remainder of the steps related to the sub-test, may be skipped.</p> <p>NOTE: In the case the SUT is operating in Modern Standby or Microsoft Windows* InstantGo* mode, the test automatically end here, and the results thus far reported to the test operator as the final test results. For desktop systems with Intel® RMT support, ensure that Intel® RMT is disabled before running S3 test flows.</p> <p>30. Inform the test operator that the SUT soon be sent into suspend state and the VNC Viewer window opens. When the VNC Viewer window opens and the SUT starts to boot, request the test operator to:</p> <ol style="list-style-type: none"> Copy the user consent code from the SUT screen to the VNC Viewer. Try using the keyboard and mouse to control the Host OS. <p>31. Record the Host OS last boot time on the SUT (to verify successful suspend/resume).</p> <p>32. Suspend to S3/MeOn the SUT via the Host OS and then wait 10 seconds.</p> <p>33. Verify that Intel® AMT is available via WLAN by requesting its version.</p> <p>34. Open a KVM Redirection session with the SUT via Intel® AMT using the VNC Viewer on the management console.</p> <p>35. Perform a Remote Power-Up of the SUT via Intel® AMT. A user consent code is displayed on the SUT screen.</p> <p>36. Wait until system resumes back to the Host OS.</p> <p>37. Verify the Host OS last boot time on the SUT does match the boot time recorded before the suspend.</p> <p>38. Request the test operator to:</p> <ol style="list-style-type: none"> Enter the user consent code into the VNC Viewer on the management console. Confirm that the redirected screen from the SUT appears in the VNC Viewer. Confirm that the keyboard and mouse can control the Host OS via the management console via the VNC Viewer.
Procedure: (continued)	<p>39. Close any open KVM Redirection session with the SUT via Intel® AMT.</p> <p>40. Close any VNC Viewer window which may still be open.</p> <p>41. Cancel any existing Intel® AMT user consent session which may be active on the SUT.</p>
Pass Criteria:	The test passes if all attempted KVM Redirection sessions are viewed via VNC Viewer on the management console, and keyboard/mouse functionality is redirected to the Host OS on the SUT. During system boot or resume, the Intel® MEBX hot-key (Ctrl+P or other keystroke) prompt is not displayed on the SUT. Additionally, no KVM redirection is permitted without first confirming the user consent code displayed on the SUT screen.
References:	For details on KVM Redirection, refer the <i>Intel® ME BIOS Specification</i> .

11.8.8 KVM Redirection during Warm Reset over Intel® AMT LAN Network Interface

ID:	AMT_046			
Title:	Keyboard, Video, and Mouse (KVM) Redirection during Warm Reset over Intel® AMT LAN Network Interface			
Requirement:	Mandatory - exempt for systems which do not support KVM with internal graphics			
System:	Form Factor	System Power Model	Intel® AMT Network Interface	LAN Type
	<input checked="" type="checkbox"/> Desktop <input checked="" type="checkbox"/> Workstation <input checked="" type="checkbox"/> Mobile	<input checked="" type="checkbox"/> Standard <input checked="" type="checkbox"/> Modern Standby or InstantGo*	<input checked="" type="checkbox"/> LAN <input type="checkbox"/> Either Used <input type="checkbox"/> WLAN <input type="checkbox"/> Not Used	<input checked="" type="checkbox"/> Integrated LAN <input type="checkbox"/> Discrete LAN <input type="checkbox"/> TBT Dock LAN



ID:	AMT_046
Method:	Automated by Intel® PETS with test operator interaction
Description:	An Intel® AMT compliant system implements KVM redirection support during warm reset.
Objective:	This test check that when the SUT experiences a warm reset that an open KVM Redirection session remains connected throughout. Additionally, when a User Consent session is established, a new session is not requested as a result of the warm reset.
Setup:	The initial state of the SUT should be S0/MeOn with Host OS running. Intel® AMT should be provisioned via manual mode. Before running this test, ensure that KVM is enabled in the Intel® MEBX. If the SUT supports switchable graphics, graphics configuration should be set to integrated graphics.
Procedure:	<ol style="list-style-type: none"> 1. Set the active power package on the SUT to Power Package 1 (Intel® ME on in S0). 2. Ensure the Intel® AMT redirection ports are enabled on the SUT. 3. Cancel any existing Intel® AMT user consent session which may be active on the SUT. 4. Ensure the Intel® AMT user consent opt-in setting is enabled on the SUT. 5. Set the KVM password to 'Admin!98' on the SUT via Intel® AMT. 6. Ensure that the VNC port 5900 is enabled on the SUT via Intel® AMT.
Procedure: (continued)	<p>The remaining steps within this block is executed as if they are part of an independent sub-test. If a failure occurs at any point during the flow below, the remainder of the steps related to the sub-test, may be skipped.</p> <ol style="list-style-type: none"> 7. Inform the test operator that the VNC Viewer window opens, and that when it does: <ol style="list-style-type: none"> a. Copy the user consent code from the SUT screen to the VNC Viewer. b. Try using the keyboard and mouse to control the Host OS. 8. Open a KVM Redirection session with the SUT via Intel® AMT using the VNC Viewer on the management console. 9. Request the test operator to: <ol style="list-style-type: none"> a. Enter the user consent code into the VNC Viewer on the management console. b. Confirm that the redirected screen from the SUT appears in the VNC Viewer. c. Confirm that the keyboard and mouse can control the Host OS via the management console via the VNC Viewer.
Procedure: (continued) S0→S0 Flow	<p>The steps within this block is executed as if they are part of an independent sub-test. If a failure occurs at any point during the flow below, the remainder of the steps related to the sub-test, may be skipped.</p> <ol style="list-style-type: none"> 10. Inform the test operator that the SUT soon be restarted, and to try using the keyboard and mouse to control the Host OS afterwards. 11. Perform a Remote Reset of the SUT via Intel® AMT. 12. Wait until system reboots back to the Host OS. 13. Request the test operator to: <ol style="list-style-type: none"> a. Confirm that the SUT did not display a user consent code following the reset. b. Confirm that the VNC Viewer on the management console did not request a user consent code following the reset. c. Confirm that the redirected screen from the SUT appears in the VNC Viewer. d. Confirm that the keyboard and mouse can control the Host OS via the management console via the VNC Viewer. 14. Perform the following additional sub-steps for two (2) cycles each: <ol style="list-style-type: none"> a. Verify that the Host OS on the SUT is available. b. Record the Host OS last boot time on the SUT (to verify successful restart). c. Perform a graceful restart of the SUT via Host OS. d. Verify that the SUT is in S0/MeOn (CM0,CM0-PG). e. Verify the Host OS last boot time on the SUT does not match the boot time recorded before the restart.
Procedure: (continued)	<ol style="list-style-type: none"> 15. Attempt to bring the SUT to a base state via the following: <ol style="list-style-type: none"> a. Verify that the SUT is in S0/MeOn (CM0,CM0-PG). b. Verify that the Host OS on the SUT is available. c. Verify that Intel® AMT on the SUT responds to version queries via the LAN network interface. <p>If any of base state verification steps above fail, perform the following as an attempt to recover the SUT before attempting the base state verification steps above one last time.</p> <ol style="list-style-type: none"> a. Bring the system to G3 and wait 10 seconds. b. Set system power configuration to AC/DC and wait another 10 seconds. c. Briefly press the Power Button on the SUT. 16. Close any open KVM Redirection session with the SUT via Intel® AMT. 17. Close any VNC Viewer window which may still be open. 18. Cancel any existing Intel® AMT user consent session which may be active on the SUT.
Pass Criteria:	The test passes if the KVM Redirection session remains up and the platform under test screen visible on the remote viewer, including BIOS screens, during the warm reset, and that when passcode is entered before the warm reset, the system does not display the user consent code.



ID:	AMT_046
References:	For details on KVM Redirection, refer the <i>Intel® ME BIOS Specification</i> .

11.8.9 KVM Redirection during Warm Reset over Intel® AMT WLAN Network Interface

ID:	AMT_047			
Title:	Keyboard, Video, and Mouse (KVM) Redirection during Warm Reset over Intel® AMT WLAN Network Interface			
Requirement:	Mandatory - exempt for systems which do not support KVM with internal graphics			
System:	<div>Form Factor</div> <div><input checked="" type="checkbox"/> Desktop <input checked="" type="checkbox"/> Workstation <input checked="" type="checkbox"/> Mobile</div>	<div>System Power Model</div> <div><input checked="" type="checkbox"/> Standard <input checked="" type="checkbox"/> Modern Standby or InstantGo*</div>	<div>Intel® AMT Network Interface</div> <div><input type="checkbox"/> LAN <input type="checkbox"/> Either Used <input checked="" type="checkbox"/> WLAN <input type="checkbox"/> Not Used</div>	<div>LAN Type</div> <div><input type="checkbox"/> Integrated LAN <input type="checkbox"/> Discrete LAN <input type="checkbox"/> TBT Dock LAN</div>
Method:	Automated by Intel® PETS with test operator interaction			
Description:	An Intel® AMT compliant system implements KVM redirection support during warm reset.			
Objective:	This test check that when the SUT experiences a warm reset that an open KVM Redirection session remains connected throughout. Additionally, when a User Consent session is established, a new session is not requested as a result of the warm reset.			
Setup:	The initial state of the SUT should be S0/MeOn with Host OS running. Intel® AMT should be provisioned via manual mode. Before running this test, ensure that KVM is enabled in the Intel® MEBX. If the SUT supports switchable graphics, graphics configuration should be set to integrated graphics.			
Procedure:	<div>1. Set the active power package on the SUT to Power Package 1 (Intel® ME on in S0).</div> <div>2. Set the Intel® AMT WLAN link policy on the SUT to Link Policy 2 (Enabled in S0).</div> <div>3. Ensure the TCP maximum data retransmission setting defined in the SUT profile is applied to both a) the management console, and b) the SUT via Intel® AMT. If the configuration on the management console is not already aligned to the SUT profile setting, the network stack on the management console need to be reset; leading to potential network connectivity loss for other applications on the system. Before synchronizing the setting on the management console, provide a warning to the test operator, with the option to proceed or cancel, indicating the TCP maximum data retransmission network setting is about to be changed and that it may be necessary to re-establish network connectivity for any other applications running on the management console. If the test operator chooses to cancel, the test step is marked as failed.</div> <div>4. Ensure the Intel® AMT redirection ports are enabled on the SUT.</div> <div>5. Cancel any existing Intel® AMT user consent session which may be active on the SUT.</div> <div>6. Ensure the Intel® AMT user consent opt-in setting is enabled on the SUT.</div> <div>7. Set the KVM password to 'Admin!98' on the SUT via Intel® AMT.</div> <div>8. Ensure that the VNC port 5900 is enabled on the SUT via Intel® AMT.</div>			
Procedure: (continued)	<div>The remaining steps within this block is executed as if they are part of an independent sub-test. If a failure occurs at any point during the flow below, the remainder of the steps related to the sub-test, may be skipped.</div> <div>9. Inform the test operator that the VNC Viewer window opens, and that when it does:<div>a. Copy the user consent code from the SUT screen to the VNC Viewer.</div><div>b. Try using the keyboard and mouse to control the Host OS.</div></div> <div>10. Verify that Intel® AMT is available via WLAN by requesting its version.</div> <div>11. Open a KVM Redirection session with the SUT via Intel® AMT using the VNC Viewer on the management console.</div> <div>12. Request the test operator to:<div>a. Enter the user consent code into the VNC Viewer on the management console.</div><div>b. Confirm that the redirected screen from the SUT appears in the VNC Viewer.</div><div>c. Confirm that the keyboard and mouse can control the Host OS via the management console via the VNC Viewer.</div></div>			



ID:	AMT_047
Procedure: (continued) S0→S0 Flow	<p>The steps within this block is executed as if they are part of an independent sub-test. If a failure occurs at any point during the flow below, the remainder of the steps related to the sub-test, may be skipped.</p> <ol style="list-style-type: none"> 13. Inform the test operator that the SUT soon be restarted, and to try using the keyboard and mouse to control the Host OS afterwards. 14. Perform a Remote Reset of the SUT via Intel® AMT. 15. Wait until system reboots back to the Host OS. 16. Verify that Intel® AMT is available via WLAN by requesting its version. 17. Request the test operator to: <ol style="list-style-type: none"> a. Confirm that the SUT did not display a user consent code following the reset. b. Confirm that the VNC Viewer on the management console did not request a user consent code following the reset. c. Confirm that the redirected screen from the SUT appears in the VNC Viewer. d. Confirm that the keyboard and mouse can control the Host OS via the management console via the VNC Viewer. 18. Perform the following additional sub-steps for two (2) cycles each: <ol style="list-style-type: none"> a. Verify that the Host OS on the SUT is available. b. Record the Host OS last boot time on the SUT (to verify successful restart). c. Perform a graceful restart of the SUT via Host OS. d. Verify that the SUT is in S0/MeOn (CM0,CM0-PG). e. Verify the Host OS last boot time on the SUT does not match the boot time recorded before the restart.
Procedure: (continued)	<ol style="list-style-type: none"> 19. Attempt to bring the SUT to a base state via the following: <ol style="list-style-type: none"> a. Verify that the SUT is in S0/MeOn (CM0,CM0-PG). b. Verify that the Host OS on the SUT is available. c. Verify that Intel® AMT on the SUT responds to version queries via the WLAN network interface. <p>If any of base state verification steps above fail, perform the following as an attempt to recover the SUT before attempting the base state verification steps above one last time.</p> <ol style="list-style-type: none"> a. Bring the system to G3 and wait 10 seconds. b. Set system power configuration to AC/DC and wait another 10 seconds. c. Briefly press the Power Button on the SUT. 20. Close any open KVM Redirection session with the SUT via Intel® AMT. 21. Close any VNC Viewer window which may still be open. 22. Cancel any existing Intel® AMT user consent session which may be active on the SUT.
Pass Criteria:	The test passes if the KVM Redirection session remains up and the platform under test screen visible on the remote viewer, including BIOS screens, during the warm reset, and that when passcode is entered before the warm reset, the system does not display the user consent code.
References:	For details on KVM Redirection, refer the <i>Intel® ME BIOS Specification</i> .

11.8.10 KVM Redirection with S0 Low Power Idle via Intel® AMT LAN Network Interface

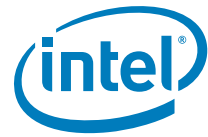
ID:	AMT_048					
Title:	Keyboard, Video, and Mouse (KVM) Redirection with S0 Low Power Idle state, as with Modern Standby or Microsoft Windows* InstantGo* mode, via Intel® AMT LAN Network Interface					
Requirement:	Mandatory - exempt for systems which do not support KVM with internal graphics					
System:	Form Factor		System Power Model	Intel® AMT Network Interface		LAN Type
	<input checked="" type="checkbox"/> Desktop <input checked="" type="checkbox"/> Mobile	<input type="checkbox"/> Workstation	<input type="checkbox"/> Standard <input checked="" type="checkbox"/> Modern Standby or InstantGo*	<input checked="" type="checkbox"/> LAN <input type="checkbox"/> WLAN	<input type="checkbox"/> Either Used <input type="checkbox"/> Not Used	<input checked="" type="checkbox"/> Integrated LAN <input type="checkbox"/> Discrete LAN <input type="checkbox"/> TBT Dock LAN
Method:	Automated by Intel® PETS with test operator interaction					
Description:	An Intel® AMT compliant system implements KVM redirection support when the system is in S0 Low Power Idle state and move to S0 state.					
Objective:	This test check that the SUT moves from S0 Low Power Idle state to S0 when KVM has been initiated.					



ID:	AMT_048
Setup:	The initial state of the SUT should be S0/MeOn with Host OS running. Intel® AMT should be provisioned via manual mode. Before running this test, ensure that KVM is enabled in the Intel® MEBX. If the SUT supports switchable graphics, graphics configuration should be set to integrated graphics. The SUT must be configured to work in Modern Standby or Microsoft Windows* InstantGo* mode.
Procedure:	<ol style="list-style-type: none">1. Set the active power package on the SUT to Power Package 1 (Intel® ME on in S0).2. Ensure the Intel® AMT redirection ports are enabled on the SUT.3. Cancel any existing Intel® AMT user consent session which may be active on the SUT.4. Ensure the Intel® AMT user consent opt-in setting is disabled on the SUT.5. Set the KVM password to 'Admin!98' on the SUT via Intel® AMT.6. Ensure that the VNC port 5900 is enabled on the SUT via Intel® AMT.
Procedure: (continued) S0LP→S0 Flow	<p>The steps within this block is executed as if they are part of an independent sub-test. If a failure occurs at any point during the flow below, the remainder of the steps related to the sub-test, may be skipped.</p> <ol style="list-style-type: none">7. Inform the test operator that after SUT enters S0 Low Power Idle state, the VNC Viewer window opens. When the VNC Viewer window opens, request the test operator to try using the keyboard and mouse to Activate and control the Host OS on the SUT.8. Request the test operator to manually place the SUT into S0 Low Power Idle state.9. Verify that the SUT has moved into S0 Low Power Idle state.10. Open a KVM Redirection session with the SUT via Intel® AMT using the VNC Viewer on the management console.11. Request the test operator to:<ol style="list-style-type: none">a. Confirm that the redirected screen from the SUT appears in the VNC Viewer.b. Confirm that the keyboard and mouse can control the Host OS via the management console via the VNC Viewer.
Procedure: (continued)	<ol style="list-style-type: none">12. Close any open KVM Redirection session with the SUT via Intel® AMT.13. Close any VNC Viewer window which may still be open.
Pass Criteria:	The test passes if the KVM Redirection session can be viewed via VNC Viewer on the management console, and keyboard/mouse functionality is redirected to the Host OS on the SUT.
References:	For details on KVM Redirection, refer the <i>Intel® ME BIOS Specification</i> .

11.8.11 KVM Redirection with S0 Low Power Idle via Intel® AMT WLAN Network Interface

ID:	AMT_049					
Title:	Keyboard, Video, and Mouse (KVM) Redirection with S0 Low Power Idle state, as with Modern Standby or Microsoft* Windows* InstantGo* mode, via Intel® AMT WLAN Network Interface					
Requirement:	Mandatory - exempt for systems which do not support KVM with internal graphics					
System:	Form Factor		System Power Model	Intel® AMT Network Interface		LAN Type
	<input checked="" type="checkbox"/> Desktop <input type="checkbox"/> Mobile <input type="checkbox"/> Workstation	<input type="checkbox"/> Standard <input checked="" type="checkbox"/> Modern Standby or InstantGo*	<input type="checkbox"/> LAN <input type="checkbox"/> Either Used <input checked="" type="checkbox"/> WLAN <input type="checkbox"/> Not Used	<input type="checkbox"/> Integrated LAN <input type="checkbox"/> Discrete LAN <input type="checkbox"/> TBT Dock LAN		
Method:	Automated by Intel® PETS with test operator interaction					
Description:	An Intel® AMT compliant system implements KVM redirection support when the system is in S0 Low Power Idle state and move to S0 state.					
Objective:	This test check that the SUT moves from S0 Low Power Idle state to S0 when KVM has been initiated.					
Setup:	The initial state of the SUT should be S0/MeOn with Host OS running. Intel® AMT should be provisioned via manual mode. Before running this test, ensure that KVM is enabled in the Intel® MEBX. If the SUT supports switchable graphics, graphics configuration should be set to integrated graphics. The SUT must be configured to work in Modern Standby or Microsoft Windows* InstantGo* mode.					



ID:	AMT_049
Procedure:	<ol style="list-style-type: none"> 1. Set the active power package on the SUT to Power Package 1 (Intel® ME on in S0). 2. Set the Intel® AMT WLAN link policy on the SUT to Link Policy 2 (Enabled in S0). 3. Ensure the TCP maximum data retransmission setting defined in the SUT profile is applied to both a) the management console, and b) the SUT via Intel® AMT. If the configuration on the management console is not already aligned to the SUT profile setting, the network stack on the management console need to be reset; leading to potential network connectivity loss for other applications on the system. Before synchronizing the setting on the management console, provide a warning to the test operator, with the option to proceed or cancel, indicating the TCP maximum data retransmission network setting is about to be changed and that it may be necessary to re-establish network connectivity for any other applications running on the management console. If the test operator chooses to cancel, the test step is marked as failed. 4. Ensure the Intel® AMT redirection ports are enabled on the SUT. 5. Cancel any existing Intel® AMT user consent session which may be active on the SUT. 6. Ensure the Intel® AMT user consent opt-in setting is disabled on the SUT. 7. Set the KVM password to 'Admin!98' on the SUT via Intel® AMT. 8. Ensure that the VNC port 5900 is enabled on the SUT via Intel® AMT.
Procedure: (continued) S0LP→S0 Flow	<p>The steps within this block is executed as if they are part of an independent sub-test. If a failure occurs at any point during the flow below, the remainder of the steps related to the sub-test, may be skipped.</p> <ol style="list-style-type: none"> 9. Inform the test operator that after SUT enters S0 Low Power Idle state, the VNC Viewer window opens. When the VNC Viewer window opens, request the test operator to try using the keyboard and mouse to Activate and control the Host OS on the SUT. 10. Request the test operator to manually place the SUT into S0 Low Power Idle state. 11. Verify that the SUT has moved into S0 Low Power Idle state. 12. Verify that Intel® AMT is available via WLAN by requesting its version. 13. Open a KVM Redirection session with the SUT via Intel® AMT using the VNC Viewer on the management console. 14. Request the test operator to: <ol style="list-style-type: none"> a. Confirm that the redirected screen from the SUT appears in the VNC Viewer. b. Confirm that the keyboard and mouse can control the Host OS via the management console via the VNC Viewer.
Procedure: (continued)	Close any open KVM Redirection session with the SUT via Intel® AMT. Close any VNC Viewer window which may still be open.
Pass Criteria:	The test passes if the KVM Redirection session can be viewed via VNC Viewer on the management console, and keyboard/mouse functionality is redirected to the Host OS on the SUT.
References:	For details on KVM Redirection, refer the <i>Intel® ME BIOS Specification</i> .

11.8.12 KVM Redirection in Discrete Graphics Mode

ID:	AMT_050						
Title:	Keyboard, Video, and Mouse (KVM) Redirection in Discrete Graphics Mode						
Requirement:	Mandatory - exempt for systems which do not have both internal and discrete graphics						
System:	Form Factor		System Power Model		Intel® AMT Network Interface		LAN Type
	<input checked="" type="checkbox"/> Desktop <input checked="" type="checkbox"/> Workstation <input checked="" type="checkbox"/> Mobile		<input checked="" type="checkbox"/> Standard <input checked="" type="checkbox"/> Modern Standby or InstantGo*		<input type="checkbox"/> LAN <input checked="" type="checkbox"/> Either Used <input type="checkbox"/> WLAN <input type="checkbox"/> Not Used		<input checked="" type="checkbox"/> Integrated LAN <input type="checkbox"/> Discrete LAN <input type="checkbox"/> TBT Dock LAN
Method:	Automated by Intel® PETS with test operator interaction						
Description:	This test checks SUT behavior when a KVM Redirection session is initiated while the system is in discrete graphics mode.						
Objective:	This test ensure that the KVM Redirection session fails to start when the SUT is operating in discrete graphics mode.						
Setup:	The initial state of the SUT should be S0/MeOn with Host OS running. Intel® AMT should be provisioned via manual mode. Before running this test, ensure that KVM is enabled in the Intel® MEBX. The graphics configuration should be set to discrete graphics.						



ID:	AMT_050
Procedure:	<ol style="list-style-type: none"> 1. Set the active power package on the SUT to Power Package 1 (Intel® ME on in S0). 2. Set the Intel® AMT WLAN link policy on the SUT to Link Policy 2 (Enabled in S0), if the WLAN network interface is used. 3. Ensure the TCP maximum data retransmission setting defined in the SUT profile is applied to both a) the management console, and b) the SUT via Intel® AMT, if the WLAN network interface is used. If the configuration on the management console is not already aligned to the SUT profile setting, the network stack on the management console need to be reset; leading to potential network connectivity loss for other applications on the system. Before synchronizing the setting on the management console, provide a warning to the test operator, with the option to proceed or cancel, indicating the TCP maximum data retransmission network setting is about to be changed and that it may be necessary to re-establish network connectivity for any other applications running on the management console. If the test operator chooses to cancel, the test step is marked as failed. 4. Ensure the Intel® AMT redirection ports are enabled on the SUT. 5. Cancel any existing Intel® AMT user consent session which may be active on the SUT. 6. Ensure the Intel® AMT user consent opt-in setting is disabled on the SUT. 7. Set the KVM password to 'Admin!98' on the SUT via Intel® AMT. 8. Ensure that the VNC port 5900 is enabled on the SUT via Intel® AMT. 9. Inform the test operator that the VNC Viewer attempt to open. Request the test operator to wait at least 30 seconds to confirm the KVM Redirection session failed to start. 10. Open a KVM Redirection session with the SUT via Intel® AMT using the VNC Viewer on the management console. 11. Request the test operator to confirm that the KVM Redirection session did not start.
Pass Criteria:	The test passes if the KVM Redirection session fails to start.
References:	For details on KVM Redirection, refer the <i>Intel® ME BIOS Specification</i> .

11.8.13 KVM Redirection and Switchable Graphics

ID:	AMT_051					
Title:	Keyboard, Video, and Mouse (KVM) Redirection and Switchable Graphics					
Requirement:	Mandatory - exempt for systems which do not have both internal and discrete graphics					
System:	Form Factor		System Power Model	Intel® AMT Network Interface		LAN Type
	<input checked="" type="checkbox"/> Desktop <input checked="" type="checkbox"/> Mobile	<input checked="" type="checkbox"/> Workstation	<input checked="" type="checkbox"/> Standard <input checked="" type="checkbox"/> Modern Standby or InstantGo*	<input type="checkbox"/> LAN <input type="checkbox"/> WLAN	<input checked="" type="checkbox"/> Either Used <input type="checkbox"/> Not Used	<input checked="" type="checkbox"/> Integrated LAN <input type="checkbox"/> Discrete LAN <input type="checkbox"/> TBT Dock LAN
Method:	Automated by Intel® PETS with test operator interaction					
Description:	This test checks SUT behavior when a KVM Redirection session is initiated while the system is in integrated graphics mode and then switched to discrete graphics mode.					
Objective:	This test ensure that the Graphics Device Interface (GDI) alerts the Intel® ME when it switches to discrete graphics mode. The Intel® ME should display the proper error when this condition occurs. Switching may be done by means of the switchable graphics control application (not provided by Intel).					
Setup:	The initial state of the SUT should be S0/MeOn with Host OS running. Intel® AMT should be provisioned via manual mode. Before running this test, ensure that KVM is enabled in the Intel® MEBX. The graphics configuration should be set to integrated graphics.					



ID:	AMT_051
Procedure:	<ol style="list-style-type: none"> 1. Set the active power package on the SUT to Power Package 1 (Intel® ME on in S0). 2. Set the Intel® AMT WLAN link policy on the SUT to Link Policy 2 (Enabled in S0), if the WLAN network interface is used. 3. Ensure the TCP maximum data retransmission setting defined in the SUT profile is applied to both a) the management console, and b) the SUT via Intel® AMT, if the WLAN network interface is used. <p>If the configuration on the management console is not already aligned to the SUT profile setting, the network stack on the management console need to be reset; leading to potential network connectivity loss for other applications on the system.</p> <p>Before synchronizing the setting on the management console, provide a warning to the test operator, with the option to proceed or cancel, indicating the TCP maximum data retransmission network setting is about to be changed and that it may be necessary to re-establish network connectivity for any other applications running on the management console. If the test operator chooses to cancel, the test step is marked as failed.</p> <ol style="list-style-type: none"> 4. Ensure the Intel® AMT redirection ports are enabled on the SUT. 5. Cancel any existing Intel® AMT user consent session which may be active on the SUT. 6. Ensure the Intel® AMT user consent opt-in setting is disabled on the SUT. 7. Set the KVM password to 'Admin!98' on the SUT via Intel® AMT. 8. Ensure that the VNC port 5900 is enabled on the SUT via Intel® AMT.
Procedure: (continued)	<p>The steps within this block is executed as if they are part of an independent sub-test. If a failure occurs at any point during the flow below, the remainder of the steps related to the sub-test, may be skipped.</p> <ol style="list-style-type: none"> 9. Inform the test operator that the VNC Viewer soon open. 10. Open a KVM Redirection session with the SUT via Intel® AMT using the VNC Viewer on the management console. 11. Request the test operator to: <ol style="list-style-type: none"> a. Confirm that the redirected screen from the SUT appears in the VNC Viewer. b. Confirm that the keyboard and mouse can control the Host OS via the management console via the VNC Viewer. c. Change the SUT from integrated graphics mode to discrete graphics mode. <p>NOTE: The KVM Redirection session should automatically disconnect.</p> <ol style="list-style-type: none"> d. Wait at least 30 seconds to confirm the KVM Redirection session closed. e. Change the SUT back to integrated graphics mode from discrete graphics mode.
Procedure: (continued)	<ol style="list-style-type: none"> 12. Close any open KVM Redirection session with the SUT via Intel® AMT. 13. Close any VNC Viewer window which may still be open.
Pass Criteria:	The test passes if KVM Redirection session is disconnected.
References:	For details on KVM Redirection, refer the <i>Intel® ME BIOS Specification</i> .

11.8.14 KVM with SOL and Storage Redirection

ID:	AMT_052				
Title:	Keyboard, Video, and Mouse (KVM) with Serial-Over-LAN (SOL) and Storage Redirection				
Requirement:	Mandatory - exempt for systems which do not support KVM with internal graphics				
System:	Form Factor		System Power Model	Intel® AMT Network Interface	LAN Type
	<input checked="" type="checkbox"/> Desktop <input checked="" type="checkbox"/> Mobile	<input checked="" type="checkbox"/> Workstation	<input checked="" type="checkbox"/> Standard <input checked="" type="checkbox"/> Modern Standby or InstantGo*	<input type="checkbox"/> LAN <input type="checkbox"/> WLAN	<input checked="" type="checkbox"/> Either Used <input type="checkbox"/> Not Used
Method:	Automated by Intel® PETS with test operator interaction				
Description:	This test checks that SOL and Storage Redirection can be activated during an open KVM Redirection session between a management console and the SUT.				
Objective:	Verify that the BIOS detects, and executes, a request (by using boot options) to perform SOL Redirection and map an ISO OS image to a drive via Storage Redirection during an active KVM Redirection session.				
Setup:	The initial state of the SUT should be S0/MeOn with Host OS running. Intel® AMT should be provisioned via manual mode. Before running this test, ensure that KVM, SOL, and Storage Redirection are enabled in the Intel® MEBX. If the SUT supports switchable graphics, graphics configuration should be set to integrated graphics.				

ID:	AMT_052
Procedure:	<ol style="list-style-type: none"> 1. Set the active power package on the SUT to Power Package 2 (Intel® ME on in S0, wake in Sx/AC). 2. Set the Intel® AMT WLAN link policy on the SUT to Link Policy 3 (Enabled in S0, Sx/AC), if the WLAN network interface is used. 3. Ensure the TCP maximum data retransmission setting defined in the SUT profile is applied to both a) the management console, and b) the SUT via Intel® AMT, if the WLAN network interface is used. If the configuration on the management console is not already aligned to the SUT profile setting, the network stack on the management console need to be reset; leading to potential network connectivity loss for other applications on the system. Before synchronizing the setting on the management console, provide a warning to the test operator, with the option to proceed or cancel, indicating the TCP maximum data retransmission network setting is about to be changed and that it may be necessary to re-establish network connectivity for any other applications running on the management console. If the test operator chooses to cancel, the test step is marked as failed. 4. Ensure the Intel® AMT redirection ports are enabled on the SUT. 5. Cancel any existing Intel® AMT user consent session which may be active on the SUT. 6. Ensure the Intel® AMT user consent opt-in setting is disabled on the SUT. 7. Set the KVM password to 'Admin!98' on the SUT via Intel® AMT. 8. Ensure that the VNC port 5900 is enabled on the SUT via Intel® AMT.
Procedure: (continued) S0→S0 Flow	<p>The steps within this block is executed as if they are part of an independent sub-test. If a failure occurs at any point during the flow below, the remainder of the steps related to the sub-test, may be skipped.</p> <ol style="list-style-type: none"> 9. Inform the test operator that the VNC Viewer soon open. 10. Open a KVM Redirection session with the SUT via Intel® AMT using the VNC Viewer on the management console. 11. Request the test operator to: <ol style="list-style-type: none"> a. Confirm that the redirected screen from the SUT appears in the VNC Viewer. b. Confirm that the keyboard and mouse can control the Host OS via the management console via the VNC Viewer. 12. Use Intel® AMT to set the SUT boot options to use SOL Redirection on the next boot. 13. Inform the test operator that a system reboot is performed by Intel® PETS requesting that the BIOS boot with text output redirected via Serial-Over-LAN. 14. Open a SOL Redirection session with the SUT via Intel® AMT using the Putty terminal program on the management console. 15. Open a Storage Redirection session with the SUT via Intel® AMT using an ISO OS image on the management console. 16. Perform a graceful Restart via the Host OS. 17. Wait until system reboots back to the Host OS. 18. Verify the Intel® AMT SOL device on the SUT exists and is operating normally. 19. Request the test operator to: <ol style="list-style-type: none"> a. Confirm that the Storage Image appears as a mapped drive in the Host OS. b. Confirm that the redirected screen from the SUT still appears in the VNC Viewer. c. Confirm that the keyboard and mouse can still control the Host OS via the management console via the VNC Viewer. d. Confirm that the redirected text from the BIOS boot flow was displayed in the Putty window.
Procedure: (continued)	<ol style="list-style-type: none"> 20. Close any open KVM Redirection session with the SUT via Intel® AMT. 21. Close any open Storage Redirection session with the SUT via Intel® AMT. 22. Close any open SOL Redirection session with the SUT via Intel® AMT. 23. Close any VNC Viewer window which may still be open. 24. Close any Putty terminal window which may still be open.
Pass Criteria:	The test passes if SOL and Storage Redirection sessions were successfully completed while the KVM Redirection session was running, and the mapped Storage Redirection drive is accessible from the Host OS of the SUT.
References:	For details on KVM, SOL and Storage Redirection, refer the <i>Intel® ME BIOS Specification</i> .

11.8.15 KVM Redirection and USB Port Availability Check

ID:	AMT_053
Title:	Keyboard, Video, and Mouse (KVM) Redirection and USB Port Availability Check
Requirement:	Mandatory - exempt for systems which do not support KVM with internal graphics



ID:	AMT_053			
System:	Form Factor	System Power Model	Intel® AMT Network Interface	LAN Type
	<input checked="" type="checkbox"/> Desktop <input checked="" type="checkbox"/> Workstation <input checked="" type="checkbox"/> Mobile	<input checked="" type="checkbox"/> Standard <input checked="" type="checkbox"/> Modern Standby or InstantGo*	<input type="checkbox"/> LAN <input checked="" type="checkbox"/> Either Used <input type="checkbox"/> WLAN <input type="checkbox"/> Not Used	<input checked="" type="checkbox"/> Integrated LAN <input type="checkbox"/> Discrete LAN <input type="checkbox"/> TBT Dock LAN
Method:	Automated by Intel® PETS with test operator interaction			
Description:	This test checks that all USB ports of the SUT are working correctly during a KVM Redirection session.			
Objective:	<p>Verify that the BIOS properly enables USB ports other than those needed for KVM Redirection support during a KVM Redirection session.</p> <p>This test is run once with the SUT configured to enable USB 2.0, and once more with the SUT configured to enable USB 3.0 where supported. If only one of those versions of USB is supported on the SUT, then this test is run once with the SUT configured to enable the supported USB version.</p>			
Setup:	<p>The initial state of the SUT should be S0/MeOn with Host OS running. Intel® AMT should be provisioned via manual mode. Before running this test, ensure that KVM Redirection is enabled in the Intel® MEBX. If the SUT supports switchable graphics, graphics configuration should be set to integrated graphics.</p> <p>The USB Storage device (USB Key) used in the test may be either USB 2.0 or USB 3.0 compliant, depending on what the SUT can support. If the SUT can support both USB 2.0 and USB 3.0, the USB Storage device should be the lower of the two (USB 2.0).</p>			
Procedure:	<ol style="list-style-type: none"> Set the active power package on the SUT to Power Package 1 (Intel® ME on in S0). Set the Intel® AMT WLAN link policy on the SUT to Link Policy 2 (Enabled in S0), if the WLAN network interface is used. Ensure the TCP maximum data retransmission setting defined in the SUT profile is applied to both a) the management console, and b) the SUT via Intel® AMT, if the WLAN network interface is used. <p>If the configuration on the management console is not already aligned to the SUT profile setting, the network stack on the management console need to be reset; leading to potential network connectivity loss for other applications on the system.</p> <p>Before synchronizing the setting on the management console, provide a warning to the test operator, with the option to proceed or cancel, indicating the TCP maximum data retransmission network setting is about to be changed and that it may be necessary to re-establish network connectivity for any other applications running on the management console. If the test operator chooses to cancel, the test step is marked as failed.</p> <ol style="list-style-type: none"> Ensure the Intel® AMT redirection ports are enabled on the SUT. Cancel any existing Intel® AMT user consent session which may be active on the SUT. Ensure the Intel® AMT user consent opt-in setting is disabled on the SUT. Set the KVM password to 'Admin!98' on the SUT via Intel® AMT. Ensure that the VNC port 5900 is enabled on the SUT via Intel® AMT. 			
Procedure: (continued)	<p>The steps within this block is executed as if they are part of an independent sub-test. If a failure occurs at any point during the flow below, the remainder of the steps related to the sub-test, may be skipped.</p> <ol style="list-style-type: none"> Inform the test operator that the VNC Viewer soon open. Open a KVM Redirection session with the SUT via Intel® AMT using the VNC Viewer on the management console. Request the test operator to: <ol style="list-style-type: none"> Confirm that the redirected screen from the SUT appears in the VNC Viewer. Confirm that the keyboard and mouse can control the Host OS via the management console via the VNC Viewer. Confirm that the USB keyboard and mouse on the SUT are both working. Confirm a USB Storage device (USB Key) can be connected to each USB port on the SUT and can be accessed via the Host OS thereon. 			
Procedure: (continued)	<ol style="list-style-type: none"> Close any open KVM Redirection session with the SUT via Intel® AMT. Close any VNC Viewer window which may still be open. Request the test operator to re-run the test, as needed, for each available USB version supported by the SUT. 			
Pass Criteria:	This test passes if all USB ports are working correctly during the KVM Redirection session for all supported USB versions on the SUT.			
References:	For details on KVM Redirection and USB device support, refer the <i>Intel® ME BIOS Specification</i> .			



11.8.16 KVM Redirection with Remote Screen Blank (RSB) Support

ID:	AMT_054			
Title:	Keyboard, Video, and Mouse (KVM) Redirection with Remote Screen Blank (RSB) Support			
Requirement:	Mandatory - exempt for systems which do not support KVM with internal graphics			
System:	Form Factor <input checked="" type="checkbox"/> Desktop <input checked="" type="checkbox"/> Workstation <input checked="" type="checkbox"/> Mobile	System Power Model <input checked="" type="checkbox"/> Standard <input checked="" type="checkbox"/> Modern Standby or InstantGo*	Intel® AMT Network Interface <input type="checkbox"/> LAN <input checked="" type="checkbox"/> Either Used <input type="checkbox"/> WLAN <input type="checkbox"/> Not Used	LAN Type <input checked="" type="checkbox"/> Integrated LAN <input type="checkbox"/> Discrete LAN <input type="checkbox"/> TBT Dock LAN
Method:	Automated by Intel® PETS with test operator interaction			
Description:	Remote screen blank is targeted at public unattended systems that require the capability to blank the screen display while IT personnel manages the system.			
Objective:	Verify that remote screen blank works properly.			
Setup:	<p>The initial state of the SUT should be S0/MeOn with Host OS running. Intel® AMT should be provisioned via manual mode. Before running this test, ensure that KVM Redirection is enabled in the Intel® MEBX. If the SUT supports switchable graphics, graphics configuration should be set to integrated graphics. Ensure that remote screen blanking ('Firmware KVM Screen Blanking') is enabled in the firmware image on the SUT and that the display is connected to an Intel® Graphics port.</p>			
Procedure:	<ol style="list-style-type: none"> 1. Set the active power package on the SUT to Power Package 2 (Intel® ME on in S0, wake in Sx/AC). 2. Set the Intel® AMT WLAN link policy on the SUT to Link Policy 3 (Enabled in S0, Sx/AC), if the WLAN network interface is used. 3. Ensure the TCP maximum data retransmission setting defined in the SUT profile is applied to both a) the management console, and b) the SUT via Intel® AMT, if the WLAN network interface is used. <p>If the configuration on the management console is not already aligned to the SUT profile setting, the network stack on the management console need to be reset; leading to potential network connectivity loss for other applications on the system.</p> <p>Before synchronizing the setting on the management console, provide a warning to the test operator, with the option to proceed or cancel, indicating the TCP maximum data retransmission network setting is about to be changed and that it may be necessary to re-establish network connectivity for any other applications running on the management console. If the test operator chooses to cancel, the test step is marked as failed.</p> <ol style="list-style-type: none"> 4. Ensure the Intel® AMT redirection ports are enabled on the SUT. 5. Cancel any existing Intel® AMT user consent session which may be active on the SUT. 6. Ensure the Intel® AMT user consent opt-in setting is disabled on the SUT. 7. Set the KVM password to 'Admin!98' on the SUT via Intel® AMT. 8. Ensure that the VNC port 5900 is enabled on the SUT via Intel® AMT. 			



ID:	AMT_054
Procedure: (continued)	<p>9. Terminate any active remote screen blanking session on the SUT via Intel® AMT. The remaining steps within this block is executed as if they are part of an independent sub-test. If a failure occurs at any point during the flow below, the remainder of the steps related to the sub-test, may be skipped.</p> <p>10. Inform the test operator that the VNC Viewer soon open.</p> <p>11. Open a KVM Redirection session with the SUT via Intel® AMT using the VNC Viewer on the management console.</p> <p>12. Request the test operator to:</p> <ol style="list-style-type: none"> Confirm that the redirected screen from the SUT appears in the VNC Viewer. Confirm that the keyboard and mouse can control the Host OS via the management console via the VNC Viewer. <p>13. Inform the test operator that remote screen blanking is activated, whereby the screen on the SUT should become blank.</p> <p>14. Activate a remote screen blanking session on the SUT via Intel® AMT.</p> <p>15. Request the test operator to:</p> <ol style="list-style-type: none"> Confirm that the display of the SUT is blank. Confirm that the redirected screen from the SUT appears in the VNC Viewer. Confirm that the keyboard and mouse can control the Host OS via the management console via the VNC Viewer. <p>16. Perform a graceful Restart via the Host OS.</p> <p>17. Wait until system reboots back to the Host OS.</p> <p>18. Request the test operator to:</p> <ol style="list-style-type: none"> Confirm that the display of the SUT remains blank. Confirm that the redirected screen from the SUT remains in the VNC Viewer. Confirm that the keyboard and mouse can continue to control the Host OS via the management console via the VNC Viewer. <p>19. Inform the test operator that remote screen blanking is terminated, whereby the screen on the SUT should become restored.</p> <p>20. Terminate the remote screen blanking session on the SUT via Intel® AMT.</p> <p>21. Request the test operator to:</p> <ol style="list-style-type: none"> Confirm that the display of the SUT is restored. Confirm that the redirected screen from the SUT appears in the VNC Viewer. Confirm that the keyboard and mouse can control the Host OS via the management console via the VNC Viewer.
Procedure: (continued)	<p>22. Terminate any active remote screen blanking session on the SUT via Intel® AMT.</p> <p>23. Close any open KVM Redirection session with the SUT via Intel® AMT.</p> <p>24. Close any VNC Viewer window which may still be open.</p>
Pass Criteria:	The test passes if the KVM Redirection session stays available during all test stages, while display blanks and turns back on according to the remote screen blank state.
References:	For details on KVM Redirection, refer the <i>Intel® ME BIOS Specification</i> . For details on Firmware KVM Screen Blanking configuration, refer the <i>Intel® ME Firmware Bring Up Guide</i> .

11.8.17 KVM Redirection with S0 Low Power Idle and Intel® ME Power Gating

ID:	AMT_055			
Title:	Keyboard, Video, and Mouse (KVM) Redirection with S0 Low Power Idle state, as with Modern Standby or Microsoft® Windows® InstantGo® mode, and Intel® ME Power Gating			
Requirement:	Mandatory - exempt for systems which do not support KVM with internal graphics			
System:	Form Factor	System Power Model	Intel® AMT Network Interface	LAN Type
	<input checked="" type="checkbox"/> Desktop <input type="checkbox"/> Workstation <input checked="" type="checkbox"/> Mobile	<input type="checkbox"/> Standard <input checked="" type="checkbox"/> Modern Standby or InstantGo®	<input type="checkbox"/> LAN <input type="checkbox"/> Either Used <input checked="" type="checkbox"/> WLAN <input type="checkbox"/> Not Used	<input type="checkbox"/> Integrated LAN <input type="checkbox"/> Discrete LAN <input type="checkbox"/> TBT Dock LAN
Method:	Automated by Intel® PETS with test operator interaction			
Description:	An Intel® AMT compliant system implements KVM redirection support when the system is in S0 Low Power Idle state and move to S0 state.			
Objective:	This test check that the SUT moves from S0 Low Power Idle state to S0 when KVM has been initiated.			



ID:	AMT_055
Setup:	The initial state of the SUT should be S0/MeOn with Host OS running. Intel® AMT should be provisioned via manual mode. Before running this test, ensure that KVM is enabled in the Intel® MEBX. If the SUT supports switchable graphics, graphics configuration should be set to integrated graphics. The SUT must be configured to work in Modern Standby or Microsoft Windows* InstantGo* mode.
Procedure:	<ol style="list-style-type: none">1. Set the active power package on the SUT to Power Package 1 (Intel® ME on in S0).2. Set the Intel® AMT WLAN link policy on the SUT to Link Policy 2 (Enabled in S0).3. Ensure the TCP maximum data retransmission setting defined in the SUT profile is applied to both a) the management console, and b) the SUT via Intel® AMT. If the configuration on the management console is not already aligned to the SUT profile setting, the network stack on the management console need to be reset; leading to potential network connectivity loss for other applications on the system. Before synchronizing the setting on the management console, provide a warning to the test operator, with the option to proceed or cancel, indicating the TCP maximum data retransmission network setting is about to be changed and that it may be necessary to re-establish network connectivity for any other applications running on the management console. If the test operator chooses to cancel, the test step is marked as failed.4. Ensure the Intel® AMT redirection ports are enabled on the SUT.5. Cancel any existing Intel® AMT user consent session which may be active on the SUT.6. Ensure the Intel® AMT user consent opt-in setting is disabled on the SUT.7. If the SUT supports LAN connectivity, request the test operator to disconnect the LAN cable. The Intel® ME cannot move to a power gated state while the LAN is physically connected.8. Set the KVM password to 'Admin!98' on the SUT via Intel® AMT.9. Ensure that the VNC port 5900 is enabled on the SUT via Intel® AMT.
Procedure: (continued) SOLP→S0 Flow	<p>The steps within this block is executed as if they are part of an independent sub-test. If a failure occurs at any point during the flow below, the remainder of the steps related to the sub-test, may be skipped.</p> <ol style="list-style-type: none">10. Keep the host in S0 by performing host-only activity; allowing the Intel® ME to idle (approximately 2 to 3 seconds) and subsequently enter a power gated state.11. Verify that the SUT is in S0/MeOn (CM0-PG).12. Inform the test operator that after SUT enters S0 Low Power Idle state, the VNC Viewer window opens. When the VNC Viewer window opens, request the test operator to try using the keyboard and mouse to Activate and control the Host OS on the SUT.13. Request the test operator to manually place the SUT into S0 Low Power Idle state.14. Verify that the SUT has moved into S0 Low Power Idle state.15. Open a KVM Redirection session with the SUT via Intel® AMT using the VNC Viewer on the management console.16. Request the test operator to:<ol style="list-style-type: none">a. Confirm that the redirected screen from the SUT appears in the VNC Viewer.b. Confirm that the keyboard and mouse can control the Host OS via the management console via the VNC Viewer.
Procedure: (continued)	<ol style="list-style-type: none">17. Close any open KVM Redirection session with the SUT via Intel® AMT.18. Close any VNC Viewer window which may still be open.19. If the SUT supports LAN connectivity, request the test operator to reconnect the LAN cable, and then verify that Intel® AMT is available via LAN by requesting its version.
Pass Criteria:	The test passes if the Intel® ME enters power gated state and afterward the KVM Redirection session can be viewed via VNC Viewer on the management console. Keyboard/mouse functionality is redirected to the Host OS on the SUT during the KVM Redirection session.
References:	For details on KVM Redirection, refer the <i>Intel® ME BIOS Specification</i> .

11.8.18 KVM Redirection over Intel® AMT WLAN Network Interface for Systems Supporting Wake On Wireless LAN

ID:	AMT_056			
Title:	Keyboard, Video, and Mouse (KVM) Redirection over Intel® AMT WLAN Network Interface for Systems supporting Wake on Wireless LAN			
Requirement:	Mandatory - exempt for systems which do not support KVM with internal graphics and Wake on Wireless LAN			
System:	Form Factor		System Power Model	Intel® AMT Network Interface
	<input checked="" type="checkbox"/> Desktop <input checked="" type="checkbox"/> Mobile	<input checked="" type="checkbox"/> Workstation	<input checked="" type="checkbox"/> Standard <input type="checkbox"/> Modern Standby or InstantGo*	<input type="checkbox"/> LAN <input checked="" type="checkbox"/> WLAN
				<input type="checkbox"/> Either Used <input type="checkbox"/> Not Used
				<input type="checkbox"/> Integrated LAN <input type="checkbox"/> Discrete LAN <input type="checkbox"/> TBT Dock LAN



ID:	AMT_056
Method:	Automated by Intel® PETS with test operator interaction
Description:	An Intel® AMT compliant system implements KVM redirection support when the system is in S3 state and moves to S0 state.
Objective:	This test check that when the SUT moves from S3 to S0 when KVM has been initiated, the BIOS would not halt and wait for the user to give consent for the KVM Redirection session, and the user consent opt-in option should not be displayed on the platform under test. The SUT's screen is visible in the Virtual Network Computing (VNC) Viewer on the management console.
Setup:	<p>The initial state of the SUT should be S0/MeOn with Host OS running. Intel® AMT should be provisioned via manual mode. Before running this test, ensure that KVM is enabled in the Intel® MEBX. If the SUT supports switchable graphics, graphics configuration should be set to integrated graphics.</p> <p>NOTE: In order to fully implement Wake on Wireless LAN (WoWLAN) in Sx states, the host BIOS must set HOST_WLAN_PP_EN. For more further details, refer the PCH <i>External Design Specification (EDS)</i> and the PCH <i>Platform Design Guide (PDG)</i>. Failure to properly set the HOST_WLAN_PP_EN bit may result in failures for this test.</p>
Procedure:	<ol style="list-style-type: none"> Set the active power package on the SUT to Power Package 2 (Intel® ME on in S0, wake in Sx/AC). Set the Intel® AMT WLAN link policy on the SUT to Link Policy 3 (Enabled in S0, Sx/AC). Ensure the Host OS Wake on Wireless LAN is enabled. Verify that Intel® AMT is available via WLAN by requesting its version. Ensure the TCP maximum data retransmission setting defined in the SUT profile is applied to both a) the management console, and b) the SUT via Intel® AMT. If the configuration on the management console is not already aligned to the SUT profile setting, the network stack on the management console need to be reset; leading to potential network connectivity loss for other applications on the system. Before synchronizing the setting on the management console, provide a warning to the test operator, with the option to proceed or cancel, indicating the TCP maximum data retransmission network setting is about to be changed and that it may be necessary to re-establish network connectivity for any other applications running on the management console. If the test operator chooses to cancel, the test step is marked as failed. Ensure the Intel® AMT redirection ports are enabled on the SUT. Cancel any existing Intel® AMT user consent session which may be active on the SUT. Ensure the Intel® AMT user consent opt-in setting is disabled on the SUT. Set the KVM password to 'Admin!98' on the SUT via Intel® AMT. Ensure that the VNC port 5900 is enabled on the SUT via Intel® AMT.
Procedure: (continued) S3→S0 Flow	<p>The steps within this block is executed as if they are part of an independent sub-test. If a failure occurs at any point during the flow below, the remainder of the steps related to the sub-test, may be skipped.</p> <ol style="list-style-type: none"> Inform the test operator that the SUT soon be sent into suspend state and the VNC Viewer window opens. When the VNC Viewer window opens and the SUT starts to boot, request the test operator to try using the keyboard and mouse to control the Host OS. Suspend to S3/MeOn the SUT via the Host OS and then wait 10 seconds. Open a KVM Redirection session with the SUT via Intel® AMT using the VNC Viewer on the management console. Wait for the SUT to return to S0/MeOn with the Host OS running. Request the test operator to: <ol style="list-style-type: none"> Press the ESC key or move the mouse in the VNC Viewer (necessary to activate the SUT screen on some systems). Confirm that the redirected screen from the SUT appears in the VNC Viewer. Confirm that the keyboard and mouse can control the Host OS via the management console via the VNC Viewer.
Procedure: (continued)	<ol style="list-style-type: none"> Close any open KVM Redirection session with the SUT via Intel® AMT. Close any VNC Viewer window which may still be open.
Pass Criteria:	The test passes if the attempted KVM Redirection session is viewed via VNC Viewer on the management console, and keyboard/mouse functionality is redirected to the Host OS on the SUT.
References:	For details on KVM Redirection, refer the <i>Intel® ME BIOS Specification</i> as well as the <i>Intel® AMT and Wake On Wireless LAN Coexistence</i> feature overview.

11.8.19 KVM Redirection on Headless Configurations

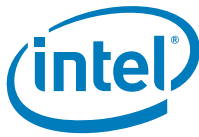
ID:	AMT_059
Title:	Keyboard, Video, and Mouse (KVM) Redirection on Headless Configurations



ID:	AMT_059																												
Requirement:	Mandatory - exempt for systems which do not support KVM with internal graphics and not supporting headless configurations (Refer below)																												
System:	<table><tr><th colspan="2">Form Factor</th><th>System Power Model</th><th colspan="2">Intel® AMT Network Interface</th><th>LAN Type</th></tr><tr><td><input checked="" type="checkbox"/> Desktop</td><td><input checked="" type="checkbox"/> Workstation</td><td><input checked="" type="checkbox"/> Standard</td><td><input type="checkbox"/> LAN</td><td><input checked="" type="checkbox"/> Either Used</td><td><input checked="" type="checkbox"/> Integrated LAN</td></tr><tr><td><input checked="" type="checkbox"/> Mobile</td><td></td><td><input checked="" type="checkbox"/> Modern Standby or InstantGo*</td><td><input type="checkbox"/> WLAN</td><td><input type="checkbox"/> Not Used</td><td><input type="checkbox"/> Discrete LAN</td></tr><tr><td></td><td></td><td></td><td></td><td></td><td><input type="checkbox"/> TBT Dock LAN</td></tr></table>	Form Factor		System Power Model	Intel® AMT Network Interface		LAN Type	<input checked="" type="checkbox"/> Desktop	<input checked="" type="checkbox"/> Workstation	<input checked="" type="checkbox"/> Standard	<input type="checkbox"/> LAN	<input checked="" type="checkbox"/> Either Used	<input checked="" type="checkbox"/> Integrated LAN	<input checked="" type="checkbox"/> Mobile		<input checked="" type="checkbox"/> Modern Standby or InstantGo*	<input type="checkbox"/> WLAN	<input type="checkbox"/> Not Used	<input type="checkbox"/> Discrete LAN						<input type="checkbox"/> TBT Dock LAN				
Form Factor		System Power Model	Intel® AMT Network Interface		LAN Type																								
<input checked="" type="checkbox"/> Desktop	<input checked="" type="checkbox"/> Workstation	<input checked="" type="checkbox"/> Standard	<input type="checkbox"/> LAN	<input checked="" type="checkbox"/> Either Used	<input checked="" type="checkbox"/> Integrated LAN																								
<input checked="" type="checkbox"/> Mobile		<input checked="" type="checkbox"/> Modern Standby or InstantGo*	<input type="checkbox"/> WLAN	<input type="checkbox"/> Not Used	<input type="checkbox"/> Discrete LAN																								
					<input type="checkbox"/> TBT Dock LAN																								
Method:	Automated by Intel® PETS with test operator interaction																												
Description:	Headless configuration support is targeted at unattended, semi-attended (example: shared by multiple users), or unassigned systems that require KVM support even when the system has no display device connected (either temporarily or permanently).																												
Objective:	Verify that KVM redirection works properly on a system with no physical display attached.																												
Setup:	<p>The initial state of the SUT should be S0/MeOn with Host OS running. Intel® AMT should be provisioned via manual mode. Before running this test, ensure that KVM Redirection is enabled in the Intel® MEBX. If the SUT supports switchable graphics, graphics configuration should be set to integrated graphics.</p> <p>Important: VBIOS (Video BIOS) and Intel® Graphics drivers supporting KVM redirection on headless configurations must also be integrated/installed on the SUT.</p>																												
Procedure:	<ol style="list-style-type: none">Set the active power package on the SUT to Power Package 2 (Intel® ME in S0, wake in Sx/AC).Set the Intel® AMT WLAN link policy on the SUT to Link Policy 3 (Enabled in S0, Sx/AC), if the WLAN network interface is used.Ensure the Host OS Wake on Wireless LAN is disabled.Ensure the TCP maximum data retransmission setting defined in the SUT profile is applied to both a) the management console, and b) the SUT via Intel® AMT, if the WLAN network interface is used. <p>If the configuration on the management console is not already aligned to the SUT profile setting, the network stack on the management console need to be reset; leading to potential network connectivity loss for other applications on the system.</p> <p>Before synchronizing the setting on the management console, provide a warning to the test operator, with the option to proceed or cancel, indicating the TCP maximum data retransmission network setting is about to be changed and that it may be necessary to re-establish network connectivity for any other applications running on the management console. If the test operator chooses to cancel, the test step is marked as failed.</p> <ol style="list-style-type: none">Ensure the Intel® AMT redirection ports are enabled on the SUT.Cancel any existing Intel® AMT user consent session which may be active on the SUT.Ensure the Intel® AMT user consent opt-in setting is disabled on the SUT.Set the KVM password to 'Admin!98' on the SUT via Intel® AMT.Ensure that the VNC port 5900 is enabled on the SUT via Intel® AMT.																												
Procedure: (continued) S5→S0 Flow	<ol style="list-style-type: none">Request the test operator to disconnect all display devices from the SUT. <p>The remaining steps within this block is executed as if they are part of an independent sub-test. If a failure occurs at any point during the flow below, the remainder of the steps related to the sub-test, may be skipped.</p> <ol style="list-style-type: none">Inform the test operator that the SUT soon be powered down and the VNC Viewer window opens. When the VNC Viewer window opens and the SUT starts to boot, request the test operator to:<ol style="list-style-type: none">Verify that the Ctrl+P (or equivalent keystroke) Intel® MEBX prompt does not appear on the SUT screen during boot.Verify that the BIOS boot screen (if any) is also visible via the VNC viewer.Try using the keyboard and mouse to control the Host OS.Gracefully shutdown to S5/MeOn the SUT via the Host OS and then wait 10 seconds.Verify that Intel® AMT is available via WLAN by requesting its version, if the WLAN network interface is used.Open a KVM Redirection session with the SUT via Intel® AMT using the VNC Viewer on the management console.Perform a Remote Power-Up of the SUT via Intel® AMT.Request the test operator to:<ol style="list-style-type: none">Confirm that the redirected screen from the SUT appears in the VNC Viewer.Confirm that the keyboard and mouse can control the Host OS via the management console via the VNC Viewer.																												



ID:	AMT_059
<p>Procedure: (continued) S4→S0 Flow</p>	<p>17. Close any open KVM Redirection session with the SUT via Intel® AMT.</p> <p>18. Close any VNC Viewer window which may still be open.</p> <p>19. Attempt to bring the SUT to a base state via the following:</p> <ol style="list-style-type: none"> Verify that the SUT is in S0/MeOn (CM0,CM0-PG). Verify that the Host OS on the SUT is available. Verify that Intel® AMT on the SUT responds to version queries via the WLAN network interface, if the WLAN network interface is used. <p>If any of base state verification steps above fail, perform the following as an attempt to recover the SUT before attempting the base state verification steps above one last time.</p> <ol style="list-style-type: none"> Bring the system to G3 and wait 10 seconds. Set system power configuration to AC/DC and wait another 10 seconds. Briefly press the Power Button on the SUT. <p>The remaining steps within this block is executed as if they are part of an independent sub-test. If a failure occurs at any point during the flow below, the remainder of the steps related to the sub-test, may be skipped.</p> <p>20. Inform the test operator that the SUT soon be sent into hibernation state and the VNC Viewer window opens. When the VNC Viewer window opens and the SUT starts to boot, request the test operator to:</p> <ol style="list-style-type: none"> Verify that the Ctrl+P (or equivalent keystroke) Intel® MEBX prompt does not appear on the SUT screen during resume from hibernation. Verify that the BIOS boot screen (if any) is also visible via the VNC viewer. Try using the keyboard and mouse to control the Host OS. <p>21. Hibernate to S4/MeOn the SUT via the Host OS and then wait 10 seconds.</p> <p>22. Verify that Intel® AMT is available via WLAN by requesting its version, if the WLAN network interface is used.</p> <p>23. Open a KVM Redirection session with the SUT via Intel® AMT using the VNC Viewer on the management console.</p> <p>24. Perform a Remote Power-Up of the SUT via Intel® AMT.</p> <p>25. Request the test operator to:</p> <ol style="list-style-type: none"> Confirm that the redirected screen from the SUT appears in the VNC Viewer. Confirm that the keyboard and mouse can control the Host OS via the management console via the VNC Viewer.
<p>Procedure: (continued) S3→S0 Flow</p>	<p>26. Close any open KVM Redirection session with the SUT via Intel® AMT.</p> <p>27. Close any VNC Viewer window which may still be open.</p> <p>28. Attempt to bring the SUT to a base state via the following:</p> <ol style="list-style-type: none"> Verify that the SUT is in S0/MeOn (CM0,CM0-PG). Verify that the Host OS on the SUT is available. Verify that Intel® AMT on the SUT responds to version queries via the WLAN network interface, if the WLAN network interface is used. <p>If any of base state verification steps above fail, perform the following as an attempt to recover the SUT before attempting the base state verification steps above one last time.</p> <ol style="list-style-type: none"> Bring the system to G3 and wait 10 seconds. Set system power configuration to AC/DC and wait another 10 seconds. Briefly press the Power Button on the SUT. <p>The remaining steps within this block is executed as if they are part of an independent sub-test. If a failure occurs at any point during the flow below, the remainder of the steps related to the sub-test, may be skipped.</p> <p>NOTE: In the case the SUT is operating in Modern Standby or Microsoft Windows* InstantGo* mode, the test automatically end here, and the results thus far reported to the test operator as the final test results. For desktop systems with Intel® RMT support, ensure that Intel® RMT is disabled before running S3 test flows.</p> <p>29. Inform the test operator that the SUT soon be sent into suspend state and the VNC Viewer window opens. When the VNC Viewer window opens and the SUT starts to boot, request the test operator to try using the keyboard and mouse to control the Host OS.</p> <p>30. Record the Host OS last boot time on the SUT (to verify successful suspend/resume).</p> <p>31. Suspend to S3/MeOn the SUT via the Host OS and then wait 10 seconds.</p> <p>32. Verify that Intel® AMT is available via WLAN by requesting its version, if the WLAN network interface is used.</p> <p>33. Open a KVM Redirection session with the SUT via Intel® AMT using the VNC Viewer on the management console.</p> <p>34. Perform a Remote Power-Up of the SUT via Intel® AMT.</p> <p>35. Wait until system resumes back to the Host OS.</p> <p>36. Verify the Host OS last boot time on the SUT does match the boot time recorded before the suspend.</p> <p>37. Request the test operator to:</p> <ol style="list-style-type: none"> Confirm that the redirected screen from the SUT appears in the VNC Viewer. Confirm that the keyboard and mouse can control the Host OS via the management console via the VNC Viewer.



ID:	AMT_059
Procedure: (continued)	38. Close any open KVM Redirection session with the SUT via Intel® AMT. 39. Close any VNC Viewer window which may still be open. 40. Request the test operator to re-connect any display devices to the SUT which had been disconnected earlier in the test.
Pass Criteria:	The test passes if all attempted KVM Redirection sessions are viewed via VNC Viewer on the management console, and keyboard/mouse functionality is redirected to the Host OS on the SUT. During system boot or resume, the Intel® MEBX hot-key (Ctrl+P or other keystroke) prompt is not displayed on the SUT.
References:	For details on KVM Redirection, refer the <i>Intel® ME BIOS Specification</i> . For details on Firmware KVM Screen Blanking configuration, refer the <i>Intel® ME Firmware Bring Up Guide</i> .

11.9 Remote Access (Fast Call for Help)

The section serves as a checklist for the environment setup and covers integration testing of the Remote Access (Fast Call for Help) feature in Intel® AMT.

11.9.1 Test Environment

The System Under Test (SUT) is to be configured with Intel® AMT set in manual provisioning mode with a DHCP assigned address configured. Static IP address configurations are not supported by the Environment Detection feature used in this section. The management console may be a laptop or a desktop with a version of Microsoft Windows* supported by Intel® PETS, and the SUT should have a version of Microsoft Windows* supported by Intel® PETS as well. The test network is comprised of a hub/switch and network cables.

Tools for testing:

- Intel® PETS: The latest version of the tool from the Intel® CSME Compliancy and Debug kit release. Refer the Intel® PETS User Guide for exact instructions on how to load and setup the Intel® PETS software.
- Intel® Automated Power Switch (Intel® APS): The SUT should be connected to an Intel® APS 3 unit. In case an Intel® APS 3 is not available, select the Manual configuration in the Intel® PETS SUT profile configuration menu.
- Intel® PETS Local Agent: The local agent must be installed on the SUT.

Where applicable, the wireless LAN interface on Intel® AMT must be on a different network/subnet than the wired LAN interface. For details on how to enter the network interface details into Intel® PETS, consult the Intel® PETS User Guide.

If the firmware image or the SUT configuration does not support some features, Intel® PETS show those features as failing when tested. Intel® PETS cannot determine in all cases which features have been deactivated and should thus be skipped during testing.

11.9.2 Fast Call for Help During System Boot

ID:	AMT_060				
Title:	Fast Call for Help During System Boot				
Requirement:	Mandatory - exempt for systems which do not support Fast Call for Help				
System:	Form Factor		System Power Model	Intel® AMT Network Interface	LAN Type
	<input checked="" type="checkbox"/> Desktop <input checked="" type="checkbox"/> Mobile	<input checked="" type="checkbox"/> Workstation	<input checked="" type="checkbox"/> Standard <input checked="" type="checkbox"/> Modern Standby or InstantGo*	<input type="checkbox"/> LAN <input type="checkbox"/> WLAN <input checked="" type="checkbox"/> Either Used <input type="checkbox"/> Not Used	<input checked="" type="checkbox"/> Integrated LAN <input type="checkbox"/> Discrete LAN <input type="checkbox"/> TBT Dock LAN



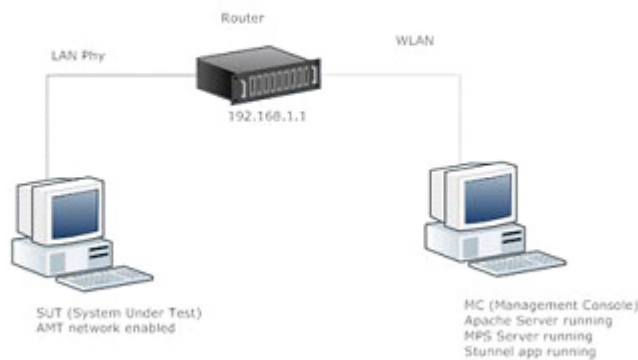
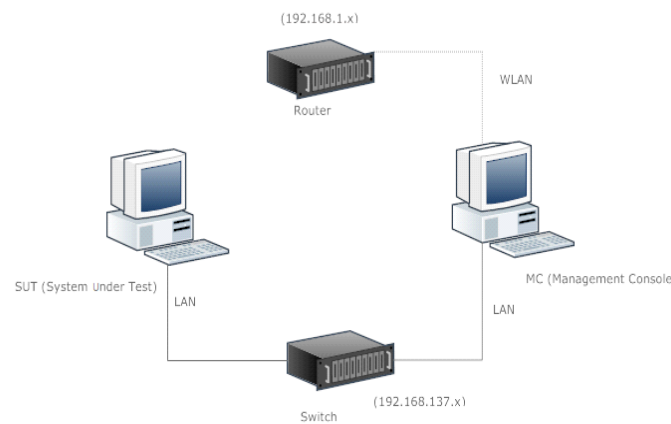
ID:	AMT_060
Method:	Automated by Intel® PETS with test operator interaction
Description:	<p>Fast Call for Help can be established by user from BIOS healing option, from Intel® MEBX or from Hardware button. Pending OEM implementation of Fast Call for Help feature, this test verify that Fast Call for Help can be initiated by means of the interface implemented by the OEM.</p> <p>This is NOT an end to end test of Fast Call for Help feature. This test check only that the session request is initiated from BIOS. In order to perform full end to end test, use ISV tools.</p>
Objective:	<p>This test verify that BIOS is sending the request for Fast Call for Help session initiation once the session is initiated from BIOS/Intel® MEBX or Hardware button.</p> <p>NOTE: Fast Call for Help connection is not supposed to succeed in this test. The test only verifies that the system is trying to initiate the connection.</p>
Setup:	The initial state of the SUT should be S0/MeOn with Host OS running. Intel® AMT should be provisioned via manual mode.
Procedure:	<ol style="list-style-type: none"> 1. Remove all Remote Access Policies on the SUT via Intel® AMT. 2. Verify that the SUT is configured to use DHCP address configuration via Intel® AMT. 3. Create a fictitious Management Presence Server (MPS) for the SUT via Intel® AMT, if not already registered. 4. Create a user initiated trigger Remote Access Policy with a Tunnel Lifetime of 120 seconds associated to the fictitious MPS in the SUT via Intel® AMT. 5. Set the BIOS as an acceptable interface from which to initiate a Remote Access connection on the SUT via Intel® AMT, if not already configured. 6. Set the Environment Detection mechanism on the SUT via Intel® AMT to look for a fictitious network. This forces the SUT to immediately recognize the test network as being outside of the Enterprise. 7. Inform the test operator that a system boot is performed. Request the test operator to press Ctrl+Alt+F1 to initiate the <i>Fast Call for Help</i> process and to view the <i>Fast Call for Help</i> screens display the following. Note, system implementations may use a different keyboard sequence to initiate the <i>Fast Call for Help</i> process.
Procedure: (continued)	<ol style="list-style-type: none"> 8. Gracefully restart the SUT via the Host OS. <p>The next screen may be displayed (on some implementations it may not be visible): <i>Intel(r) Remote Assistance mechanism is trying to get a network connection. This may take a couple of minutes... Press <ESC> to abort...</i></p> <p>The next screen should display the Remote Access connection attempt: <i>Connecting to <fictional server name>... Press <ESC> to abort</i></p> <p>NOTE: It is expected that the connection attempt fails.</p> <ol style="list-style-type: none"> 9. Request the test operator to confirm that the SUT attempted to connect to the fictional MPS server, but did not succeed. 10. Clear the Environment Detection mechanism in the SUT via Intel® AMT, to clean up. 11. Remove all Remote Access Policies on the SUT via Intel® AMT, to clean up.
Pass Criteria:	The test passes if the Fast Call For Help connection attempt screen is displayed. This means that the connection was initiated but no MPS server was found (as expected).
References:	For details on Remote Access operations, refer the <i>Intel® ME BIOS Specification</i> .

11.9.3 Fast Call for Help During System Boot (End-to-End)

ID:	AMT_061				
Title:	Fast Call for Help During System Boot (End-to-End)				
Requirement:	Optional				
System:	Form Factor		System Power Model	Intel® AMT Network Interface	LAN Type
	<input checked="" type="checkbox"/> Desktop <input checked="" type="checkbox"/> Mobile	<input checked="" type="checkbox"/> Workstation	<input checked="" type="checkbox"/> Standard <input checked="" type="checkbox"/> Modern Standby or InstantGo*	<input checked="" type="checkbox"/> LAN <input type="checkbox"/> WLAN <input type="checkbox"/> Either Used <input type="checkbox"/> Not Used	<input checked="" type="checkbox"/> Integrated LAN <input type="checkbox"/> Discrete LAN <input type="checkbox"/> TBT Dock LAN
Method:	Manual				

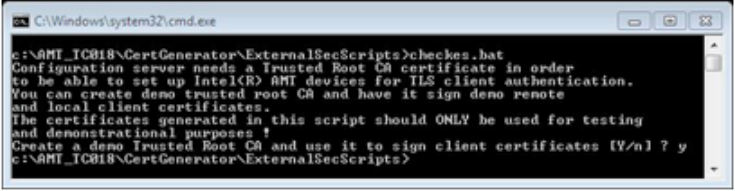


ID:	AMT_061
Description:	Fast Call for Help can be initiated by user from BIOS healing option, from Intel® MEBX or from Hardware button. Pending OEM implementation of Fast Call for Help feature, this test verify that a full Fast Call for Help session can be established by means of the interface implemented by the OEM.
Objective:	This test verify that a Fast Call for Help session can be established between Intel® AMT and MPS. This is not a mandatory test. The mandatory section of Fast Call for Help implementation is tested in AMT_060.
Setup:	Test Environment Device Roles: <ul style="list-style-type: none">• System Under Test (SUT):<ul style="list-style-type: none">a. Initially participates on the Enterprise Network for configuration.b. Later is moved to the Remote Network for CIRA testing.• management console:<ul style="list-style-type: none">a. Exists on the Enterprise Network (by means of a Wi-Fi connection) and configures the SUT.b. Provides DHCP services for the Remote Network through Microsoft Windows* Internet Connection Sharing (by means of a LAN connection).• Wireless AP:<ul style="list-style-type: none">a. Provides DHCP services to the Enterprise Network by means of wireless (to management console) and wired ports (to SUT when connected).• Switch:<ul style="list-style-type: none">a. Exists on the Remote Network and provides a connection point for the SUT.b. Provides continuous electrical signaling to the management console LAN PHY to enable Microsoft Windows* Internet Connection Sharing configuration.
Setup: (continued)	Network Topology: <ul style="list-style-type: none">• Enterprise Network: (Refer diagram #1)<ul style="list-style-type: none">a. Address Range: 192.168.1.x (Class C)b. Domain Name: enterprise-domain.comc. DHCP Server: Wireless AP• Remote Network (Refer diagram #2)<ul style="list-style-type: none">a. Address Range: 192.168.137.x (Class C)b. Domain Name: mshome.net DHCP Server: Microsoft Windows* Internet Connection Sharing on management console PC

ID:	AMT_061
<p>Diagram Number 1—When SUT is in the Same Network as that of the management console</p>  <p>SUT (System Under Test) AMT network enabled</p> <p>MC (Management Console) Apache Server running MPS Server running Stunnel app running</p>	
<p>Diagram Number 2—When SUT Moves out of the Network (Remote Network)</p>  <p>(192.168.1.x) Router</p> <p>WLAN</p> <p>SUT (System Under Test)</p> <p>LAN</p> <p>MC (Management Console)</p> <p>LAN</p> <p>Switch (192.168.137.x)</p>	
Setup: (continued)	<p>System Under Test Pre-requisite The System Under Test must be able to support TLS, although Intel® ME does not need to be configured to use TLS. Without TLS support, the SUT would not be able to communicate back through the stunnel to the MPS. Some boards may require rework to support TLS.</p> <p>Management Console Setup</p> <p>Network Configuration: Connect by means of a Wireless LAN static IP to the Enterprise Network. (for example, 192.168.1.20 for examples in this document.) Connect by means of a Wired LAN to the Remote Network. Note: This step is only needed if there is no other device or system available to provide DHCP services to the Remote Network. Follow the Microsoft Windows* Internet Connection Sharing configuration instructions provided by Microsoft*. The Microsoft Windows* Internet Connection Sharing configuration instructions can be found at the link below: http://windows.microsoft.com/en-US/windows7/Using-ICS-Internet-Connection-Sharing</p>

ID:	AMT_061															
Setup: (continued)	<p>When using Microsoft Windows* Internet Connection sharing, make sure to confirm the following:</p> <ul style="list-style-type: none">In some system configurations, the DHCP services may not be available or are not enabled by default for the wireless adapter. To verify that the DHCP services are available and configured, open the <i>Properties</i> dialog for the wireless adapter, select the <i>Sharing</i> tab and click the <i>Settings</i> button in the <i>Internet Connection Sharing</i> section.<ul style="list-style-type: none">If available, verify that both DHCP (67) and DHCP (68) check boxes in the services list are selected.If the DHCP service ports are not listed, add services for Port 67 and Port 68 manually. When entering the Name or IP address for the service, use the IP address of the MPS server (for example, 192.168.1.20). For the DHCP service on Port 67, enter 67 for the External Port number and Internal Port number of the service. Repeat the same process for the DHCP service on Port 68 using the respective port value of 68 for the external and internal ports as well as the same IP address of the MPS server.The SUT LAN MAC address must be valid. (for example, not 88:88:88:88:87:88).The SUT LAN interface should be operating in DHCP mode to receive an address from the Microsoft Windows* Internet Connection Sharing service on the management console.The management console wireless interface should be shared from the device driver Properties. When this happens, the LAN interface automatically be set to 192.168.137.1 (ICS default value). The SUT's LAN IP address should then be set within the 192.168.137.x subnet range.															
Setup: (continued)	<p>Tools Setup and Configuration: The following table contains the best known configuration of software deployed herein:</p> <table><tr><th>Software</th><th>Version</th><th>Location</th></tr><tr><td>Intel® AMT Software Development Kit</td><td>10 or later</td><td>https://software.intel.com/en-us/articles/download-the-latest-intel-amt-software-development-kit-sdk</td></tr><tr><td>Intel® Setup and Configuration Software (Intel® SCS)</td><td>8.1.4.16 or later</td><td>https://software.intel.com/en-us/articles/download-the-latest-version-of-intel-amt-setup-and-configuration-service-scs</td></tr><tr><td>stunnel</td><td>4.53</td><td>http://stunnel.mirt.net</td></tr><tr><td>Apache (win32-x86-no_ssl)</td><td>2.2.8</td><td>http://archive.apache.org/dist/httpd/binaries/win32</td></tr></table> <p>NOTE: For stunnel software, it may be necessary to locate an archived version available from one of the mirror repositories listed in the site above to find the exact version listed in this configuration. When selecting a package to download, use the Intel-compatible version with an Installer (for example, 'stunnel-4.53-installer.exe').</p>	Software	Version	Location	Intel® AMT Software Development Kit	10 or later	https://software.intel.com/en-us/articles/download-the-latest-intel-amt-software-development-kit-sdk	Intel® Setup and Configuration Software (Intel® SCS)	8.1.4.16 or later	https://software.intel.com/en-us/articles/download-the-latest-version-of-intel-amt-setup-and-configuration-service-scs	stunnel	4.53	http://stunnel.mirt.net	Apache (win32-x86-no_ssl)	2.2.8	http://archive.apache.org/dist/httpd/binaries/win32
Software	Version	Location														
Intel® AMT Software Development Kit	10 or later	https://software.intel.com/en-us/articles/download-the-latest-intel-amt-software-development-kit-sdk														
Intel® Setup and Configuration Software (Intel® SCS)	8.1.4.16 or later	https://software.intel.com/en-us/articles/download-the-latest-version-of-intel-amt-setup-and-configuration-service-scs														
stunnel	4.53	http://stunnel.mirt.net														
Apache (win32-x86-no_ssl)	2.2.8	http://archive.apache.org/dist/httpd/binaries/win32														
Setup: (continued)	<ol style="list-style-type: none">On both the SUT and the management console, set the system clocks in the BIOS to the current time before proceeding. This helps to ensure that there are no stunnel connectivity issues due to expired certificates.On the SUT, copy the contents of the following applications and scripts from the Intel® Setup and Configuration Software (Intel® SCS) archive file to the directory C:\AMT_061\ (create the destination directory if not available.)<ol style="list-style-type: none">The Intel® AMT Configuration Utility application directory found at: IntelSCS\ACU_WizardMove to the management console and copy the contents of the following applications and scripts from the Intel® AMT SDK to the directory C:\AMT_061\ (create the destination directory if not available.)<ol style="list-style-type: none">The MPS sample application directory found at: Windows\Intel_AMT\Bin\MPSThe MPSNotification application found at: Windows\Intel_AMT\Bin\Copy the contents of the following applications and scripts from the Intel® PETS Installation to the directory C:\AMT_061\<ol style="list-style-type: none">The CertGenerator directory found at: <PETS Install Directory>\Plugins\ME\Configuration\bin\CertGeneratorCreate the MPS server and Trusted Root certificates by means of External Security Scripts:<ol style="list-style-type: none">Edit the checks.bat file in the CertGenerator\ExternalSecScripts directory:<ol style="list-style-type: none">Find and replace all three instances of intel.com with enterprise-domain.com.Save the configuration file and close it.Open a DOS shell (Windows+R -> "cmd" <enter>).Change directory to the C:\AMT_061\CertGenerator\ExternalSecScripts directory and run checks.bat.															

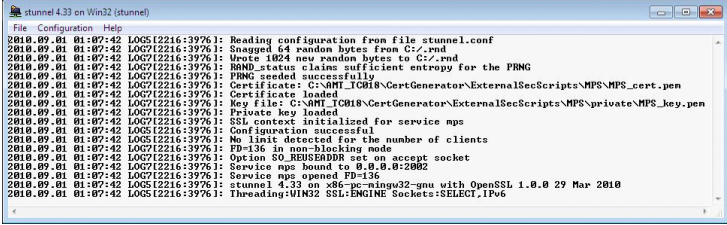
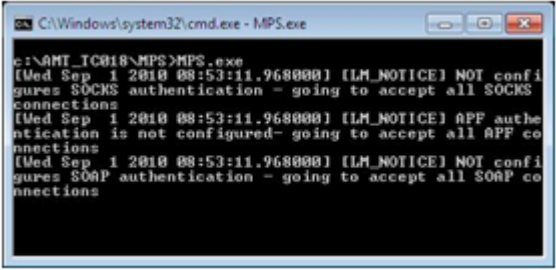


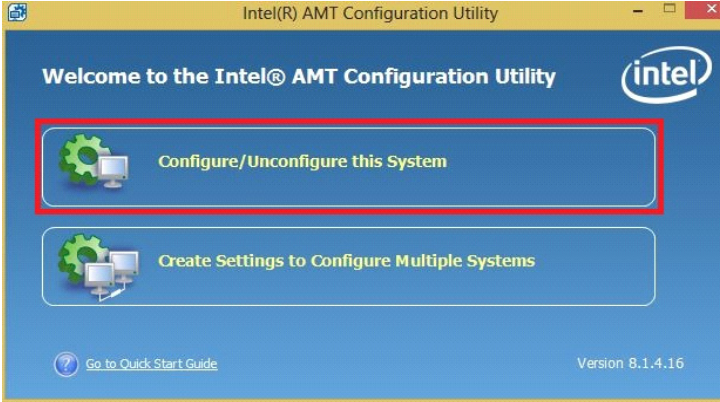
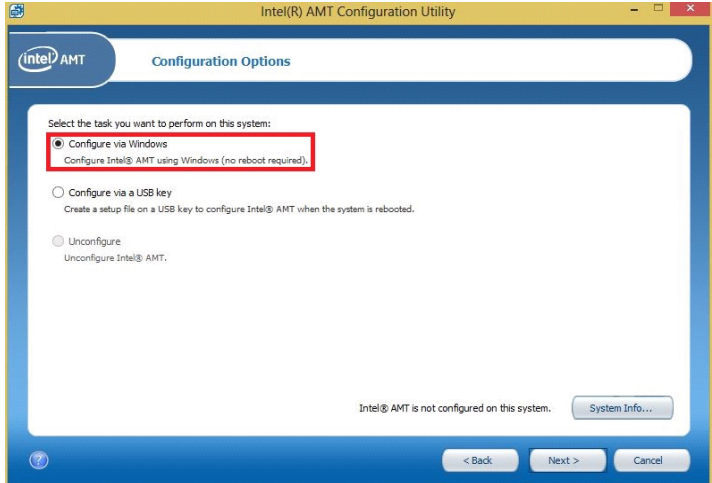
ID:	AMT_061
<p>Setup: (continued)</p>	<p>d. When prompted to create a <i>Demo Trusted Root CA</i> and use it to sign client certificates, enter Y and enter. The scripts create the MPS server and Trusted Root certificates.</p>  <p>e. Exit the DOS shell.</p> <p>6. Install Apache into the C:\AMT_061\ directory:</p> <ol style="list-style-type: none"> During setup, configure the <i>Server Information</i> wizard page as such: <ol style="list-style-type: none"> In the <i>Network Domain</i> field enter enterprise-domain.com. In the <i>Server Name</i> field enter www.enterprise-domain.com. In the <i>Administrator's Email Address</i> field enter admin@enterprise-domain.com. Select the install "<i>only for the Current User, on Port 8080, when started Manually</i>" radio button. Click <i>Next</i> to continue. On the <i>Setup Type</i> wizard page, select the <i>Typical</i> radio button and click <i>Next</i> to continue.
<p>Setup: (continued)</p>	<ol style="list-style-type: none"> On the <i>Destination Folder</i> wizard page, click the <i>Change...</i> button. In the <i>Change Current Destination Folder</i> dialog: <ol style="list-style-type: none"> In the <i>Folder name:</i> field enter C:\AMT_061\apache\. Click <i>OK</i> to close the dialog. Click <i>Next</i> to continue. Click <i>Install</i> to start the installation. Click <i>Finish</i> to finalize the installation and exit the installer. Overwrite the following files in the Apache installation with those from the MPS sample application directory: Source: C:\AMT_061\MPS\Apache Destination: C:\AMT_061\apache\modules File(s): mod_proxy.so, mod_proxy_connect.so Edit the Apache configuration file stored in C:\AMT_061\apache\conf\httpd.conf: <ol style="list-style-type: none"> Uncomment the <i>ServerName</i> directive: ServerName www.enterprise-domain.com:8080 Enable the following modules by un-commenting them: LoadModule proxy_module modules/mod_proxy.so LoadModule proxy_connect module modules/mod_proxy_connect.so LoadModule proxy_http_module modules/mod_proxy_http.so

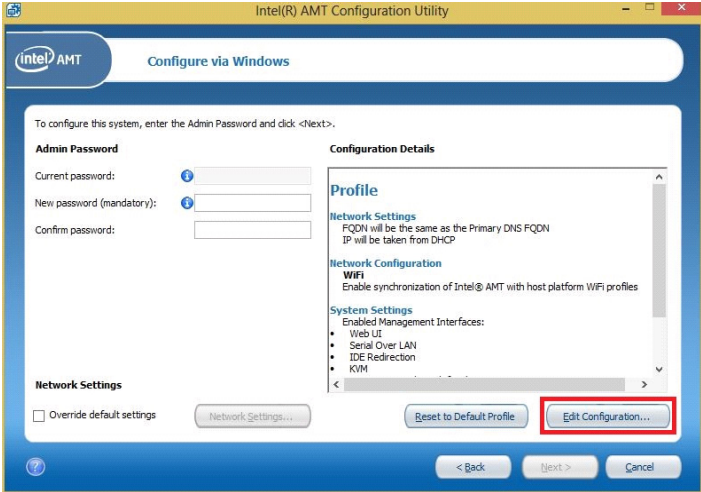
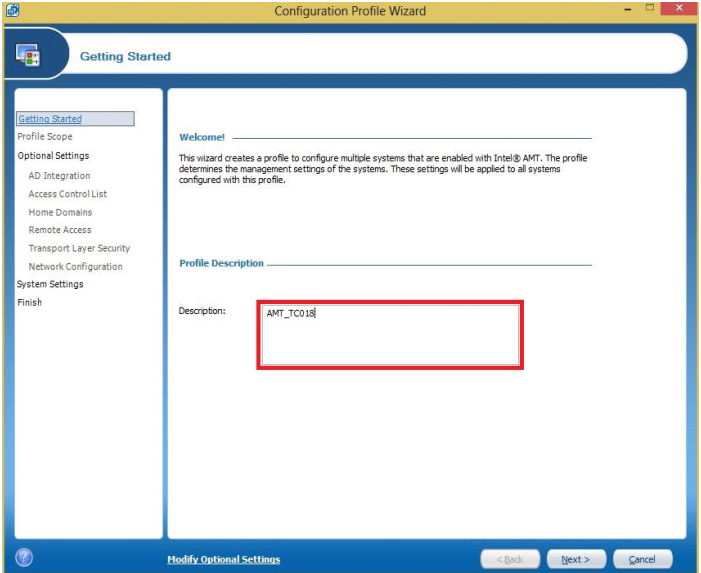


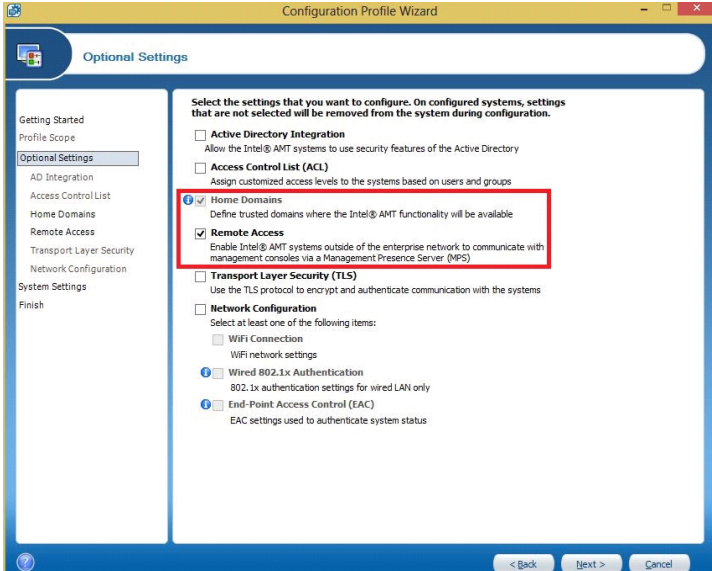
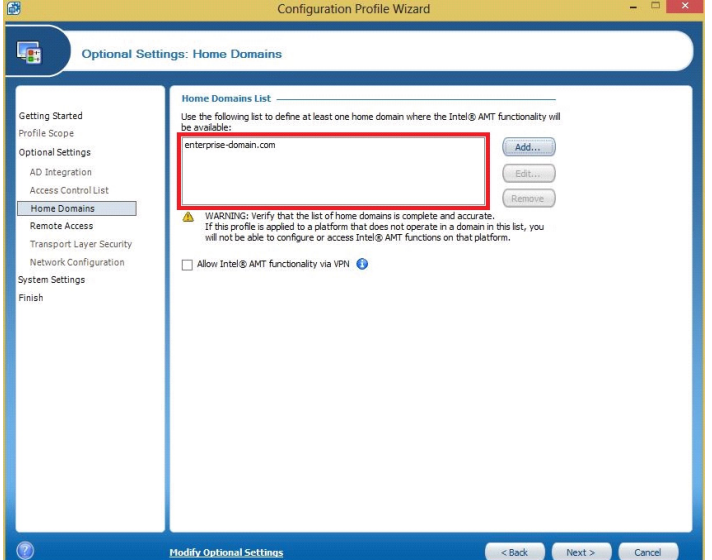
ID:	AMT_061
Setup: (continued)	<ul style="list-style-type: none">iii. Add the following configuration information to the end of the configuration file: AllowCONNECT 433 16992 16993 16994 16995 16996 ProxyRequests On ProxyVia On ProxySocks On ProxySocksIp 192.168.1.20 ProxySocksPort 4322 ProxySocksDnsMode Remote ProxySocksAuth Offiv. Save and close the file. <p>7. Install stunnel and proceed with configuration. During installation, a DOS command window may appear which is trying to create a private key 'stunnel.pem'. If this occurs, simply close the window and allow the installation to finish.</p> <ul style="list-style-type: none">a. Move the stunnel configuration file from C:\Program Files\stunnel\stunnel.conf to the Desktop and open it in an editor:<ul style="list-style-type: none">i. Comment out the three lines for each of pop3s, imaps and smtp protocols.ii. Add the following lines: [mps] accept = 2002 connect = 192.168.1.20:20015iii. Set the cert option to cert = C:\AMT_061\CertGenerator\ExternalSecScripts\MPS\MPS_cert.pemiv. Uncomment the key option and set it to: key = C:\AMT_061\CertGenerator\ExternalSecScripts\MPS\private\MPS_key.pemv. Uncomment the CAfile option and set it to: CAfile = C:\AMT_061\CertGenerator\ExternalSecScripts\trusted_rootCA\trusted_cert.pemvi. Uncomment the debug = 7 option if you wish to refer detailed debugging information.vii. Save and close the file.
Setup: (continued)	<ul style="list-style-type: none">b. Move the stunnel configuration file back to C:\Program Files\stunnel\ from the Desktop.c. In Windows Explorer, navigate to the following directory and right click on <i>trusted_cert.cer</i>, select <i>Install Certificate</i>: C:\AMT_061\CertGenerator\ExternalSecScripts\trusted_rootCA\ The Certificate Import Wizard appears.<ul style="list-style-type: none">i. Click <i>Next</i> to move to the next screen.ii. Select the <i>Place all certificates in the following store</i> radio button.iii. Click the <i>Browse...</i> button.iv. In the <i>Select Certificate Store</i> dialog:<ul style="list-style-type: none">— Select the <i>Show physical stores</i> radio button.— Select the <i>Trusted Root Certification Authorities\Registry</i> store.— Click <i>OK</i> to close the dialog.v. Click <i>Next</i> to move to the next screen.vi. Click <i>Finish</i> on the last screen to close the Wizard and import the certificate.vii. A Security Warning dialog appears, click the <i>Yes</i> button to finish installation of the certificate.
Setup: (continued)	<p>8. Configure the MPS sample application:</p> <ul style="list-style-type: none">a. Edit the MPS configuration file stored in C:\AMT_061\MPS\conf\mps.config:<ul style="list-style-type: none">i. Modify the Network section so that it reads: [Network] AMTListenIP = 192.168.1.20 AMTListenPort = 20015 HttpListenIP = 192.168.1.20 HttpListenPort = 8080 SocksListenIP = 192.168.1.20 SocksListenPort = 4322 SOAPListenIP = 192.168.1.20 SOAPListenPort = 7793ii. Save and close the file.b. Edit the MPS notification list configuration file stored in C:\AMT_061\MPS\conf\NotificationList.config:<ul style="list-style-type: none">i. Modify the following line so that it reads: Original: http://195.168.1.1:9971 Modified: http://192.168.1.20:9971ii. Save and close the file.

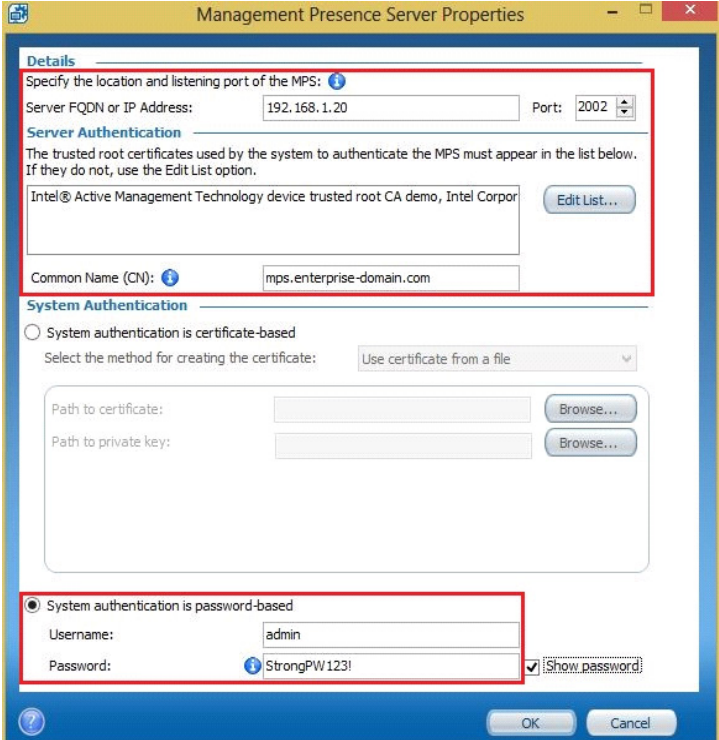


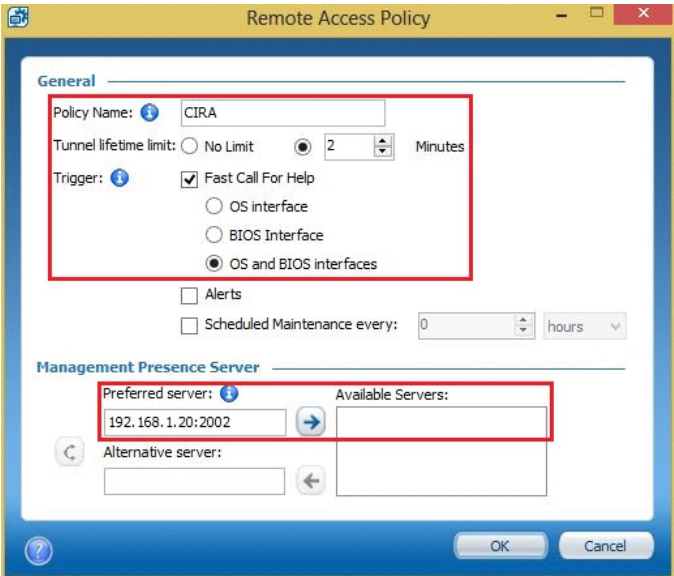
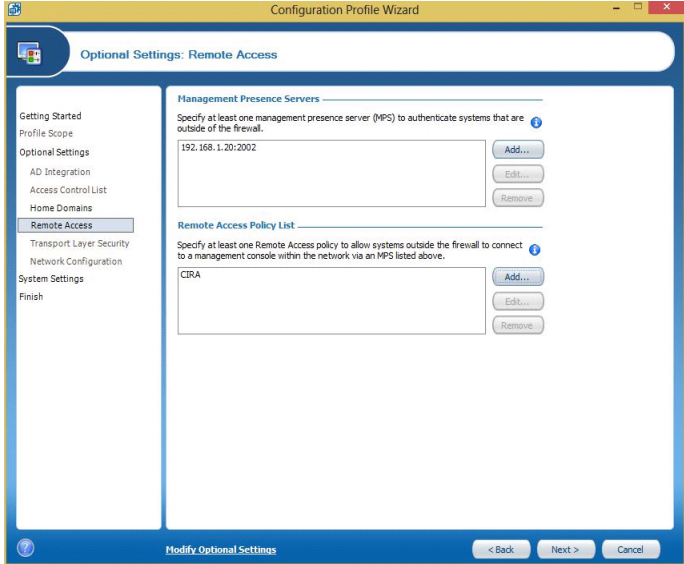
ID:	AMT_061
Procedure:	<p>Test Procedure Execution:</p> <p>Perform the following steps after configuring the Network Environment, the management console and verifying that the SUT is not provisioned. If the SUT is provisioned, there is a configuration failure later when trying to provision the SUT with the Intel® AMT Configuration Utility.</p> <ol style="list-style-type: none"> On the management console start the test infrastructure tools: <ol style="list-style-type: none"> Run the tunnel service by means of the following: <ol style="list-style-type: none"> Run <i>Windows Start tunnel Run</i> tunnel to start the application. A small icon appears in the System Tray. Right click on the <i>tunnel</i> System Tray icon and select <i>Log</i> to view the runtime log. Verify that there were no problems loading the MPS certificate and private key. 
Procedure: (continued)	<ol style="list-style-type: none"> Start the MPS sample application by means of the following: <ol style="list-style-type: none"> Open a DOS shell (<i>Windows+R -> "cmd" <enter></i>). Change directory to <i>C:\AMT_061\MPS\</i> and run <i>MPS.exe</i>.  <p>Note: To close the MPS sample application, use Microsoft Windows* Task Manager to find and terminate the process. Control+C interrupts are not processed by the application.</p> <p>Note: If the application exits soon after startup, verify the network configuration of the management console again.</p> <ol style="list-style-type: none"> Start the MPS Notification application to view incoming CIRA connections: <ol style="list-style-type: none"> Open a DOS shell (<i>Windows+R -> "cmd" <enter></i>). Change directory to <i>C:\AMT_061\</i> and run <i>MPSNotification.exe</i>. <p>Note: To close the MPS Notification application, press <i>Control+C</i>.</p> <ol style="list-style-type: none"> Run the Apache server by means of <i>Windows Start Apache HTTP Server 2.2 Control Apache Server / Start Apache</i> in Console to start the application. A black empty DOS Shell window appears.

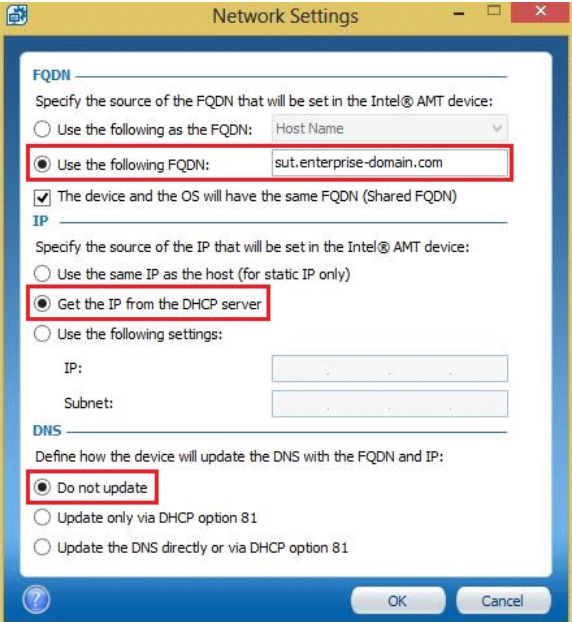
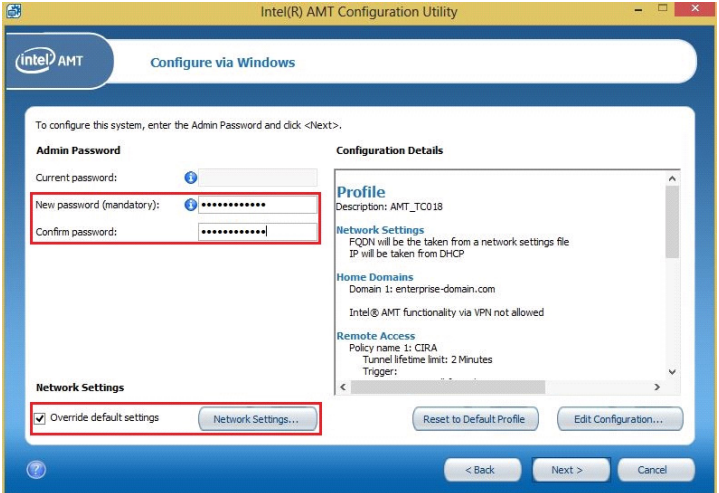
ID:	AMT_061
<p>Procedure: (continued)</p>	<p>2. On the SUT, start the Intel® AMT Configuration Utility ACSWizard.exe by double-clicking on it. If the current user is not an Administrator account, then the utility need to be run as Administrator:</p> <ol style="list-style-type: none"> At the application start screen, select Configure/Unconfigure this System. 
<p>Procedure: (continued)</p>	<ol style="list-style-type: none"> The Configuration Options window, select the default Configure by means of Microsoft Windows* option and then Next. 

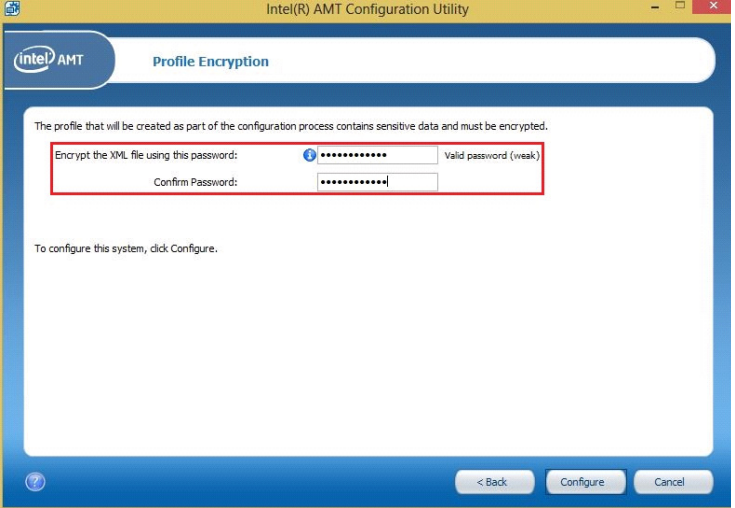
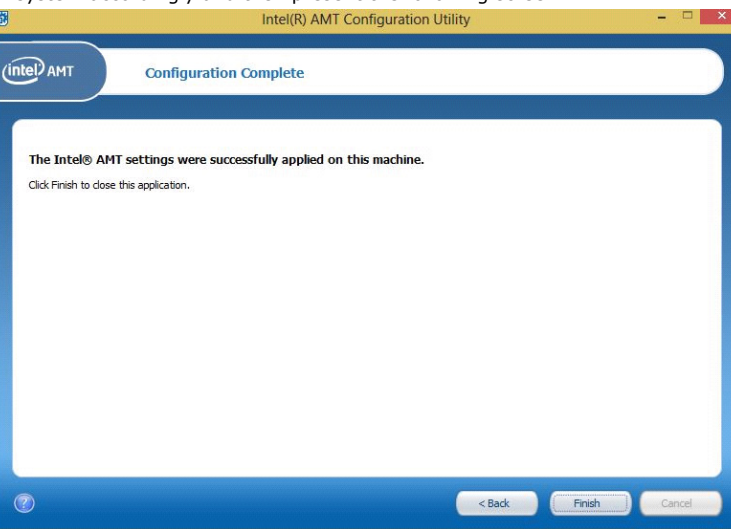
ID:	AMT_061
Procedure: (continued)	<p>c. In the Configure by means of Microsoft Windows* screen, select Edit Configuration...</p> 
Procedure: (continued)	<p>d. In the Getting Started screen, enter in "AMT_061" as the profile description and click Next.</p> 

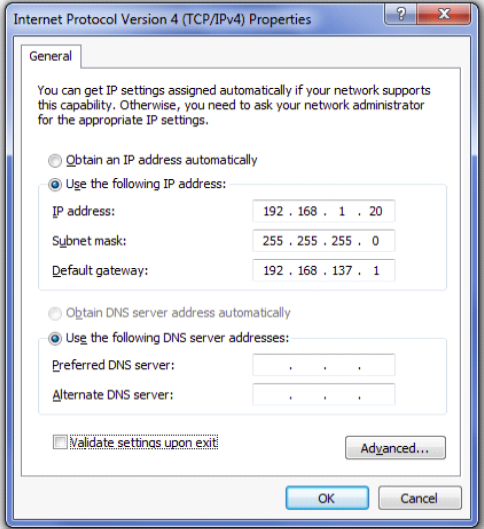
ID:	AMT_061
<p>Procedure: (continued)</p>	<p>e. In the Optional Settings screen, select the Home Domains and Remote Access check boxes and click Next.</p> 
<p>Procedure: (continued)</p>	<p>NOTE: Home Domains becomes greyed-out after Remote Access is selected. This is because Remote Access requires a Home Domain to be configured.</p> <p>f. In the <i>Optional Settings: Home Domains</i> screen, add the “enterprise-domain.com” home domain and click Next.</p> 

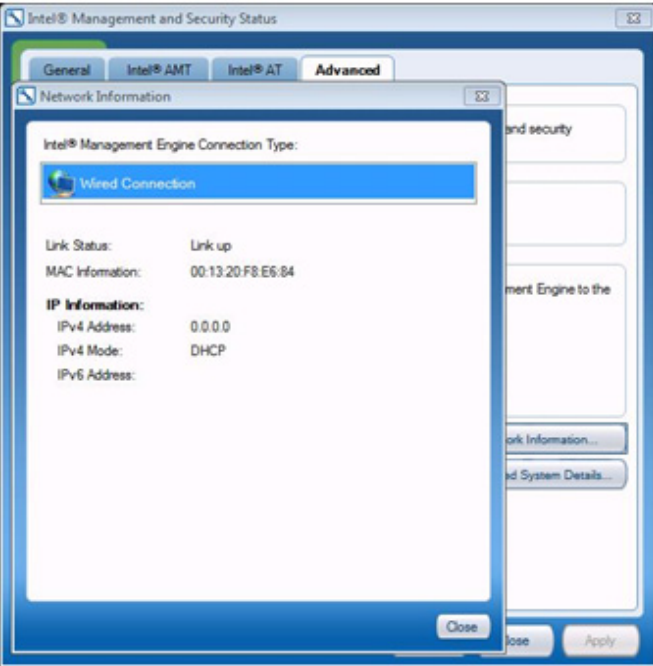
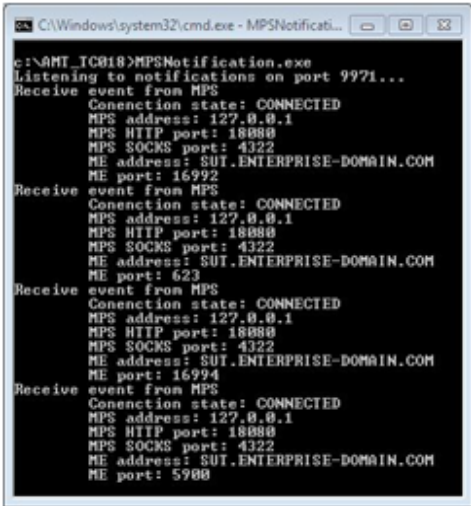
ID:	AMT_061
Procedure: (continued)	<p>g. In the Optional Settings: Remote Access screen, click Add to add a management presence server. In the Management Presence Server Properties dialog box:</p> <ol style="list-style-type: none"> Enter "192.168.1.20" for the Server FQDN or IP Address and set the Port to "2002". Enter "mps.enterprise-domain.com" into the Common Name (CN) field. Select the System authentication is password-based radio button and enter a Username of "admin" and a Password of "StrongPW123!" into their respective fields. 
Procedure: (continued)	<p>iv. Click Edit List... in the Server Authentication settings to add a trusted root certificate from file. Use the following file created on the management console: C:\AMT_061\CertGenerator\ExternalSecScripts\trusted_rootCA\trusted_cert.pem</p> <p>NOTE: That during the certificate installation, the following warning regarding the recommended period of validity for the certificate may appear. If so, click Yes to continue the configuration process.</p> <p>v. Click OK to close the dialog.</p> <p>h. Keeping within the Optional Settings: Remote Access screen, click Add to add a remote access policy. In the Remote Access Policy dialog box:</p> <ol style="list-style-type: none"> Enter "CIRA" for the Policy Name. Set the <i>Tunnel lifetime limit</i> to 2 minutes. Select the Trigger as <i>Fast Call For Help by means of the OS or BIOS interfaces</i>. Use the arrow to set the "192.168.1.20:2002" management presence server as the <i>Preferred server</i> from the available servers list.

ID:	AMT_061
<p>Procedure: (continued)</p>	<p>v. Enter "mps.enterprise-domain.com" into the <i>Common Name (CN)</i> field.</p>  <p>vi. Click <i>OK</i> to close the dialog.</p>
<p>Procedure: (continued)</p>	<p>i. The <i>Optional Setting: Remote Access</i> screen should appear as shown below; click <i>Next</i> to continue.</p>  <p>j. In the <i>System Settings</i> screen, leave all the default values as they are and click <i>Next</i>.</p> <p>k. On the <i>Finish</i> screen click <i>Finish</i> to close the wizard.</p>

ID:	AMT_061
<p>Procedure: (continued)</p>	<p>i. Back at the <i>Configure by means of the Microsoft Windows*</i> screen, check the <i>Override default settings</i> checkbox and click the <i>Network Settings...</i> button to open the <i>Network Settings</i> dialog:</p> <ol style="list-style-type: none"> Select the <i>Use the following FQDN</i> radio button and enter "sut.enterprise-domain.com" into the corresponding field. In the <i>IP</i> options, select the <i>Get the IP from the DHCP server</i> radio button. In the <i>DNS</i> options, select the <i>Do not update</i> radio button.  <p>iv. Click OK to close the dialog.</p>
<p>Procedure: (continued)</p>	<p>m. Finally, enter "StrongPW123!" for the <i>New password (mandatory)</i> and confirmation fields then click Next.</p> 

ID:	AMT_061
<p>Procedure: (continued)</p>	<p>n. The profile that has been created is encrypted to protect the Administrator passwords inside. In the <i>Profile Encryption</i> screen, enter "StrongPW123!" as the encryption password for the XML profile file.</p>  <p>NOTE: The profile created is stored in the ACU_Wizard directory as Profile.xml. The next time the application is launched and Configure by means of Microsoft Windows* is selected, it finds this file and ask for the password entered at this step to load the profile again.</p>
<p>Procedure: (continued)</p>	<p>Once this profile is created, there is no need to rebuild it on subsequent tests. Simply follow steps 2.a and 2.b, enter the profile file password, and then press the <i>Configure</i> button on the <i>Configure by means of the Microsoft Windows*</i> screen.</p> <p>o. Finally, provision the SUT with the settings that have been captured in the profile by clicking <i>Configure</i>. The application communicate with the Intel® ME to provision the system accordingly and then present the following screen.</p> 

ID:	AMT_061
Procedure: (continued)	<p>p. Click <i>Finish</i> to close the Intel® AMT Configuration Utility.</p> <p>Optional: If it is desired to run Intel® AMT features testing (such as SOL/Storage Redirection) under CIRA mode, on the management console change the MPS default as follows by means of the WLAN interface Internet Protocol Version 4 properties dialog:</p> 
Procedure: (continued)	<ul style="list-style-type: none"> • Enter the IP address the wireless IP assigned to management console (for example, 192.168.1.20) • Enter Subnet mask as 255.255.255.0 • Enter Default Gateway as 192.168.137.1 <p>This route all traffic from the MPS through the 192.168.137.x subnet in order to avoid packet loss when running Intel® AMT testing.</p> <p>NOTE: The configuration described above is only applicable to the example Test Environment described in this test case. For CIRA testing within an actual enterprise network environment, consult with IT regarding the applicable network topology and configuration.</p> <p>3. Move the SUT LAN connection to the Remote Network.</p> <ol style="list-style-type: none"> a. Open the <i>Intel® Management and Security Status</i> application on the SUT and select the <i>Advanced</i> tab.

ID:	AMT_061
<p>Procedure: (continued)</p>	<p>b. Click the <i>Network Information...</i> button to display the <i>Network Information</i> window:</p> <ol style="list-style-type: none"> The <i>Link Status</i>: should display <i>Link up</i>. The <i>IPv4 Address</i>: should be set to <i>0.0.0.0</i>.  <p>This indicates that the Environment Detection feature has determined that the SUT is operating outside of the Enterprise Network and has configured the Intel® ME network interface to allow only communications through the TLS tunnel.</p>
<p>Procedure: (continued)</p>	<p>4. Restart the SUT and press <i>Ctrl+Alt+F1</i> to initiate the <i>Fast Call for Help</i> process. On the management console, the MPS Notification application should report the following:</p> 



ID:	AMT_061
Procedure: (continued)	<p>Note: If the SUT cannot connect through to the MPS and generate a notification to the MPSNotification application:</p> <ul style="list-style-type: none"> — Check the stunnel error log. There may an error indicating that a certificate has expired. — If the Microsoft Windows* Firewall is running on the management console, it may also be necessary to open port 16993. Refer the documentation for the version of Microsoft Windows* on the management console for more details. <p>On the SUT, the next screen <u>may</u> be displayed (not visible on some implementations): Intel® Remote Assistance mechanism is trying to get a network connection. This may take a couple of minutes... Press <ESC> to abort...</p> <p>The next screen should display information about to the Remote Access connection: Connected to MPS Host 192.168.1.20 Press <ESCAPE> to close the connection and continue to boot Press <ENTER> to keep the connection and continue to boot</p>
Procedure: (continued)	<p>5. In the Web Browser on the management console, configure the Proxy Settings: For Microsoft* Internet Explorer, refer the instructions contained here: http://windows.microsoft.com/en-US/windows7/Change-proxy-settings-in-Internet-Explorer</p> <p>For Mozilla Firefox, refer the instructions contained here: http://support.mozilla.com/en-US/kb/Options+window++Advanced+panel#Connection_Settings_Dialog</p> <ol style="list-style-type: none"> Set the Address of the Proxy server to 192.168.1.20. Set the Port of the Proxy server to 8080. Apply the settings above for all protocols. (for example, HTTP, Secure, FTP, Socks) <p>6. In the Web Browser on the management console connect to the SUT using its FQDN. (for example, http://sut.enterprise-domain.com:16992)</p> <p>NOTE: This step must be completed before the connection timeout expires and the SUT disconnects from the MPS.</p> <ul style="list-style-type: none"> • If connection occurs in the Web Browser on the management console and a login page from the SUT resembling that of the Intel® ME WebUI appears, the end-to-end configuration of CIRA support has been confirmed. <p>7. In the Web Browser on the management console, reset the Proxy Settings back to their previous configuration before step 6.</p>
Procedure: (continued)	<p>8. On the management console shutdown the test infrastructure tools:</p> <ol style="list-style-type: none"> Shutdown the Apache server by means of the Microsoft Windows* Task Manager application: <ol style="list-style-type: none"> Find all processes named "httpd.exe" and terminate them. <p>NOTE: Closing the DOS shell window does not close the Apache server processes.</p> <ol style="list-style-type: none"> Shutdown the MPS Notification application by means of <i>Control+C</i> and exit the DOS shell. Shutdown the MPS sample application by means of the Microsoft Windows* Task Manager application: <ol style="list-style-type: none"> Find and terminate the "MPS.exe" process and terminate it. <p>NOTE: <i>Control+C</i> interrupts are <u>not</u> processed by the application.</p> <ol style="list-style-type: none"> Shutdown the stunnel service by: <ol style="list-style-type: none"> Right-click on the <i>stunnel</i> System Tray icon in the task bar and select <i>Exit</i>.
Pass Criteria:	The test passes if the Fast Call for Help connection was triggered, and Fast Call for Help session was established between the SUT and the MPS, and the SUT was successfully managed from the management console.



11.10 Settings, Storage, and Security Configuration

The section serves as a checklist for the environment setup and covers testing of the Settings, Storage, and Security Configuration features in Intel® AMT.

11.10.1 Test Environment

The System Under Test (SUT) is to be configured with Intel® AMT set in manual provisioning mode with static IP address or DHCP. The management console may be a laptop or a desktop with a version of Microsoft Windows* supported by Intel® PETS, and the SUT should have a version of Microsoft Windows* supported by Intel® PETS as well. The test network is comprised of a hub/switch and network cables.

Tools for testing:

- Intel® PETS: The latest version of the tool from the Intel® CSME Compliancy and Debug kit release. Refer the Intel® PETS User Guide for exact instructions on how to load and setup the Intel® PETS software.
- Intel® Automated Power Switch (Intel® APS): The SUT should be connected to an Intel® APS 3 unit. In case an Intel® APS 3 is not available, select the Manual configuration in the Intel® PETS SUT profile configuration menu.
- Intel® PETS Local Agent: The local agent must be installed on the SUT.

Where applicable, the wireless LAN interface on Intel® AMT must be on a different network/subnet than the wired LAN interface. For details on how to enter the network interface details into Intel® PETS, consult the Intel® PETS User Guide.

If the firmware image or the SUT configuration does not support some features, Intel® PETS show those features as failing when tested. Intel® PETS cannot determine in all cases which features have been deactivated and should thus be skipped during testing.

11.10.2 General Settings Information

ID:	AMT_070					
Title:	General Settings Information					
Requirement:	Optional					
System:	Form Factor		System Power Model	Intel® AMT Network Interface		LAN Type
	<input checked="" type="checkbox"/> Desktop <input checked="" type="checkbox"/> Workstation <input checked="" type="checkbox"/> Mobile	<input checked="" type="checkbox"/> Standard <input checked="" type="checkbox"/> Modern Standby or InstantGo*	<input type="checkbox"/> LAN <input checked="" type="checkbox"/> Either Used <input type="checkbox"/> WLAN <input type="checkbox"/> Not Used	<input checked="" type="checkbox"/> Integrated LAN <input checked="" type="checkbox"/> Discrete LAN <input type="checkbox"/> TBT Dock LAN		
Method:	Automated by Intel® PETS with test operator interaction					
Description:	The Intel® AMT interface supports access to general settings information about the system.					
Objective:	This test uses the Intel® AMT interface to extract the general settings information about the system and present it to the test operator.					
Setup:	The initial state of the SUT should be S0/MeOn with Host OS running. Intel® AMT should be provisioned via manual mode.					



ID:	AMT_070
Procedure:	<ol style="list-style-type: none"> Retrieve and display to the test operator general settings information, including: <ul style="list-style-type: none"> Configuration State Security Parameters <ul style="list-style-type: none"> Administrator Control Mode (ACM) or Client Control Mode (CCM) Transport Layer Security (TLS) (enabled/disabled) Hardware Cryptography (enabled/disabled) Network Interface (enabled/disabled) System BIOS Version Information Intel® ME Firmware Version Information Network Feature States <ul style="list-style-type: none"> Web UI (enabled/disabled) Storage Redirection (enabled/disabled) Serial-Over-LAN (SOL) (enabled/disabled) Keyboard, Video and Mouse (KVM) (enabled/disabled) Redirection Ports (enabled/disabled) Network Interface States <ul style="list-style-type: none"> LAN IPv4 and IPv6 (when available) Wireless LAN IPv4 and IPv6 (when available) IEEE 802.1x Profile Configuration
Pass Criteria:	The test passes if the information is collected and displayed to the test operator.

11.10.3 Security Administration Realm Interface

ID:	AMT_071			
Title:	Security Administration Realm Interface			
Requirement:	Optional			
System:	Form Factor <input checked="" type="checkbox"/> Desktop <input checked="" type="checkbox"/> Workstation <input checked="" type="checkbox"/> Mobile	System Power Model <input checked="" type="checkbox"/> Standard <input checked="" type="checkbox"/> Modern Standby or InstantGo*	Intel® AMT Network Interface <input type="checkbox"/> LAN <input checked="" type="checkbox"/> Either Used <input type="checkbox"/> WLAN <input type="checkbox"/> Not Used	LAN Type <input checked="" type="checkbox"/> Integrated LAN <input type="checkbox"/> Discrete LAN <input type="checkbox"/> TBT Dock LAN
Method:	Automated by Intel® PETS			
Description:	The Intel® AMT interface supports access to various functions via the Security Administration realm (ADMIN_SECURITY_ADMINISTRATION_REALM).			
Objective:	This test uses the Intel® AMT interface with access rights within the Security Administration realm to toggle the active Intel® AMT Power Package.			
Setup:	The initial state of the SUT should be S0/MeOn with Host OS running. Intel® AMT should be provisioned via manual mode.			
Procedure:	<ol style="list-style-type: none"> With credentials in the Security Administration realm, use the Intel® AMT interface to: <ol style="list-style-type: none"> get the active power package. set the power package to the opposite value (example: if Power Package 1, select Power Package 2, or vice versa). set the active power package back to the original value before the test started. 			
Pass Criteria:	The test passes if the active power package can be toggled using the Security Administration realm.			

11.10.4 Transport Layer Security (TLS) Authentication

ID:	AMT_073
Title:	Transport Layer Security (TLS) Authentication
Requirement:	Optional



ID:	AMT_073			
System:	Form Factor		System Power Model	Intel® AMT Network Interface
	<input checked="" type="checkbox"/> Desktop <input checked="" type="checkbox"/> Mobile	<input checked="" type="checkbox"/> Workstation	<input checked="" type="checkbox"/> Standard <input checked="" type="checkbox"/> Modern Standby or InstantGo*	<input type="checkbox"/> LAN <input type="checkbox"/> WLAN <input checked="" type="checkbox"/> Either Used <input type="checkbox"/> Not Used
				<input checked="" type="checkbox"/> Integrated LAN <input type="checkbox"/> Discrete LAN <input type="checkbox"/> TBT Dock LAN
Method:	Automated by Intel® PETS with test operator interaction			
Description:	The Intel® AMT interface supports access to the system via Transport Layer Security (TLS) authentication.			
Objective:	This test configures the Intel® AMT to enable TLS authentication and then retrieve the Intel® AMT core version via the secured interface.			
Setup:	The initial state of the SUT should be S0/MeOn with Host OS running. Intel® AMT should be provisioned via manual mode.			
Procedure:	<ol style="list-style-type: none">1. Warn the test operator that this test unprovision the SUT upon conclusion. If the test operator does not wish to have the SUT unprovisioned, they may select to abort the test in which case the test status is reflected as Aborted.2. Configure the SUT to enable TLS (server side authentication) via Intel® AMT.3. Install a certificate on the SUT allowing TLS Server side connection.4. Connect to the SUT with a TLS connection, and request the Intel® AMT core version.5. Verify that the SUT responded over the TLS connection.6. Fully unprovision the SUT.7. Verify the SUT is in Pre-Provisioning state.8. Prompt the test operator to provision the SUT again in order to proceed with other testing.			
Pass Criteria:	The test passes if the Intel® AMT core version is collected via TLS connection.			



11.10.5 Wake By Means of an Alarm Clock

11.10.5.1 Alarm Wake from S5

ID	AMT_074
Title	Alarm Wake from S5
Requirement	Optional
Method	Automated by Intel® PETS
Form Factor	Desktop/Mobile
Description	Original Power State: S0/CM0; Power Policy - PP2, ACDC;
Objective	This test checks that the system wakes up by means of Alarm Clock from S5/M3 state.
Setup	The initial state of the SUT should be S0/MeOn with Host OS running. Intel® AMT should be provisioned via manual mode.
Procedure	<ol style="list-style-type: none"> 1. Configure BIOS to keep the system in S5 after exiting G3. 2. Set the power source to AC + DC. 3. Boot the system to S0/CM0 and make sure OS is up. 4. Verify that Intel® CSME is on. This can be done by either checking SLP_A# signal, that should be de-asserted or running Intel® MEinfo tool indicating Intel® CSME is on. 5. Synchronize the Intel® CSME time with Universal Time Clock (UTC). 6. Set an alarm to another 5 minutes from now. 7. Move platform to S5. 8. Delay 6 minutes. 9. Verify platform is in S0. 10. Check HostBootReason (to confirm wake was caused by alarm). 11. Move to S5. 12. Delay 5 min. 13. Verify platform is in S0. 14. Check HostBootReason (to confirm wake was caused by alarm). 15. Delete alarm.
Test Pass/Fail Criteria	Host wakes up both times

11.10.5.2 Alarm Wake from S4

ID	AMT_075
Title	Alarm Wake from S4
Requirement	Optional
Method	Automated by Intel® PETS
Form Factor	Desktop/Mobile
Description	Original Power State: S0/CM0; Power Policy - PP2, ACDC;
Objective	This test checks that the system wakes up by means of Alarm Clock from S4/M3 state.



ID	AMT_075
Setup	The initial state of the SUT should be S0/MeOn with Host OS running. Intel® AMT should be provisioned via manual mode.
Procedure	<ol style="list-style-type: none">1. Configure BIOS to keep the system in S5 after exiting G3.2. Set the power source to AC + DC.3. Boot the system to S0/CM0 and make sure OS is up.4. Verify that Intel® CSME is on. This can be done by either checking SLP_A# signal, that should be de-asserted or running Intel® MEInfo tool indicating Intel® CSME is on.5. Synchronize the Intel® CSME time with Universal Time Clock (UTC).6. Set an alarm to another 5 minutes from now.7. Move platform to S4.8. Delay 6 minutes.9. Verify platform is in S0.10. Check HostBootReason (to confirm wake was caused by alarm).11. Move to S4.12. Delay 5 minutes.13. Verify platform is in S0.14. Check HostBootReason (to confirm wake was caused by alarm).15. Delete alarm.
Test Pass/ Fail Criteria	Host wakes up both times.



11.10.5.3 Alarm Wake from S3

ID	AMT_076
Title	Alarm Wake from S3
Requirement	Optional
Method	Automated by Intel® PETS
Form Factor	Desktop/Mobile
Description	Original Power State: S0/CM0; Power Policy - PP2, ACDC;
Objective	This test checks that the system wakes up by means of Alarm Clock from S3/M3 state.
Setup	The initial state of the SUT should be S0/MeOn with Host OS running. Intel® AMT should be provisioned via manual mode.
Procedure	<ol style="list-style-type: none"> 1. Configure BIOS to keep the system in S5 after exiting G3 2. Set the power source to AC + DC 3. Boot the system to S0/CM0 and make sure OS is up 4. Verify that Intel® CSME is on. This can be done by either checking SLP_A# signal, that should be de-asserted or running Intel® MEInfo tool indicating Intel® CSME is on. 5. Synchronize the Intel® CSME time with Universal Time Clock (UTC). 6. Set an alarm to another 5 minutes from now. 7. Move platform to S3. 8. Delay 6 minutes. 9. Verify platform is in S0. 10. Check HostBootReason (to confirm wake was caused by alarm). 11. Move to S3. 12. Delay 5 minutes. 13. Verify platform is in S0. 14. Check HostBootReason (to confirm wake was caused by alarm). 15. Delete alarm.
Test Pass/ Fail Criteria	Host wakes up both times

11.11 Remote Secure Erase

The section serves as a checklist for the environment setup and covers integration testing of the BIOS Remote Secure Erase boot option in Intel® AMT. This feature allows an IT administrator to remotely erase the system drive in a secure fashion; enabling effective system waterfall without the need for direct access.

Warning: The testing conducted in this section is specifically designed to check conformity to the Remote Secure Erase feature implementation; which if implemented properly, **ERASE** or otherwise **RENDER LOST** the **FULL CONTENTS** of the system drive of the System Under Test (SUT). Read the following information carefully to properly complete testing of this feature.

The following type(s) of drives are supported under the tests in this section:

- SATA - Following the Serial ATA (AT Attachment) interface specification. For these drives, **both** User and Master password credentials **must** be set before Remote Secure Erase can start.
- NVMe* - Following the Non-Volatile Memory Express* host controller interface specification, and implemented as a PCI Express* (PCIe*)-based SSD. These drives do not support password security.

The following type(s) of drives and/or drive configurations are **not yet** supported under the tests in this section:

- Opal* - Following the Trusted Computing Group™ Opal Security Subsystem Class (SSC) self-encrypting drive (SED) storage specification. These drives implement Opal Security Mode with associated Security ID (SID) support when Opal is activated/provisioned.

Important: A drive which supports Opal features, but has not yet been activated/provisioned, may still be eligible for text execution as long as it adheres to the requirements listed above for supported drive types.

Support for each of the drive types above is dependent on the system BIOS and in some cases the SUT's hardware configuration. The BIOS must inform the Intel® ME through the SMBIOS Type 130 table whether or not the Remote Secure Erase feature is supported as a capability of the BIOS (and system). This setting in the SMBIOS Type 130 table determines how the capability is advertised from the Intel® AMT API to remote management consoles. For more information about the BIOS integration requirements, refer the *Intel® ME BIOS Specification*.

The tests conducted herein:

- **Do not** verify actual erasure of data from the target drive(s). Implementation of the drive data erasure protocols deployed by the different drive types covered in this section is in some cases manufacturer dependent. Rather, the tests herein focus on confirming that proper integration of BIOS functionality with Intel® AMT to enable Remote Secure Erase feature support as follows:
 - Remote Secure Erase capability advertisement from Intel® AMT API per BIOS feature capability reporting in the SMBIOS Type 130 table.
 - Proper management within the Intel® ME of the Secure Erase boot option as set or cleared remotely by the management console.
 - Proper delivery of the Secure Erase boot option to the BIOS during the system boot process.
 - Proper management of the Secure Erase boot option by the BIOS upon completion of the actual drive erase activity.
 - Proper delivery of the drive password (where applicable), either via SOL/KVM redirection through Intel® AMT, or direct password input through Intel® AMT.
 - Proper implementation of BIOS last boot status after Secure Erase completion by the BIOS.
- **Assume** that the system has at least one primary drive supporting RSE. Support for simultaneous multiple drive Remote Secure Erase is determined by BIOS implementation and system configuration.

Tip: The ability to configure the drive password or authentication access procedures is also BIOS dependent (and in the case of Opal* may require third-party ISV software support to deactivate/unprovision before attempting Remote Secure Erase). Be sure to carefully review available third-party documentation regarding drive password and/or authentication configuration measures for the target drive before beginning testing. These topics are out-of-scope for this document, and Intel cannot provide support for them.

11.11.1 Test Environment

The tests in this section are based on the expectation that two kinds of drives have been prepared for testing, and that during testing the drives may be interchanged:

- **System Validation Drive** - is used for primary system validation for tests in this section, as well as others found in this document and beyond. Only one drive should be prepared for testing; and may be the same drive as had been used in other sections of this chapter.



- **Remote Secure Erase Drive** - is intended for tests in this section. One drive per supported drive type should be prepared. These drives may be fully erased multiple times, may not contain a valid Host OS to boot to, and do not contain any critical information necessary for system validation work.

The SUT is to be configured with Intel® AMT set in manual provisioning mode with static IP address or DHCP. The management console may be a laptop or a desktop with a version of Microsoft Windows* supported by Intel® PETS, and the **System Validation Drive** used with the SUT should have a version of Microsoft Windows* supported by Intel® PETS as well. The test network is comprised of a hub/switch and network cables.

Tools for testing:

- Intel® PETS: The latest version of the tool from the Intel® CSME Compliancy and Debug kit release. Refer the Intel® PETS User Guide for exact instructions on how to load and setup the Intel® PETS software.
- SUT: Should be connected to Intel® APS 3. In case an Intel® APS 3 is not available, select the Manual configuration in the Intel® PETS SUT profile configuration menu.
- Intel® PETS Local Agent: The local agent must be installed on the **System Validation Drive** of the SUT.

In order for Intel® PETS to work properly, ensure the following:

- the SUT has a valid System UUID. This can be checked by confirming a non-zero value is reported by the Intel® MEInfo tool.
- the firmware image is configured to **not** require user consent on redirection. This can be done by checking the following value of the SPI image via the Intel® FIT tool in the 'Intel(R) AMT' tab: 'Redirection Configuration' | 'Redirection Privacy / Security Level' set to "Default".

Where applicable, the wireless LAN interface on Intel® AMT must be on a different network/subnet than the wired LAN interface. For details on how to enter the network interface details into Intel® PETS, consult the Intel® PETS User Guide.

If the firmware image or the SUT configuration does not support some features, Intel® PETS show those features as failing when tested. Intel® PETS cannot determine in all cases which features have been deactivated and should thus be skipped during testing.

11.11.1.1 Common Issues and Troubleshooting

Warning: If there is a failure during testing, **DO NOT** reconnect the **System Validation Drive** with the SUT, as the Secure Erase boot option may still be set in firmware (even after G3). In this case, first use test AMT_080 to safely clear the Secure Erase boot option before proceeding with any further testing or corrective action.

The following is a list of common issues that can occur during Remote Secure Erase testing and associated recommendations on how to check test environment and system configuration.

1. Remote Secure Erase did not start.
 - Verify that the BIOS and system support the feature. Check the SMBIOS Type 130 table which the BIOS provides to the Intel® ME firmware to confirm that the capability is indeed enabled.
 - Verify that the **Remote Secure Erase Drive** is properly attached to the system and that the BIOS can properly identify it. Depending on BIOS implementation, there may be considerations regarding boot list ordering, and therefore may require drive relocation to the first position in the boot list in order to be identified by the BIOS as a device for use with Remote Secure



Erase. Confirm with the system BIOS design for implementation specific details related to **Remote Secure Erase Drive** detection. Refer the *Intel® ME BIOS Specification* for further information boot order and Secure Erase command execution order.

2. Remote Secure Erase did not complete successfully for an unlocked drive which **does not require** authentication (password or user authentication).

When this occurs, the SUT should shutdown and the Secure Erase boot option remain set. In this case, on the following boot, the BIOS detects the Secure Erase boot option and attempt the erase operation again.

IT administrators who set the Secure Erase boot option and initiate system boot can check the boot option setting as well as the Intel® AMT API to verify if the boot options had been cleared upon successful erasure.

Failure to properly execute secure erase and clear the Secure Erase boot option may occur for several reasons. Verify the following when a failure occurs:

- Erase feature is not supported by the BIOS or system for the target drive.
- Target drive is not properly installed or connected.
- BIOS feature support not completely implemented.
- Target drive failure to perform selected erase action.

3. Remote Secure Erase did not complete successfully for a locked drive which **does require** authentication (password or user authentication).

When this occurs, it may be necessary to connect to the SUT via Serial-Over-LAN (SOL) or Keyboard, Video, and Mouse (KVM) to view and respond to the authentication prompt displayed on the SUT screen if the drive password was **not** already provided directly via Intel® AMT for use during the Remote Secure Erase procedure.

In the case where User Consent is required to establish a SOL or KVM session, a timeout may occur where the User Consent display expires without confirmation from the management console. In this case, a drive authentication timeout occurs.

As such, verify the following when a failure occurs:

- Failure to input the correct password or to properly authenticate with the target drive.
- A User Consent code timeout did not occur during KVM or SOL session activation.

Note: All tests in this section, other than test AMT_080, require that Intel® AMT power package be set to Power Package 2 (Intel® ME on in S0, wake in Sx/AC) on the SUT. If the WLAN network interface is used, the Intel® AMT WLAN link policy is set to Link Policy 3 (Enabled in S0, Sx/AC) on the SUT. The intention is to allow the Secure Erase state to be cleared via test AMT_080 in the case where there is a failure during boot and the BIOS shuts down the system to S5.

11.11.2 Clear Secure Erase Boot Option

ID:	AMT_080
Title:	Clear Secure Erase Boot Option
Requirement:	Mandatory - exempt for systems which do not support the Secure Erase boot option



ID:	AMT_080			
System:	Form Factor		System Power Model	Intel® AMT Network Interface
	<input checked="" type="checkbox"/> Desktop <input checked="" type="checkbox"/> Workstation <input checked="" type="checkbox"/> Mobile	<input checked="" type="checkbox"/> Standard <input checked="" type="checkbox"/> Modern Standby or InstantGo*	<input type="checkbox"/> LAN <input checked="" type="checkbox"/> Either Used <input type="checkbox"/> WLAN <input type="checkbox"/> Not Used	<input checked="" type="checkbox"/> Integrated LAN <input type="checkbox"/> Discrete LAN <input type="checkbox"/> TBT Dock LAN
Method:	Automated by Intel® PETS with test operator interaction			
Description:	This test attempts to clear the Remote Secure Erase boot option.			
Objective:	Verify that the BIOS properly advertises the Secure Erase boot option as a capability via the SMBIOS Type 130 table. If the capability is properly configured, the Intel® AMT API indicate feature support. The test then check the boot option setting, and attempt to clear it.			
Setup:	<p>The initial state of the SUT may be in either S0 or S3/S4/S5 with either Power Package 1 (Intel® ME on in S0) or Power Package 2 (Intel® ME on in S0, wake in Sx/AC) applied to Intel® AMT respectively. Similarly if the WLAN network interface is used, the Intel® AMT WLAN link policy on the SUT must be set to either Link Policy 2 (Enabled in S0) when the system is in S0, or Link Policy 3 (Enabled in S0, Sx/AC) when the system is in S5.</p> <p>The test would not pass if the system is in G3 or Deep Sx, or if the WLAN network interface is used but not configured in the appropriate Link Policy 2 or Link Policy 3 for the SUT Sx state.</p> <p>The test would not apply power to a SUT if found in G3. Doing so, with the risk that the Secure Erase boot option is set in firmware, may lead to the system booting from S5 and starting the erasure process on an attached drive.</p>			
Procedure:	<ol style="list-style-type: none"> Request the test operator to perform the following steps: Steps 1 through 3, if the Remote Secure Erase Drive has NOT already been installed. <ol style="list-style-type: none"> Shut down the SUT gracefully to G3 (if needed). Install the Remote Secure Erase Drive for testing. Attach AC power. Boot the SUT, with the Remote Secure Erase Drive, to the Intel® MEBX menu. NOTE: It may be necessary to enter a drive password. Wait for 3 minutes, when only the WLAN network interface is available. This is to allow network connectivity stabilization with the active WLAN profile. Set the active power package on the SUT to Power Package 2 (Intel® ME on in S0, wake in Sx/AC). Set the Intel® AMT WLAN link policy on the SUT to Link Policy 3 (Enabled in S0, Sx/AC), when only the WLAN network interface is available. Verify that Intel® AMT is available by requesting its version. Check that the SUT supports booting to Secure Erase by querying the Intel® AMT and checking the boot capabilities. <ol style="list-style-type: none"> If supported, continue to the next step. If not supported, end the test and request the test operator to confirm the BIOS support of 'Secure Erase' OEMCapabilities3 setting provided to the Intel® ME via the SMBIOS Type 130 table. Get the Secure Erase boot option setting on the SUT via Intel® AMT and log it. Clear the Secure Erase boot option on the SUT via Intel® AMT. Perform a Remote Power-Down of the SUT via Intel® AMT. Verify that the SUT is in S5. 			
Pass Criteria:	This test passes if the system was in a supported state at the beginning of testing, and Intel® AMT could be used to confirm the Secure Erase boot option capability, check its status, and clear the setting if set.			
References:	For details on the Secure Erase boot option, refer the <i>Intel® ME BIOS Specification</i> .			

11.11.3 Remote Secure Erase without Drive Authentication

ID:	AMT_081
Title:	Remote Secure Erase without Drive Authentication
Requirement:	Mandatory - exempt for systems which: <ul style="list-style-type: none"> do not support the Secure Erase boot option, or support only configurations requiring drive authentication



ID:	AMT_081			
System:	Form Factor <input checked="" type="checkbox"/> Desktop <input checked="" type="checkbox"/> Workstation <input checked="" type="checkbox"/> Mobile	System Power Model <input checked="" type="checkbox"/> Standard <input checked="" type="checkbox"/> Modern Standby or InstantGo*	Intel® AMT Network Interface <input type="checkbox"/> LAN <input checked="" type="checkbox"/> Either Used <input type="checkbox"/> WLAN <input type="checkbox"/> Not Used	LAN Type <input checked="" type="checkbox"/> Integrated LAN <input type="checkbox"/> Discrete LAN <input type="checkbox"/> TBT Dock LAN
Method:	Automated by Intel® PETS with test operator interaction			
Description:	This test attempts to initiate the Remote Secure Erase boot option and verify that the BIOS has completed execution of the erase operation on a drive which does not require authentication.			
Objective:	<p>Verify that the BIOS properly advertises and implements the Secure Erase boot option on system configurations which do not require drive authentication.</p> <p>This test is intended for systems which support NVMe* drives which do not require password configuration, or systems which support SATA drives and do not require end-user drive password configuration (as may be provided via supplemental BIOS feature support).</p>			
Setup:	<p>The initial state of the SUT should be either G3 or S5 with the Remote Secure Erase Drive attached after executing AMT_080. Intel® AMT should be provisioned via manual mode with Power Package 2 (Intel® ME on in S0, wake in Sx/AC) and Intel® AMT WLAN link policy on the SUT to Link Policy 3 (Enabled in S0, Sx/AC), when only the WLAN network interface is available.</p>			
Procedure:	<ol style="list-style-type: none"> 1. Prompt the test operator exit this test and run AMT_080 with the target Remote Secure Erase Drive if they have not done so already. 2. Request the test operator to perform the following steps: Steps 1 through 4, if the BIOS settings have NOT already been confirmed. <ol style="list-style-type: none"> 1. Boot the SUT to the BIOS menu. 2. Verify device boot order to ensure BIOS' Remote Secure Erase Drive detection. 3. Ensure the drive password(s) have been cleared for applicable drives as needed. 4. Save any BIOS settings changes. 5. Shutdown the SUT to S5. <p>NOTE: It may be necessary to enter a drive password during these steps.</p> <ol style="list-style-type: none"> 3. Verify that the SUT is in S5. 			
Procedure: (continued)	<ol style="list-style-type: none"> 4. Prompt the test operator to acknowledge that operations past this point may ERASE or otherwise RENDER LOST the FULL CONTENTS of the system drive. The test operator may cancel the test at this time via the prompt or via Intel® PETS test controls. 5. Check that the SUT supports booting to Secure Erase by querying the Intel® AMT and checking the boot capabilities. <ol style="list-style-type: none"> a. If supported, continue to the next step. b. If not supported, end the test and request the test operator to confirm the BIOS support of 'Secure Erase' OEMCapabilities3 setting provided to the Intel® ME via the SMBIOS Type 130 table. 6. Cancel any existing Intel® AMT user consent session which may be active on the SUT. 7. Ensure the Intel® AMT user consent opt-in setting is disabled on the SUT. 8. Set the Secure Erase boot option on the SUT via Intel® AMT. 9. Perform a Remote Power-Up of the SUT via Intel® AMT. 10. Wait for the SUT to return to S0/MeOn. At this point, the BIOS should receive the Secure Erase boot option and begin drive erasure. 11. Poll the system for S5 for 10 minutes (maximum wait) for drive erasure completion. The test operator is able to configure the polling duration to control the maximum duration for drives that take longer to complete erasure. 12. Get the Secure Erase boot option setting on the SUT via Intel® AMT and log it. 13. Clear the Secure Erase boot option on the SUT via Intel® AMT (safety precaution). 14. Verify that the BIOS last boot status reports success via Intel® AMT. 15. Verify that the value of Secure Erase boot option setting retrieved at step 11 was cleared by the BIOS. 			
Procedure: (continued)	<ol style="list-style-type: none"> 16. Set the SUT to G3 via Intel® APS. 17. Verify that the SUT is in G3. <p>If there was a failure during the test, consider running AMT_080 to safely clear the Secure Erase boot option before returning the System Validation Drive to the SUT.</p>			
Pass Criteria:	This test passes if the Remote Secure Erase Drive supported by the SUT can be erased remotely using the Secure Erase boot option, and the BIOS successfully clears the boot options at the end of the operation.			
References:	For details on the Secure Erase boot option, refer the <i>Intel® ME BIOS Specification</i> .			



11.11.4 Remote Secure Erase with Drive Authentication via SOL Redirection

ID:	AMT_082											
Title:	Remote Secure Erase with Drive Authentication via Serial-Over-LAN (SOL) Redirection											
Requirement:	Mandatory - exempt for systems which: <ul style="list-style-type: none">do not support the Secure Erase boot option, orsupport only NVMe* configurations not requiring drive authentication											
System:	<table><tr><th>Form Factor</th><th>System Power Model</th><th>Intel® AMT Network Interface</th><th>LAN Type</th></tr><tr><td><input checked="" type="checkbox"/> Desktop <input checked="" type="checkbox"/> Workstation</td><td><input checked="" type="checkbox"/> Standard <input checked="" type="checkbox"/> Modern Standby or InstantGo*</td><td><input type="checkbox"/> LAN <input checked="" type="checkbox"/> Either Used <input type="checkbox"/> WLAN <input type="checkbox"/> Not Used</td><td><input checked="" type="checkbox"/> Integrated LAN <input type="checkbox"/> Discrete LAN <input type="checkbox"/> TBT Dock LAN</td></tr></table>	Form Factor	System Power Model	Intel® AMT Network Interface	LAN Type	<input checked="" type="checkbox"/> Desktop <input checked="" type="checkbox"/> Workstation	<input checked="" type="checkbox"/> Standard <input checked="" type="checkbox"/> Modern Standby or InstantGo*	<input type="checkbox"/> LAN <input checked="" type="checkbox"/> Either Used <input type="checkbox"/> WLAN <input type="checkbox"/> Not Used	<input checked="" type="checkbox"/> Integrated LAN <input type="checkbox"/> Discrete LAN <input type="checkbox"/> TBT Dock LAN			
Form Factor	System Power Model	Intel® AMT Network Interface	LAN Type									
<input checked="" type="checkbox"/> Desktop <input checked="" type="checkbox"/> Workstation	<input checked="" type="checkbox"/> Standard <input checked="" type="checkbox"/> Modern Standby or InstantGo*	<input type="checkbox"/> LAN <input checked="" type="checkbox"/> Either Used <input type="checkbox"/> WLAN <input type="checkbox"/> Not Used	<input checked="" type="checkbox"/> Integrated LAN <input type="checkbox"/> Discrete LAN <input type="checkbox"/> TBT Dock LAN									
Method:	Automated by Intel® PETS with test operator interaction											
Description:	This test attempts to initiate the Remote Secure Erase boot option and verify that the BIOS has completed execution of the erase operation on a drive which requires authentication via Serial-Over-LAN (SOL).											
Objective:	<p>Verify that the BIOS properly advertises and implements the Secure Erase boot option for drives which require authentication via Serial-Over-LAN (SOL). Proper User Consent verification is also confirmed.</p> <p>This test should be run once per each drive type supported on the SUT (which have been prepared via one sample each in the set of Remote Secure Erase Drives described in the beginning of this section).</p>											
Setup:	<p>The initial state of the SUT should be either G3 or S5 with the Remote Secure Erase Drive attached after executing AMT_080. Intel® AMT should be provisioned via manual mode with Power Package 2 (Intel® ME on in S0, wake in Sx/AC) and Intel® AMT WLAN link policy on the SUT to Link Policy 3 (Enabled in S0, Sx/AC), when only the WLAN network interface is available.</p> <p>Before running this test, ensure that SOL is enabled in the Intel® MEBX.</p> <p>The default number of rows shown in the Putty terminal window may differ from the number of rows displayed by the BIOS. When this occurs, the Putty terminal display incurs line wrapping problems. To avoid this problem, change the settings of the Putty application to align with the BIOS via the following steps:</p> <ol style="list-style-type: none">Open the ".\Intel(R) Platform Enablement Test Suite\Plugins\Me\Redirection\bin\" directory.Start putty.exe, and in the Category section:<ol style="list-style-type: none">Select Window, and change the Rows value to the required number of rows.Select Session, then select <i>Default Settings</i>, and finally click the <u>S</u>ave button.Close the Putty Configuration window.To confirm, start putty.exe again, and make sure Row number is set to the new value.											
Procedure:	<ol style="list-style-type: none">Prompt the test operator exit this test and run AMT_080 with the target Remote Secure Erase Drive if they have not done so already.Request the test operator to perform the following steps: Steps 1 through 4, if the BIOS settings have NOT already been confirmed.<ol style="list-style-type: none">Boot the SUT to the BIOS menu.Verify device boot order to ensure BIOS' Remote Secure Erase Drive detection.Ensure the drive password(s) have been set.Save any BIOS settings changes.---Shutdown the SUT to S5. <p>NOTE: It may be necessary to enter a drive password during these steps.</p> <ol style="list-style-type: none">Verify that the SUT is in S5.											



ID:	AMT_082
Procedure: (continued)	<ol style="list-style-type: none">4. Prompt the test operator to acknowledge that operations past this point may ERASE or otherwise RENDER LOST the FULL CONTENTS of the system drive. The test operator may cancel the test at this time via the prompt or via Intel® PETS test controls.5. Check that the SUT supports booting to Secure Erase by querying the Intel® AMT and checking the boot capabilities.<ol style="list-style-type: none">a. If supported, continue to the next step.b. If not supported, end the test and request the test operator to confirm the BIOS support of 'Secure Erase' OEMCapabilities3 setting provided to the Intel® ME via the SMBIOS Type 130 table.6. Ensure the TCP maximum data retransmission setting defined in the SUT profile is applied to both a) the management console, and b) the SUT via Intel® AMT, if the WLAN network interface is used.<p>If the configuration on the management console is not already aligned to the SUT profile setting, the network stack on the management console need to be reset; leading to potential network connectivity loss for other applications on the system.</p><p>Before synchronizing the setting on the management console, provide a warning to the test operator, with the option to proceed or cancel, indicating the TCP maximum data retransmission network setting is about to be changed and that it may be necessary to re-establish network connectivity for any other applications running on the management console. If the test operator chooses to cancel, the test step is marked as failed.</p>7. Ensure the Intel® AMT redirection ports are enabled on the SUT.8. Cancel any existing Intel® AMT user consent session which may be active on the SUT.9. Ensure the Intel® AMT user consent opt-in setting is disabled on the SUT.10. Prompt the test operator to input the drive password via the Putty terminal program on the management console. <p>NOTE: For SATA drives, the Master password should be used.</p> <ol style="list-style-type: none">11. Use Intel® AMT to set the SUT boot options to use SOL Redirection and activate Secure Erase on the next boot.12. Open a SOL Redirection session with the SUT via Intel® AMT using the Putty terminal program on the management console.13. Perform a Remote Power-Up of the SUT via Intel® AMT.14. Wait for the SUT to return to S0/MeOn. At this point, the BIOS should receive the Secure Erase boot option and begin drive erasure, but stop at a drive authentication prompt.15. Close the SOL Redirection session with the SUT via Intel® AMT.16. Poll the system for S5 for 10 minutes (maximum wait) for drive erasure completion. The test operator is able to configure the polling duration to control the maximum duration for drives that take longer to complete erasure.17. Get the Secure Erase boot option setting on the SUT via Intel® AMT and log it.18. Clear the Secure Erase boot option on the SUT via Intel® AMT (safety precaution).19. Verify that the BIOS last boot status reports success via Intel® AMT.20. Verify that the value of Secure Erase boot option setting retrieved at step 15 was cleared by the BIOS.



ID:	AMT_082
Procedure: (continued)	<p>21. Request the test operator to perform the following steps: Steps 1 through 4, if the BIOS settings have NOT already been confirmed.</p> <ol style="list-style-type: none"> Boot the SUT to the BIOS menu. Verify device boot order to ensure BIOS' Remote Secure Erase Drive detection. Ensure the drive password(s) have been set. Save any BIOS settings changes. <p>---</p> <ol style="list-style-type: none"> Boot the SUT to S0. <p>NOTE: It may be necessary to enter a drive password.</p> <p>22. Verify that the SUT is in S0.</p> <p>23. Wait for 3 minutes, when only the WLAN network interface is available. This is to allow network connectivity stabilization with the active WLAN profile.</p> <p>24. Wait until Intel® AMT responds to WS-MAN call.</p> <p>25. Ensure the Intel® AMT user consent opt-in setting is enabled for boot options (ALL) on the SUT.</p> <p>26. Initiate a user consent session with Intel® AMT.</p> <p>27. Perform a Remote Power-Down of the SUT via Intel® AMT.</p> <p>28. Verify that the SUT is in S5.</p> <p>29. Prompt the test operator to input the drive password via the Putty terminal program on the management console.</p> <p>NOTE: For SATA drives, the Master password should be used.</p> <p>30. Use Intel® AMT to set the SUT boot options to use SOL Redirection and activate Secure Erase on the next boot.</p> <p>31. Open a SOL Redirection session with the SUT via Intel® AMT using the Putty terminal program on the management console.</p> <p>32. Perform a Remote Power-Up of the SUT via Intel® AMT.</p> <p>33. Wait for the SUT to return to S0/MeOn. At this point, the BIOS should receive the Secure Erase boot option and begin drive erasure, but stop at a drive authentication prompt.</p> <p>34. Close the SOL Redirection session with the SUT via Intel® AMT.</p> <p>35. Poll the system for S5 for 10 minutes (maximum wait) for drive erasure completion. The test operator is able to configure the polling duration to control the maximum duration for drives that take longer to complete erasure.</p> <p>36. Get the Secure Erase boot option setting on the SUT via Intel® AMT and log it.</p> <p>37. Clear the Secure Erase boot option on the SUT via Intel® AMT (safety precaution).</p> <p>38. Verify that the BIOS last boot status reports success via Intel® AMT.</p> <p>39. Verify that the value of Secure Erase boot option setting retrieved at step 35 was cleared by the BIOS.</p>
Procedure: (continued)	<p>40. Set the SUT to G3 via Intel® APS.</p> <p>41. Verify that the SUT is in G3.</p> <p>42. Request the test operator to repeat the test for each remaining representative type of Remote Secure Erase Drive supported by the SUT. Otherwise, return the System Validation Drive to the SUT.</p> <p>If there was a failure during the test, consider running AMT_080 to safely clear the Secure Erase boot option before returning the System Validation Drive to the SUT.</p>
Pass Criteria:	This test passes if each of the representative sample types of Remote Secure Erase Drive supported by the SUT can each be erased remotely using the Secure Erase boot option with drive authentication via SOL (also under User Consent control), and the BIOS successfully clears the boot options at the end of each operation.
References:	For details on the Secure Erase boot option, refer the <i>Intel® ME BIOS Specification</i> .

11.11.5 Remote Secure Erase with Drive Authentication via KVM Redirection

ID:	AMT_083
Title:	Remote Secure Erase with Drive Authentication via Keyboard, Video and Mouse (KVM) Redirection
Requirement:	<p>Mandatory - exempt for systems which:</p> <ul style="list-style-type: none"> Do not support the Secure Erase boot option, or Support only NVMe* configurations not requiring drive authentication, or Do not support KVM with internal graphics



ID:	AMT_083			
System:	Form Factor <input checked="" type="checkbox"/> Desktop <input checked="" type="checkbox"/> Workstation <input checked="" type="checkbox"/> Mobile	System Power Model <input checked="" type="checkbox"/> Standard <input checked="" type="checkbox"/> Modern Standby or InstantGo*	Intel® AMT Network Interface <input type="checkbox"/> LAN <input checked="" type="checkbox"/> Either Used <input type="checkbox"/> WLAN <input type="checkbox"/> Not Used	LAN Type <input checked="" type="checkbox"/> Integrated LAN <input type="checkbox"/> Discrete LAN <input type="checkbox"/> TBT Dock LAN
Method:	Automated by Intel® PETS with test operator interaction			
Description:	This test attempts to initiate the Remote Secure Erase boot option and verify that the BIOS has completed execution of the erase operation on a drive which requires authentication via Keyboard, Video and Mouse (KVM).			
Objective:	<p>Verify that the BIOS properly advertises and implements the Secure Erase boot option for drives which require authentication via Keyboard, Video and Mouse (KVM). Proper User Consent verification is also confirmed.</p> <p>This test should be run once per each drive type supported on the SUT (which have been prepared via one sample each in the set of Remote Secure Erase Drives described in the beginning of this section).</p>			
Setup:	<p>The initial state of the SUT should be either G3 or S5 with the Remote Secure Erase Drive attached after executing AMT_080. Intel® AMT should be provisioned via manual mode with Power Package 2 (Intel® ME on in S0, wake in Sx/AC) and Intel® AMT WLAN link policy on the SUT to Link Policy 3 (Enabled in S0, Sx/AC), when only the WLAN network interface is available.</p> <p>Before running this test, ensure that KVM is enabled in the Intel® MEBX. If the SUT supports switchable graphics, graphics configuration should be set to integrated graphics.</p>			
Procedure:	<ol style="list-style-type: none"> Prompt the test operator exit this test and run AMT_080 with the target Remote Secure Erase Drive if they have not done so already. Request the test operator to perform the following steps: Steps 1 through 4, if the BIOS settings have NOT already been confirmed. <ol style="list-style-type: none"> Boot the SUT to the BIOS menu. Verify device boot order to ensure BIOS' Remote Secure Erase Drive detection. Ensure the drive password(s) have been set. Save any BIOS settings changes. <p>---</p> <ol style="list-style-type: none"> Shutdown the SUT to S5. <p>NOTE: It may be necessary to enter a drive password during these steps.</p> <ol style="list-style-type: none"> Verify that the SUT is in S5. 			



ID:	AMT_083
Procedure: (continued)	<ol style="list-style-type: none"> 4. Prompt the test operator to acknowledge that operations past this point may ERASE or otherwise RENDER LOST the FULL CONTENTS of the system drive. The test operator may cancel the test at this time via the prompt or via Intel® PETS test controls. 5. Check that the SUT supports booting to Secure Erase by querying the Intel® AMT and checking the boot capabilities. <ol style="list-style-type: none"> a. If supported, continue to the next step. b. If not supported, end the test and request the test operator to confirm the BIOS support of 'Secure Erase' OEMCapabilities3 setting provided to the Intel® ME via the SMBIOS Type 130 table. 6. Ensure the TCP maximum data retransmission setting defined in the SUT profile is applied to both a) the management console, and b) the SUT via Intel® AMT, if the WLAN network interface is used. If the configuration on the management console is not already aligned to the SUT profile setting, the network stack on the management console need to be reset; leading to potential network connectivity loss for other applications on the system. Before synchronizing the setting on the management console, provide a warning to the test operator, with the option to proceed or cancel, indicating the TCP maximum data retransmission network setting is about to be changed and that it may be necessary to re-establish network connectivity for any other applications running on the management console. If the test operator chooses to cancel, the test step is marked as failed. 7. Ensure the Intel® AMT redirection ports are enabled on the SUT. 8. Cancel any existing Intel® AMT user consent session which may be active on the SUT. 9. Ensure the Intel® AMT user consent opt-in setting is disabled on the SUT. 10. Prompt the test operator to input the drive password via the VNC Viewer program on the management console. <p>NOTE: For SATA drives, the Master password should be used.</p> <ol style="list-style-type: none"> 11. Set the KVM password to 'Admin!98' on the SUT via Intel® AMT. 12. Ensure that the VNC port 5900 is enabled on the SUT via Intel® AMT. 13. Open a KVM Redirection session with the SUT via Intel® AMT using the VNC Viewer on the management console. 14. Set the Secure Erase boot option on the SUT via Intel® AMT. 15. Perform a Remote Power-Up of the SUT via Intel® AMT. 16. Wait for the SUT to return to S0/MeOn. At this point, the BIOS should receive the Secure Erase boot option and begin drive erasure, but stop at a drive authentication prompt. 17. Close the KVM Redirection session with the SUT via Intel® AMT. 18. Poll the system for S5 for 10 minutes (maximum wait) for drive erasure completion. The test operator is able to configure the polling duration to control the maximum duration for drives that take longer to complete erasure. 19. Get the Secure Erase boot option setting on the SUT via Intel® AMT and log it. 20. Clear the Secure Erase boot option on the SUT via Intel® AMT (safety precaution). 21. Verify that the BIOS last boot status reports success via Intel® AMT. 22. Verify that the value of Secure Erase boot option setting retrieved at step 17 was cleared by the BIOS.



ID:	AMT_083
Procedure: (continued)	<p>23. Request the test operator to perform the following steps: Steps 1 through 4, if the BIOS settings have NOT already been confirmed.</p> <ol style="list-style-type: none"> 1. Boot the SUT to the BIOS menu. 2. Verify device boot order to ensure BIOS' Remote Secure Erase Drive detection. 3. Ensure the drive password(s) have been set. 4. Save any BIOS settings changes. <p>---</p> <ol style="list-style-type: none"> 5. Shutdown the SUT to S5. <p>Note: It may be necessary to enter a drive password during these steps.</p> <p>24. Verify that the SUT is in S5.</p> <p>25. Prompt the test operator to input the drive password via the VNC Viewer on the management console.</p> <p>NOTE: For SATA drives, the Master password should be used.</p> <p>26. Ensure the Intel® AMT user consent opt-in setting is enabled for KVM on the SUT.</p> <p>27. Open a KVM Redirection session with the SUT via Intel® AMT using the VNC Viewer on the management console.</p> <p>28. Set the Secure Erase boot option on the SUT via Intel® AMT.</p> <p>29. Perform a Remote Power-Up of the SUT via Intel® AMT. A user consent code is displayed on the SUT screen.</p> <p>30. Request the test operator to enter the user consent code into the VNC Viewer on the management console.</p> <p>31. Wait for the SUT to return to S0/MeOn. At this point, the BIOS should receive the Secure Erase boot option and begin drive erasure, but stop at a drive authentication prompt.</p> <p>32. Close the KVM Redirection session with the SUT via Intel® AMT.</p> <p>33. Poll the system for S5 for 10 minutes (maximum wait) for drive erasure completion. The test operator is able to configure the polling duration to control the maximum duration for drives that take longer to complete erasure.</p> <p>34. Get the Secure Erase boot option setting on the SUT via Intel® AMT and log it.</p> <p>35. Clear the Secure Erase boot option on the SUT via Intel® AMT (safety precaution).</p> <p>36. Verify that the BIOS last boot status reports success via Intel® AMT.</p> <p>37. Verify that the value of Secure Erase boot option setting retrieved at step 33 was cleared by the BIOS.</p>
Procedure: (continued)	<p>38. Set the SUT to G3 via Intel® APS.</p> <p>39. Verify that the SUT is in G3.</p> <p>40. Request the test operator to repeat the test for each remaining representative type of Remote Secure Erase Drive supported by the SUT. Otherwise, return the System Validation Drive to the SUT.</p> <p>If there was a failure during the test, consider running AMT_080 to safely clear the Secure Erase boot option before returning the System Validation Drive to the SUT.</p>
Pass Criteria:	This test passes if each of the representative sample types of Remote Secure Erase Drive supported by the SUT can each be erased remotely using the Secure Erase boot option with drive authentication via KVM (also under User Consent control), and the BIOS successfully clears the boot options at the end of each operation.
References:	For details on the Secure Erase boot option, refer the <i>Intel® ME BIOS Specification</i> .

11.11.6 Remote Secure Erase with Drive Authentication via Direct Password Input

ID:	AMT_084			
Title:	Remote Secure Erase with Drive Authentication via Direct Password Input			
Requirement:	Mandatory - exempt for systems which: <ul style="list-style-type: none"> • Do not support the Secure Erase boot option, or • Support only NVMe* configurations not requiring drive authentication 			
System:	Form Factor <input checked="" type="checkbox"/> Desktop <input checked="" type="checkbox"/> Workstation <input checked="" type="checkbox"/> Mobile	System Power Model <input checked="" type="checkbox"/> Standard <input checked="" type="checkbox"/> Modern Standby or InstantGo*	Intel® AMT Network Interface <input type="checkbox"/> LAN <input checked="" type="checkbox"/> Either Used <input type="checkbox"/> WLAN <input type="checkbox"/> Not Used	LAN Type <input checked="" type="checkbox"/> Integrated LAN <input type="checkbox"/> Discrete LAN <input type="checkbox"/> TBT Dock LAN
Method:	Automated by Intel® PETS with test operator interaction			



ID:	AMT_084
Description:	This test attempts to initiate the Remote Secure Erase boot option and verify that the BIOS has completed execution of the erase operation on a drive which requires authentication via direct password input from the management console.
Objective:	Verify that the BIOS properly advertises and implements the Secure Erase boot option for drives which require authentication via direct password input from the management console. This test should be run once per each drive type supported on the SUT (which have been prepared via one sample each in the set of Remote Secure Erase Drives described in the beginning of this section).
Setup:	The initial state of the SUT should be either G3 or S5 with the Remote Secure Erase Drive attached after executing AMT_080. Intel® AMT should be provisioned via manual mode with Power Package 2 (Intel® ME on in S0, wake in Sx/AC) and Intel® AMT WLAN link policy on the SUT to Link Policy 3 (Enabled in S0, Sx/AC), when only the WLAN network interface is available.
Procedure:	<ol style="list-style-type: none"> Prompt the test operator exit this test and run AMT_080 with the target Remote Secure Erase Drive if they have not done so already. Request the test operator to perform the following steps: Steps 1 through 4, if the BIOS settings have NOT already been confirmed. <ol style="list-style-type: none"> Boot the SUT to the BIOS menu. Verify device boot order to ensure BIOS' Remote Secure Erase Drive detection. Ensure the drive password(s) have been set. Save any BIOS settings changes. --- Shutdown the SUT to S5. <p>NOTE: It may be necessary to enter a drive password during these steps.</p> <ol style="list-style-type: none"> Verify that the SUT is in S5.
Procedure: (continued)	<ol style="list-style-type: none"> Prompt the test operator to acknowledge that operations past this point may ERASE or otherwise RENDER LOST the FULL CONTENTS of the system drive. The test operator may cancel the test at this time via the prompt or via Intel® PETS test controls. Check that the SUT supports booting to Secure Erase by querying the Intel® AMT and checking the boot capabilities. <ol style="list-style-type: none"> If supported, continue to the next step. If not supported, end the test and request the test operator to confirm the BIOS support of 'Secure Erase' OEMCapabilities3 setting provided to the Intel® ME via the SMBIOS Type 130 table. Cancel any existing Intel® AMT user consent session which may be active on the SUT. Ensure the Intel® AMT user consent opt-in setting is disabled on the SUT. Prompt the test operator to input the drive password via Intel® PETS on the management console. <p>NOTE: For SATA drives, the Master password should be used.</p> <ol style="list-style-type: none"> Set the Secure Erase boot option and the drive password on the SUT via Intel® AMT. Perform a Remote Power-Up of the SUT via Intel® AMT. Wait for the SUT to return to S0/MeOn. At this point, the BIOS should receive the Secure Erase boot option and begin drive erasure using the drive password which was provided through Intel® PETS from the management console. Poll the system for S5 for 10 minutes (maximum wait) for drive erasure completion. The test operator is able to configure the polling duration to control the maximum duration for drives that take longer to complete erasure. Get the Secure Erase boot option setting on the SUT via Intel® AMT and log it. Clear the Secure Erase boot option on the SUT via Intel® AMT (safety precaution). Verify that the BIOS last boot status reports success via Intel® AMT. Verify that the value of Secure Erase boot option setting retrieved at step 12 was cleared by the BIOS.
Procedure: (continued)	<ol style="list-style-type: none"> Set the SUT to G3 via Intel® APS. Verify that the SUT is in G3. Request the test operator to repeat the test for each remaining representative type of Remote Secure Erase Drive supported by the SUT. Otherwise, return the System Validation Drive to the SUT. <p>If there was a failure during the test, consider running AMT_080 to safely clear the Secure Erase boot option before returning the System Validation Drive to the SUT.</p>
Pass Criteria:	This test passes if each of the representative sample types of Remote Secure Erase Drive supported by the SUT can each be erased remotely using the Secure Erase boot option with drive authentication via direct password input from the management console, and the BIOS successfully clears the boot options at the end of each operation.
References:	For details on the Secure Erase boot option, refer the <i>Intel® ME BIOS Specification</i> .



11.11.7 Remote Secure Erase with Drive Authentication Failure via SOL Redirection

ID:	AMT_085			
Title:	Remote Secure Erase with Drive Authentication Failure via Serial-Over-LAN (SOL) Redirection			
Requirement:	Mandatory - exempt for systems which: <ul style="list-style-type: none"> Do not support the Secure Erase boot option, or Support only NVMe* configurations not requiring drive authentication 			
System:	Form Factor <input checked="" type="checkbox"/> Desktop <input checked="" type="checkbox"/> Workstation <input checked="" type="checkbox"/> Mobile	System Power Model <input checked="" type="checkbox"/> Standard <input checked="" type="checkbox"/> Modern Standby or InstantGo*	Intel® AMT Network Interface <input type="checkbox"/> LAN <input checked="" type="checkbox"/> Either Used <input type="checkbox"/> WLAN <input type="checkbox"/> Not Used	LAN Type <input checked="" type="checkbox"/> Integrated LAN <input type="checkbox"/> Discrete LAN <input type="checkbox"/> TBT Dock LAN
Method:	Automated by Intel® PETS with test operator interaction			
Description:	This test attempts to initiate the Remote Secure Erase boot option and verify that the BIOS has implemented proper error handling of the erase operation on a drive which requires authentication via Serial-Over-LAN (SOL).			
Objective:	<p>Verify that the BIOS properly advertises and implements error handling with the Secure Erase boot option for drives which require authentication via Serial-Over-LAN (SOL) but were not authenticated during the erasure process.</p> <p>This test should be run once per each drive type supported on the SUT (which have been prepared via one sample each in the set of Remote Secure Erase Drives described in the beginning of this section).</p>			
Setup:	<p>The initial state of the SUT should be either G3 or S5 with the Remote Secure Erase Drive attached after executing AMT_080. Intel® AMT should be provisioned via manual mode with Power Package 2 (Intel® ME on in S0, wake in Sx/AC) and Intel® AMT WLAN link policy on the SUT to Link Policy 3 (Enabled in S0, Sx/AC), when only the WLAN network interface is available.</p> <p>Before running this test, ensure that SOL is enabled in the Intel® MEBX.</p> <p>The default number of rows shown in the Putty terminal window may differ from the number of rows displayed by the BIOS. When this occurs, the Putty terminal display incur line wrapping problems. To avoid this problem, change the settings of the Putty application to align with the BIOS via the following steps:</p> <ol style="list-style-type: none"> Open the ".\Intel(R) Platform Enablement Test Suite\Plugins\Me\Redirection\bin\" directory. Start putty.exe, and in the Category section: <ol style="list-style-type: none"> Select Window, and change the Rows value to the required number of rows. Select Session, then select <i>Default Settings</i>, and finally click the Save button. Close the Putty Configuration window. To confirm, start putty.exe again, and make sure Row number is set to the new value. 			
Procedure:	<ol style="list-style-type: none"> Prompt the test operator exit this test and run AMT_080 with the target Remote Secure Erase Drive if they have not done so already. Request the test operator to perform the following steps: Steps 1 through 4, if the BIOS settings have NOT already been confirmed. <ol style="list-style-type: none"> Boot the SUT to the BIOS menu. Verify device boot order to ensure BIOS' Remote Secure Erase Drive detection. Ensure the drive password(s) have been set. Save any BIOS settings changes. <p>---</p> <ol style="list-style-type: none"> Shutdown the SUT to S5. <p>NOTE: It may be necessary to enter a drive password during these steps.</p> <ol style="list-style-type: none"> Verify that the SUT is in S5. 			



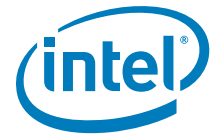
ID:	AMT_085
Procedure: (continued)	<p>4. Prompt the test operator to acknowledge that operations past this point may ERASE or otherwise RENDER LOST the FULL CONTENTS of the system drive. The test operator may cancel the test at this time via the prompt or via Intel® PETS test controls.</p> <p>5. Check that the SUT supports booting to Secure Erase by querying the Intel® AMT and checking the boot capabilities.</p> <ol style="list-style-type: none"> If supported, continue to the next step. If not supported, end the test and request the test operator to confirm the BIOS support of 'Secure Erase' OEMCapabilities3 setting provided to the Intel® ME via the SMBIOS Type 130 table. <p>6. Ensure the TCP maximum data retransmission setting defined in the SUT profile is applied to both a) the management console, and b) the SUT via Intel® AMT, if the WLAN network interface is used.</p> <p>If the configuration on the management console is not already aligned to the SUT profile setting, the network stack on the management console need to be reset; leading to potential network connectivity loss for other applications on the system.</p> <p>Before synchronizing the setting on the management console, provide a warning to the test operator, with the option to proceed or cancel, indicating the TCP maximum data retransmission network setting is about to be changed and that it may be necessary to re-establish network connectivity for any other applications running on the management console. If the test operator chooses to cancel, the test step is marked as failed.</p> <p>7. Ensure the Intel® AMT redirection ports are enabled on the SUT.</p> <p>8. Cancel any existing Intel® AMT user consent session which may be active on the SUT.</p> <p>9. Ensure the Intel® AMT user consent opt-in setting is disabled on the SUT.</p> <p>10. Prompt the test operator to input an invalid drive password via the Putty terminal program on the management console as many times as needed for authentication failure to occur.</p> <p>11. Use Intel® AMT to set the SUT boot options to use SOL Redirection and activate Secure Erase on the next boot.</p> <p>12. Open a SOL Redirection session with the SUT via Intel® AMT using the Putty terminal program on the management console.</p> <p>13. Perform a Remote Power-Up of the SUT via Intel® AMT.</p> <p>14. Wait for the SUT to return to S0/MeOn. At this point, the BIOS should receive the Secure Erase boot option and begin drive erasure, but stop at a drive authentication prompt.</p> <p>15. Close the SOL Redirection session with the SUT via Intel® AMT.</p> <p>16. Poll the system for S5 for 10 minutes (maximum wait) for drive erasure completion. The test operator is able to configure the polling duration to control the maximum duration for drives that take longer to complete erasure.</p> <p>17. Get the Secure Erase boot option setting on the SUT via Intel® AMT and log it.</p> <p>18. Clear the Secure Erase boot option on the SUT via Intel® AMT (safety precaution).</p> <p>19. Verify that the BIOS last boot status reports authentication failure via Intel® AMT.</p> <p>20. Verify that the value of Secure Erase boot option setting retrieved at step 15 was not cleared by the BIOS.</p>
Procedure: (continued)	<p>21. Set the SUT to G3 via Intel® APS.</p> <p>22. Verify that the SUT is in G3.</p> <p>23. Request the test operator to repeat the test for each remaining representative type of Remote Secure Erase Drive supported by the SUT. Otherwise, return the System Validation Drive to the SUT.</p> <p>If there was a failure during the test, consider running AMT_080 to safely clear the Secure Erase boot option before returning the System Validation Drive to the SUT.</p>
Pass Criteria:	This test passes if each of the representative sample types of Remote Secure Erase Drive supported by the SUT are not erased remotely using the Secure Erase boot option with drive authentication failure via SOL (also under User Consent control), and the BIOS does not clear the boot options at the end of each operation.
References:	For details on the Secure Erase boot option, refer the <i>Intel® ME BIOS Specification</i> .

11.11.8 Remote Secure Erase with Drive Authentication Failure via Direct Password Input

ID:	AMT_086
Title:	Remote Secure Erase with Drive Authentication Failure via Direct Password Input
Requirement:	<p>Mandatory - exempt for systems which:</p> <ul style="list-style-type: none"> Do not support the Secure Erase boot option, or Support only NVMe* configurations not requiring drive authentication



ID:	AMT_086			
System:	Form Factor <input checked="" type="checkbox"/> Desktop <input checked="" type="checkbox"/> Workstation <input checked="" type="checkbox"/> Mobile	System Power Model <input checked="" type="checkbox"/> Standard <input checked="" type="checkbox"/> Modern Standby or InstantGo*	Intel® AMT Network Interface <input type="checkbox"/> LAN <input checked="" type="checkbox"/> Either Used <input type="checkbox"/> WLAN <input type="checkbox"/> Not Used	LAN Type <input checked="" type="checkbox"/> Integrated LAN <input type="checkbox"/> Discrete LAN <input type="checkbox"/> TBT Dock LAN
Method:	Automated by Intel® PETS with test operator interaction			
Description:	This test attempts to initiate the Remote Secure Erase boot option and verify that the BIOS has implemented proper error handling of the erase operation on a drive which requires authentication via direct password input from the management console.			
Objective:	<p>Verify that the BIOS properly advertises and implements error handling with the Secure Erase boot option for drives which require authentication via direct password input from the management console but were not authenticated during the erasure process.</p> <p>This test should be run once per each drive type supported on the SUT (which have been prepared via one sample each in the set of Remote Secure Erase Drives described in the beginning of this section).</p>			
Setup:	The initial state of the SUT should be either G3 or S5 with the Remote Secure Erase Drive attached after executing AMT_080. Intel® AMT should be provisioned via manual mode with Power Package 2 (Intel® ME on in S0, wake in Sx/AC) and Intel® AMT WLAN link policy on the SUT to Link Policy 3 (Enabled in S0, Sx/AC), when only the WLAN network interface is available.			
Procedure:	<ol style="list-style-type: none"> Prompt the test operator exit this test and run AMT_080 with the target Remote Secure Erase Drive if they have not done so already. Request the test operator to perform the following steps: Steps 1 through 4, if the BIOS settings have NOT already been confirmed. <ol style="list-style-type: none"> Boot the SUT to the BIOS menu. Verify device boot order to ensure BIOS' Remote Secure Erase Drive detection. Ensure the drive password(s) have been set. Save any BIOS settings changes. Shutdown the SUT to S5. <p>NOTE: It may be necessary to enter a drive password during these steps.</p>			
Procedure: (continued)	<ol style="list-style-type: none"> Prompt the test operator to acknowledge that operations past this point may ERASE or otherwise RENDER LOST the FULL CONTENTS of the system drive. The test operator may cancel the test at this time via the prompt or via Intel® PETS test controls. Check that the SUT supports booting to Secure Erase by querying the Intel® AMT and checking the boot capabilities. <ol style="list-style-type: none"> If supported, continue to the next step. If not supported, end the test and request the test operator to confirm the BIOS support of 'Secure Erase' OEMCapabilities3 setting provided to the Intel® ME via the SMBIOS Type 130 table. Cancel any existing Intel® AMT user consent session which may be active on the SUT. Ensure the Intel® AMT user consent opt-in setting is disabled on the SUT. Prompt the test operator to input an invalid drive password via Intel® PETS on the management console. Set the Secure Erase boot option and the drive password on the SUT via Intel® AMT. Perform a Remote Power-Up of the SUT via Intel® AMT. Wait for the SUT to return to S0/MeOn. At this point, the BIOS should receive the Secure Erase boot option and begin drive erasure using the drive password which was provided through Intel® PETS from the management console. Poll the system for S5 for 10 minutes (maximum wait) for drive erasure completion. The test operator is able to configure the polling duration to control the maximum duration for drives that take longer to complete erasure. Get the Secure Erase boot option setting on the SUT via Intel® AMT and log it. Clear the Secure Erase boot option on the SUT via Intel® AMT (safety precaution). Verify that the BIOS last boot status reports authentication failure via Intel® AMT. Verify that the value of Secure Erase boot option setting retrieved at step 12 was not cleared by the BIOS. 			
Procedure: (continued)	<ol style="list-style-type: none"> Set the SUT to G3 via Intel® APS. Verify that the SUT is in G3. Request the test operator to repeat the test for each remaining representative type of Remote Secure Erase Drive supported by the SUT. Otherwise, return the System Validation Drive to the SUT. <p>If there was a failure during the test, consider running AMT_080 to safely clear the Secure Erase boot option before returning the System Validation Drive to the SUT.</p>			



ID:	AMT_086
Pass Criteria:	This test passes if each of the representative sample types of Remote Secure Erase Drive supported by the SUT are not erased remotely using the Secure Erase boot option with drive authentication failure via direct password input from the management console, and the BIOS does not clear the boot options at the end of each operation.
References:	For details on the Secure Erase boot option, refer the <i>Intel® ME BIOS Specification</i> .

§ §



12 Intel® CSME Power Management for Corporate Designs

This chapter covers system power flow transitions which involve the Intel® CSME firmware (and/or software). Test coverage for Intel® Active Management Technology (Intel® AMT), as an application within in the Intel® CSME firmware, related configurations and flows found in Corporate designs are also included herein.

12.1 System Power States

The following section describes power states that exist beyond the standard ACPI System Level Sx (S0, S3, S4, and S5) system S-states.

12.1.1 Deep S4/S5 Support

To minimize power consumption while in S4/S5, the PCH supports a lower power version of these power states known as Deep S4/S5. In these states, Deep S4 and Deep S5, the suspend well is powered off, while the Deep S4/S5 Well (DSW) remains powered. A limited set of wake events are supported by the logic located in the DSW. The Deep S4/S5 capability and the SUSPWRDNACK pin functionality are mutually exclusive.

Deep S4/S5 feature can be enabled/disabled by means of the Intel® FIT. Beyond this, a combination of conditions is required for entry into Deep S4/S5. All of the following must be met:

Intel® CSME must be in CM-Off AND either a OR b as defined below:

- a. ((DPS4_EN_AC AND S4) OR (DPS5_EN_AC AND S5)) (desktop only)
- b. ((AC_PRESENT = 0) AND ((DPS4_EN_DC AND S4) OR (DPS5_EN_DC AND S5)))

How to enable DSX in softstrap - **Deep SX Enable = true** in PCHSTRP10

Table 12-1. Supported Deep S4/S5 Policy Configurations

Configuration	DPS4_EN_DC	DPS4_EN_AC	DPS5_EN_DC	DPS5_EN_AC
Enabled in S5 when on Battery (ACPRESENT = 0)	0	0	1	0
Enabled in S5 (ACPRESENT not considered) (Desktop only)	0	0	1	1

**Table 12-1. Supported Deep S4/S5 Policy Configurations**

Configuration	DPS4_EN_DC	DPS4_EN_AC	DPS5_EN_DC	DPS5_EN_AC
Enabled in S4 and S5 when on Battery (ACPRESENT = 0)	1	0	1	0
Enabled in S4 and S5 (ACPRESENT not considered) (Desktop only)	1	1	1	1
Deep S4/S5 disabled	0	0	0	0

The PCH initiates DeepSx entry in Sx/CM-Off state upon sensing that all of the above conditions are satisfied. The PCH asserts SUSWARN# as notification that it is about to enter Deep S4/S5. Before the PCH proceeds and asserts SLP_SUS#, the PCH waits for SUSACK# to assert.

12.1.1.1 Exit from Deep S4/S5

While in Deep S4/S5, the PCH monitors and responds to a limited set of wake events (RTC Alarm, Power Button, and GPIO27). Upon sensing an enabled Deep S4/S5 wake event, the PCH brings up the Suspend well by de-asserting SLP_SUS#.

12.1.2 Intel® ME Power Gating

Intel® CSME firmware enters power gated state (CM0-PG) when the firmware is idle and system state is either S0 or S0ix. Intel® CSME firmware exits CM0-PG state to process power management events on the system and when host applications require Intel® CSME firmware services. When the Intel® CSME is in CM3 state, after Intel® AMT idle timeout, Intel® CSME enters CM3-PG state.

Intel® ME Power Gating feature is available only when the following conditions are satisfied:

- Intel® ME Power Gating feature supported when Intel® AMT is un-configured and the platform is in S0 state. In this case Intel® CSME may enter power gated state (CM0-PG) when the firmware reaches idle state.
- Intel® ME Power Gating feature supported when Intel® AMT is configured and the platform is in Sx state. In this case Intel® CSME is in CM3 state, after Intel® AMT idle timeout expiration, Intel® CSME enters CM3-PG state.
- Intel® LAN Ethernet cable must be disconnected.

Note: If the machine is configured to operate in Modern Standby or Microsoft* Windows* InstantGo, all S3 tests are not relevant, and should be replaced with the CM0-PG tests.

Note: For more details on Intel® ME Power Gating refer Intel® CSME 11.5 Firmware refer the Product Requirements Document (PRD).

12.1.3 Intel® RMT

Intel® Ready Mode Technology (Intel® RMT) is applicable for Desktop/All-in-one designs and is an alternate to Microsoft* Windows* Sleep (S3). Hence when Intel® RMT is enabled on desktop platforms, S3 test cases is not applicable. If Intel® RMT is disabled, S3 test cases are applicable, and in this configuration the SUT should move to S3 upon Host OS Sleep.



12.2 Test Environment and System Configuration

Each test in this chapter contains a section outlining the test configuration.

Unless where stated otherwise, Intel® AMT should be provisioned.

The Intel® AMT networking interface used by the test, if any, is documented in the test configuration section as well. 'LAN' and 'WLAN' indicate that the test is explicitly using the respective LAN and/or wireless LAN (WLAN) interface. Some tests may have a combination of targeted network configurations, example: WLAN-only and/or LAN+WLAN.

The test should be run on the SUT only in the case where a matching network configuration is described.

Note: Not all Workstation and Intel® AMT Server designs may have Intel® AMT wireless LAN interface support.

Other details about the configuration of the SUT are described on a per-test basis. Refer the test contents for details.

12.2.1 Test Parameters

Each test in this chapter contains a table describing the system configuration to which the test is applicable. Below are some example test parameters blocks:

System Power Source		AC+DC or AC-only
Power States	Initial	S0/MeOn (CM0, CM0-PG)
	Final	S0/MeOn (CM0, CM0-PG)
	Trigger	Remote Power Cycle
Intel® AMT	Power Package	PP2 (Intel® ME on in S0, wake in Sx/AC)
	WLAN Link Policy	LP3 (Enabled in S0, Sx/AC) where available

Example 1: Two-state with single trigger.

System Power Source		AC+DC or AC-only
Power States	Initial	S5/MeOn (CM3)
	Middle	G3/MeOff (CM-Off)
	Final	S5/MeOn (CM3)
	Trigger	Power loss → Power attach
Intel® AMT	Power Package	PP2 (Intel® ME on in S0, wake in Sx/AC)
	WLAN Link Policy	LP3 (Enabled in S0, Sx/AC) where available

Example 2: Three-state with double trigger

System Power Source: Describes the initial power source configuration of the system. Can be one of 'AC-only', 'DC-only', 'AC+DC', 'AC+DC,AC-only' (AC+DC or AC-only). The system may transition to different power source configurations during the test.

Power States: Describes the 'Initial', 'Middle' (where applicable), and 'Final' power states of the SUT. The description is provided in terms of basic ACPI Sx states (S0, S3, S4, S5, G3) as well as Intel® CSME availability ('MeOn' or 'MeOff'). Exact detail of



system power states, including Deep Sx and/or Intel® CSME power gating availability, is provided in each test. Included is also the 'Trigger' used to initiate the power flow transition. Many tests are limited one trigger, but some tests have two.

Intel® AMT: Describes the 'Power Package' and 'WLAN Link Policy' (where available and applicable) that apply to the test. The Power Package controls when manageability is available on the SUT and what power states the SUT and particularly the Intel® CSME may transition to and from. The WLAN Link Policy describes, relative to Wireless LAN support, when manageability is available via Intel® AMT Wireless Networking support.

12.2.2 Tools for Testing

The following tools, as provided by Intel, may be used to execute automated tests listed herein:

- Intel® PETS: The latest version of the tool from the Intel® CSME Compliance and Debug kit release. Refer the Intel® PETS User Guide for exact instructions on how to load and setup the Intel® PETS software.
- Intel® Automated Power Switch (Intel® APS): The SUT should be connected to an Intel® APS 3 unit. In case an Intel® APS 3 is not available, select the Manual configuration in the Intel® PETS SUT profile configuration menu.
- Intel® PETS Local Agent: The local agent must be installed on the SUT.

12.2.3 Test Environment Setup

The SUT is to be configured with Intel® AMT set in manual provisioning mode with static IP address or DHCP. The management console may be a laptop or a desktop with a version of Microsoft® Windows® supported by Intel® PETS, and the SUT should have a version of Microsoft® Windows® supported by Intel® PETS as well. The test network is comprised of a hub/switch and network cables. The SUT should have only one HDD.

When completing tests within this chapter, especially those which send the system to a specific S-state (S3, S4, S5, Deep Sx, and so forth), it is important to ensure that the network wake events are properly configured for each applicable device (LAN and/or WLAN).

If not properly configured, the system may wake from a given S-state unexpectedly during test execution as a result of various network traffic within the test environment, and cause the test to result in a *false failure*.

The following Host OS LAN/WLAN driver settings allow the network device to process specific network frames **without** waking the system where supported.

- ARP (Address Resolution Protocol) offload should be **enabled**
- NS (Neighbor Solicitation) offload should be **enabled**

The following Host OS LAN/WLAN driver settings allow the network device to wake the system, where supported, when specific network frames are received.

- Wake on Magic Packet should be **disabled**
- Wake on Pattern Match should be **disabled**
- Wake on Magic Packet from power off state should be **disabled**

Note:

The wording used for the Host OS driver settings above may vary, and in some cases may not be available depending on driver support or system configuration.



Beyond the guidance in this section, refer individual test setup information for details on specifically when to enable relevant wake functionality in the network device, as applicable to the test. In all other cases, the above settings should be applied by default.

The following additional checkpoints are recommended before Intel® CSME firmware Power Management testing:

- Install all platform drivers (Chipset, Graphics, LAN, WLAN, Intel® MEI, LMS_SOL)
- Client platform OS can be Microsoft* Windows* 7, Windows* 8.1, or Windows* 10,
- For wired LAN network use a hub/switch and network cables.
- Wireless setup:
 - Wireless card should be installed.
 - Setup an active wireless profile.
- LAN and WLAN interfaces should be setup on different subnets
- For Global reset tests to pass (ME_PM_18), the SUT should be in manufacturing mode

Note:

Intel® CSME FWSTS values are updated except for test cases which have Power Gating (PG) validation and Deep Sx enabled.

Following test step has been added to Power Flows which ends at S0 state resuming back from S4 Hibernation. This helps to ensure System resumed from S4 state only and no other Sx state.

Verify that Windows* booted from hibernate i.e. value should be 0x02. "Run the following power shell command" Get-WinEvent-ProviderName Microsoft-Windows-Kernel-boot-MaxEvents 10|where-Object {\$_.message -like "The Boot type*"}

12.2.4 Test Step Execution and Verification

The tests described in this chapter contain test steps which are executed by Intel® PETS. While Intel® PETS brings a certain level of convenience and speed to the testing process, there are times where manual verification of steps is critical toward issue triage and debug.

The following is a list of non-trivial test steps and a description of how they may be manually executed. The list assumes that the test operator has access to information available in the PCH External Design Specification (EDS), and the Intel® AMT SDK.

1. Set the active power package on the SUT to **Power Package 1** (Intel® ME on in S0).
 - Log into the WebUI via of the SUT at http://<ip_address>:16992/ to view and manually change the Power Policy therein.



- To configure the Intel® AMT power package to PP1, run the following command from the Management Console:

Mobile

```
$> PowerPackage.exe -applyguid djmXEQtWUEOIcJgS85G1YA== -host <ip_address> -user <user> -pass <password>
```

Desktop

```
$> PowerPackage.exe -applyguid IE+DEvsQT9yWjh4jKwyQZQ== -host <ip_address> -user <user> -pass <password>
```

Upon successful execution, the Intel® AMT firmware active power package is returned. The PowerPackage application is located in the Intel® AMT SDK.

- Set the active power package on the SUT to **Power Package 2** (Intel® ME on in S0, wake in Sx/AC).
 - Log into the WebUI via of the SUT at http://<ip_address>:16992/ to view and manually change the Power Policy therein.
 - To configure the Intel® AMT power package to PP2, run the following command from the Management Console:

Mobile

```
$> PowerPackage.exe -applyguid MIAN7gnAeEOvKHhootu+Og== -host <ip_address> -user <user> -pass <password>
```

Desktop

```
$> PowerPackage.exe -applyguid cyJzRiPcQy+pihPTeYLYVQ== -host <ip_address> -user <user> -pass <password>
```

Upon successful execution, the Intel® AMT firmware active power package is returned. The PowerPackage application is located in the Intel® AMT SDK.
- Set the Intel® AMT WLAN link policy on the SUT to Link Policy [1,2,3].
 - Log into the WebUI via of the SUT at http://<ip_address>:16992/ and manually change the Link Policy via the Wireless Settings screen therein.
- Send three magic packets, at **2 second** intervals, by means of the [active,LAN] network interface.
 - Sending magic packets is supported by various tools and utilities available on the internet.
- Ensure the Intel® AMT idle timeout on the SUT is set to **1 minute**.
 - The following command may be used set the Intel® AMT idle timeout on the SUT from the Management Console:


```
$> PowerPackage.exe -setidletimeout 1 -host <ip_address> -user <user> -pass <password>
```

Upon successful execution, the Intel® AMT idle timeout is set. The getidletimeout command line option may be used to confirm the setting. The PowerPackage application is located in the Intel® AMT SDK.
- Ensure that CF9h Global Reset (CF9GR) is [set,cleared].
 - Read 32-bits from PCI configuration space B0:D31:F2 (Bus:Device:Function) at offset ACh and confirm that CF9 Global Reset (CF9GR) bit 20 is set to 1b (set) or 0b (clear). Information describing how to access this value may be found in the PCH EDS.

The following is a list of commonly used test steps and a description of how they may be manually verified. The list assumes that the test operator has access to information available in the PCH External Design Specification (EDS), Platform Design Guide (PDG), PCH BIOS Specification, the Intel® AMT SDK, as well as power management related signals (as described by the Intel® APS header found in the PDG) on the SUT.



1. Confirm that the BIOS has **not set** the CF9 Lockdown.
 - Read 32-bits from PCI configuration space B0:D31:F2 (Bus:Device:Function) at offset ACh and confirm that CF9 Lockdown (CF9LOCK) bit 31 is set to **0b**. Information describing how to access this value may be found in the PCH EDS.
2. Confirm that Intel® RMT feature support is [enabled,disabled] on the SUT.
 - For information on Intel® RMT feature support, refer the Intel® RMT white paper 535877.
3. Verify that Intel® AMT on the SUT responds to version query via the [LAN,WLAN,active,any] network interface.
 - For a given network interface for which Intel® AMT should be responsive, the following command may be used to confirm connectivity from the Management Console:

```
$> GeneralInfo.exe -host <ip_address> -user <user> -pass <password> -CoreVersion
```

 Upon successful execution, the Intel® AMT firmware core version is returned. The GeneralInfo application is located in the Intel® AMT SDK.
4. Verify that the SUT is in S0.
 - Confirm that signals SLP_S3#, SLP_S4#, and SLP_S5# are all de-asserted (high) for at least **5 seconds**.
5. Verify that the SUT is in Sx[,Deep Sx]/Me[On/Off] (CMx[-PG]).
 - Confirm that signals and power rails are asserted (low)/de-asserted (high) or powered/off respectively for the associated SUT state for at least **5 seconds**:

State	SLP_S3#	SLP_S4#	SLP_S5#	SLP_A#	VccSUS3_3	VccDSW3_3
S0	1	1	1	N/A	Powered	Powered
S3	0	1	1	N/A	Powered	Powered
S4	0	0	1	N/A	Powered	Powered
S5	0	0	0	N/A	Powered	Powered
MeOn	N/A	N/A	N/A	1	Powered	Powered
MeOff	N/A	N/A	N/A	0	Powered	Powered
Deep S4	0	0	1	0	Off	Powered
Deep S5	0	0	0	0	Off	Powered
G3	0	0	0	0	Off	Off

Note: VccSUS3_3 is also referred to as VCCPRIM_3p3 in the PCH EDS and PDG. Similarly, VccDSW3_3 is also referred to as VCCDSW_3p3 as well. The labels VccSUS3_3 and VccDSW3_3 are listed in the table above to assist test operators identification of the corresponding signals (as silk-screened) on their Intel® APS adapter (refer the PDG for details).

- In S0, the CM0-PG and CM0 Intel® CSME 'MeOn' states appears the same in the table above. Follow the procedure below via the Host OS on the SUT to confirm if the Intel® CSME is Power Gated (CM0-PG):
 - i. Get the PWRMBASE (32-bits) by reading the PCI configuration space B0:D31:F2 (Bus:Device:Function) at offset 48h. Information describing how to access this value may be found in either the PCH EDS or the PCH BIOS Specification.
 - ii. Read 32-bits at PWRMBASE + 590h and verify that bits 31:24 equal F9h.
 - iii. Read 32-bits at PWRMBASE + 594h and verify that bits 7:0 equal FFh.



- In S3, S4, or S5, the CM3-PG and CM-Off Intel® CSME 'MeOff' states appears the same in the table above. The Intel® CSME may enter CM3-PG (supporting wake) upon Intel® AMT idle timeout when the Intel® AMT Power Policy configuration is set to PP2 (Intel® ME on in S0, wake in Sx/AC).

Caution:

When using Intel® PETS to verify the power state of the SUT, it is critical to ensure that the Advanced Power Settings configuration in the SUT profile is correctly set. Failure to set the correct policy configuration supported by the SUT may lead to false test results or incomplete evaluation. Refer the Intel® PETS User Guide for further details.

- Verify that the SUT is in G3/MeOff (CM-Off).
 - Confirm that signals SLP_S3#, SLP_S4#, SLP_S5#, and SLP_A# are asserted low. Additionally, VccSus3_3 (and VccDSW3_3 for systems supporting Deep Sx) should be powered off.
 - The signal and power rail state should remain stable for at least **5 seconds**. Furthermore, measurements should not be taken for at least **10 seconds** after state transition to allow full electric dissipation from the system.
- Verify that the Host OS on the SUT is available.
 - A connection test with the Intel® PETS Local Agent service on the SUT can be used to confirm that the Host OS is available remotely from the Management Console:

```
$> PsService.exe \\<ip_address> -u <user> -pass <password> query PeTSLocalAgent
```

 Upon successful execution, the Intel® PETS Local Agent status should be displayed. The PsService tools is available from Microsoft* Windows* Sysinternals website.
- Verify that the Intel® ME on the SUT is on.
 - Confirm that the SLP_A# signal is de-asserted (high) for at least **5 seconds**.
- Verify that the Intel® ME on the SUT is off.
 - Confirm that the SLP_A# signal is asserted (low) for at least **5 seconds**.
- Verify that the Intel® ME is configured in manufacturing mode.
 - The manufacturing mode status is available by querying the Intel® CSME firmware status bits via the MEInfo tool on the SUT. The following example shows tool usage in a UEFI shell:

```
$> MEInfo.efi -fwsts
```

 Upon successful execution, the Intel® CSME Manufacturing Mode status should read "Enabled". The MEInfo tool is available from Intel via the Intel® CSME firmware kit.
- Verify that a DC battery is connected to the SUT, and that it is charged.
 - The battery information on SUT can be queried via the Microsoft* Windows* Management Instrumentation Command (WMIC) tool.

```
$> WMIC PATH Win32_Battery Get EstimatedChargeRemaining
```
 - It is recommended that tests in this chapter be run on no less than **30%** battery charge. More information about the WMIC is available from Microsoft*, including how to connect remotely and perform queries via various command-line switches.



12.2.5 Setup Environment Tests

The following tests are defined as Setup Environment Test (SET) tests. These are intended to confirm basic test environment configuration and should be run before any other automated test described in this chapter.

Because Intel® AMT is provisioned in many of the tests in this chapter, it is strongly recommended to run the Setup Environment Tests for that technology as well before running any test in this chapter.

ID:	Check S3		
Title:	S0/CM0 to S3/CM3 to S0/CM0 via Host OS suspend cycle (AC-only/PP2)		
Requirement:	Optional	Non-Support	☑ Modern Standby and InstantGo* systems
Method:	Automated by Intel® PETS		
Objective:	This test checks the SUT power flow from S0/CM0 to S3/CM3 to S0/CM0 via Host OS suspend cycle with the parameters outlined below.		
Configuration:	Intel® AMT should be provisioned via manual mode.		
Parameters:	System Power Source		AC-only
	Power States	Initial	S0/MeOn (CM0, CM0-PG)
		Middle	S3/MeOn (CM3)
		Final	S0/MeOn (CM0, CM0-PG)
		Trigger	Host OS suspend ➡ Power Button press
	Intel® AMT	Power Package	PP2 (Intel® ME on in S0, wake in Sx/AC)
WLAN Link Policy		[Not applicable.]	
Setup:	<div>1. Set the SUT power source to AC-only.</div> <div>2. Bring the SUT to the base state of S0/MeOn (CM0,CM0-PG), and confirm that the Host OS is available.</div> <div>3. Set the active power package on the SUT to Power Package 2 (Intel® ME on in S0, wake in Sx/AC).</div> <div>4. Ensure that the Host OS network device drivers are configured to not wake the SUT. This includes enabling ARP and/or NS Offload features where available to help prevent unexpected host wake events. Most especially, ensure that the Host OS Wireless Wake on LAN driver setting on the SUT is disabled, if the WLAN network interface is available</div> <div>5. Ensure that Intel® RMT is disabled, if running on a Desktop or All-in-One (AIO) SUT with feature support.</div>		
Procedure:	<div>1. Suspend the SUT via the Host OS.</div> <div>2. Verify that the SUT is in S3/MeOn (CM3).</div> <div>3. Briefly press the Power Button on the SUT.</div> <div>4. Verify that the SUT is in S0/MeOn (CM0,CM0-PG).</div>		
Pass Criteria:	The test passes if the SUT moves to S3 and then to S0, and the Intel® CSME is in MeOn (CM0, CM0-PG).		

ID:	Check S4	
Title:	S0/CM0 to S4/CM3 to S0/CM0 via Host OS hibernate cycle (AC-only/PP2)	
Requirement:	Optional	
Method:	Automated by Intel® PETS	
Objective:	This test checks the SUT power flow from S0/CM0 to S4/CM3 to S0/CM0 via Host OS hibernate cycle with the parameters outlined below.	
Configuration:	Intel® AMT should be provisioned via manual mode.	



ID:	Check S4	
Parameters:	System Power Source	AC-only
	Power States	Initial S0/MeOn (CM0, CM0-PG)
		Middle S4,S5/MeOn (CM3)
		Final S0/MeOn (CM0, CM0-PG)
		Trigger Host OS hibernate ➡ Power Button press
	Intel® AMT	Power Package PP2 (Intel® ME on in S0, wake in Sx/AC)
		WLAN Link Policy [Not applicable.]
Setup:	<ol style="list-style-type: none"> 1. Set the SUT power source to AC-only. 2. Bring the SUT to the base state of S0/MeOn (CM0,CM0-PG), and confirm that the Host OS is available. 3. Set the active power package on the SUT to Power Package 2 (Intel® ME on in S0, wake in Sx/AC). 4. Ensure that the Host OS network device drivers are configured to not wake the SUT. This includes enabling ARP and/or NS Offload features where available to help prevent unexpected host wake events. 	
Procedure:	<ol style="list-style-type: none"> 1. Hibernate the SUT via the Host OS. 2. Verify that the SUT is in S4, S5/MeOn (CM3). 3. Briefly press the Power Button on the SUT. 4. Verify that the SUT is in S0/MeOn (CM0,CM0-PG). 	
Pass Criteria:	The test passes if the SUT moves to S4 and then to S0, and the Intel® CSME is in MeOn (CM0, CM0-PG).	

ID:	Check S5	
Title:	S0/CM0 to S5/CM3 to S0/CM0 via Host OS shutdown cycle (AC-only/PP2)	
Requirement:	Optional	
Method:	Automated by Intel® PETS	
Objective:	This test checks the SUT power flow from S0/CM0 to S5/CM3 to S0/CM0 via Host OS shutdown cycle with the parameters outlined below.	
Configuration:	Intel® AMT should be provisioned via manual mode.	
Parameters:	System Power Source	AC-only
	Power States	Initial S0/MeOn (CM0, CM0-PG)
		Middle S5/MeOn (CM3)
		Final S0/MeOn (CM0, CM0-PG)
		Trigger Host OS shutdown ➡ Power Button press
	Intel® AMT	Power Package PP2 (Intel® ME on in S0, wake in Sx/AC)
		WLAN Link Policy [Not applicable.]
Setup:	<ol style="list-style-type: none"> 1. Set the SUT power source to AC-only. 2. Bring the SUT to the base state of S0/MeOn (CM0,CM0-PG), and confirm that the Host OS is available. 3. Set the active power package on the SUT to Power Package 2 (Intel® ME on in S0, wake in Sx/AC). 4. Ensure that the Host OS network device drivers are configured to not wake the SUT. This includes enabling ARP and/or NS Offload features where available to help prevent unexpected host wake events. 	
Procedure:	<ol style="list-style-type: none"> 1. Shutdown the SUT via the Host OS. 2. Verify that the SUT is in S5/MeOn (CM3). 3. Briefly press the Power Button on the SUT. 4. Verify that the SUT is in S0/MeOn (CM0,CM0-PG). 	
Pass Criteria:	The test passes if the SUT moves to S5 and then to S0, and the Intel® CSME is in MeOn (CM0, CM0-PG).	

ID:	Check Deep S4	
Title:	S0/CM0 to S4/CM-Off to S0/CM0 via Host OS hibernate cycle (AC-only/PP1)	



ID:	Check Deep S4		
Requirement:	Optional	Non-Support	<input checked="" type="checkbox"/> Systems not supporting Deep S4
Method:	Automated by Intel® PETS		
Objective:	This test checks the SUT power flow from S0/CM0 to S4/CM-Off to S0/CM0 via Host OS hibernate cycle with the parameters outlined below.		
Configuration:	Intel® AMT should be provisioned via manual mode. If Deep S4 is supported on the SUT, confirm the following: <ul style="list-style-type: none">the SUT and/or BIOS are properly configured to permit Deep S4 entry.the correct Deep Sx policy is applied to the SUT profile in Intel® PETS.		
Parameters:	System Power Source		AC-only
	Power States	Initial	S0/MeOn (CM0, CM0-PG)
		Middle	Deep S4/MeOff (CM-Off)
		Final	S0/MeOn (CM0, CM0-PG)
		Trigger	Host OS hibernate ➡ Power Button press
	Intel® AMT	Power Package	PP1 (Intel® ME on in S0)
		WLAN Link Policy	[Not applicable.]
Setup:	<ol style="list-style-type: none">Set the SUT power source to AC-only.Bring the SUT to the base state of S0/MeOn (CM0,CM0-PG), and confirm that the Host OS is available.Set the active power package on the SUT to Power Package 1 (Intel® ME on in S0).Ensure that the Host OS network device drivers are configured to not wake the SUT. This includes enabling ARP and/or NS Offload features where available to help prevent unexpected host wake events.		
Procedure:	<ol style="list-style-type: none">Request the test operator to confirm the SUT is properly configured to enter Deep S4 upon Host OS hibernate.Hibernate the SUT via the Host OS.Verify that the SUT is in Deep S4/MeOff (CM-Off).Briefly press the Power Button on the SUT.Verify that the SUT is in S0/MeOn (CM0,CM0-PG).		
Pass Criteria:	The test passes if the SUT moves to Deep S4 and then to S0, and the Intel® CSME is in MeOn (CM0, CM0-PG).		

ID:	Check Deep S5		
Title:	S0/CM0 to S5/CM-Off to S0/CM0 via Host OS shutdown cycle (AC-only/PP1)		
Requirement:	Optional	Non-Support	☑ Systems not supporting Deep S5
Method:	Automated by Intel® PETS		
Objective:	This test checks the SUT power flow from S0/CM0 to S5/CM-Off to S0/CM0 via Host OS shutdown cycle with the parameters outlined below.		
Configuration:	Intel® AMT should be provisioned via manual mode. If Deep S5 is supported on the SUT, confirm the following: <ul style="list-style-type: none">the SUT and/or BIOS are properly configured to permit Deep S5 entry.the correct Deep Sx policy is applied to the SUT profile in Intel® PETS.		
Parameters:	System Power Source		AC-only
	Power States	Initial	S0/MeOn (CM0, CM0-PG)
		Middle	Deep S5/MeOff (CM-Off)
		Final	S0/MeOn (CM0, CM0-PG)
		Trigger	Host OS shutdown ➡ Power Button press
	Intel® AMT	Power Package	PP1 (Intel® ME on in S0)
		WLAN Link Policy	[Not applicable.]



ID:	Check Deep S5
Setup:	<ol style="list-style-type: none"> 1. Set the SUT power source to AC-only. 2. Bring the SUT to the base state of S0/MeOn (CM0,CM0-PG), and confirm that the Host OS is available. 3. Set the active power package on the SUT to Power Package 1 (Intel® ME on in S0). 4. Ensure that the Host OS network device drivers are configured to not wake the SUT. This includes enabling ARP and/or NS Offload features where available to help prevent unexpected host wake events.
Procedure:	<ol style="list-style-type: none"> 1. Request the test operator to confirm the SUT is properly configured to enter Deep S5 upon Host OS shutdown. 2. Shutdown the SUT via the Host OS. 3. Verify that the SUT is in Deep S5/MeOff (CM-Off). 4. Briefly press the Power Button on the SUT. 5. Verify that the SUT is in S0/MeOn (CM0,CM0-PG).
Pass Criteria:	The test passes if the SUT moves to Deep S5 and then to S0, and the Intel® CSME is in MeOn (CM0, CM0-PG).

ID:	Check Intel® CSME		
Title:	S0/CM0 to S5/CM-Off to S0/CM0 via Host OS shutdown cycle (AC-only/PP1)		
Requirement:	Optional		
Method:	Automated by Intel® PETS		
Objective:	This test checks the SUT power flow from S0/CM0 to S5/CM3 to S0/CM0 via Host OS shutdown cycle with the parameters outlined below.		
Configuration:	Intel® AMT should be provisioned via manual mode. If Deep S5 and/or G3 are supported on the SUT, please confirm the following: <ul style="list-style-type: none">the SUT and/or BIOS are properly configured to permit Deep S5 or G3 entry.the correct Deep Sx policy is applied to the SUT profile in Intel® PETS.		
Parameters:	System Power Source		AC-only
	Power States	Initial	S0/MeOn (CM0, CM0-PG)
		Middle	S5/MeOn (CM3)
		Final	S0/MeOn (CM0, CM0-PG)
		Trigger	Host OS shutdown ➡ Power Button press
	Intel® AMT	Power Package	PP1 (Intel® ME on in S0)
		WLAN Link Policy	[Not applicable.]
Setup:	<ol style="list-style-type: none">Set the SUT power source to AC-only.Bring the SUT to the base state of S0/MeOn (CM0,CM0-PG), and confirm that the Host OS is available.Set the active power package on the SUT to Power Package 1 (Intel® ME on in S0).Ensure that the Host OS network device drivers are configured to not wake the SUT. This includes enabling ARP and/or NS Offload features where available to help prevent unexpected host wake events.		
Procedure:	<ol style="list-style-type: none">Shutdown the SUT via the Host OS.Verify that the SUT is in S5, Deep S5, G3/MeOff (CM-Off).Briefly press the Power Button on the SUT.Verify that the SUT is in S0/MeOn (CM0,CM0-PG).		
Pass Criteria:	The test passes if the SUT moves to S5 (or Deep S5 or G3) and then to S0, and the Intel® CSME is in MeOff (CM-Off) when the SUT is in S5 (or Deep S5 or G3).		

ID:	Check DC Power
Title:	Check DC power connectivity to the SUT (AC+DC)
Requirement:	Optional Non-Support <input checked="" type="checkbox"/> Non-Mobile (AC-only) systems
Method:	Automated by Intel® PETS
Objective:	This test checks the SUT power flow from AC+DC to DC-only with the parameters outlined below.



ID:	Check DC Power	
Configuration:	Intel® AMT should be provisioned via manual mode.	
Parameters:	System Power Source	AC+DC
	Power States	Initial S0/MeOn (CM0, CM0-PG)
		Final S0/MeOn (CM0, CM0-PG)
		Trigger AC-detach
	Intel® AMT	Power Package [Not applicable.]
		WLAN Link Policy [Not applicable.]
Setup:	<ol style="list-style-type: none"> Set the SUT power source to AC+DC. Bring the SUT to the base state of S0/MeOn (CM0,CM0-PG), and confirm that the Host OS is available. 	
Procedure:	<ol style="list-style-type: none"> Set the SUT power source to DC-only. Wait 5 seconds before proceeding to allow the test environment to stabilize. Verify that the SUT is operating on DC-only power. 	
Pass Criteria:	The test passes if the SUT moves from AC+DC power to DC-only power.	

ID:	Check AC Power	
Title:	Check AC power connectivity to the SUT (AC+DC, AC-only)	
Requirement:	Optional	
Method:	Automated by Intel® PETS	
Objective:	This test checks the SUT power flow from AC+DC to AC-only with the parameters outlined below.	
Configuration:	Intel® AMT should be provisioned via manual mode.	
Parameters:	System Power Source	AC+DC or AC-only
	Power States	Initial S0/MeOn (CM0, CM0-PG)
		Final S0/MeOn (CM0, CM0-PG)
		Trigger DC-detach where available
	Intel® AMT	Power Package [Not applicable.]
		WLAN Link Policy [Not applicable.]
Setup:	<ol style="list-style-type: none"> Set the SUT power source to AC+DC where supported; otherwise AC-only. Bring the SUT to the base state of S0/MeOn (CM0,CM0-PG), and confirm that the Host OS is available. 	
Procedure:	<ol style="list-style-type: none"> Set the SUT power source to AC-only. Wait 5 seconds before proceeding to allow the test environment to stabilize. Verify that the SUT is operating on AC-only power. 	
Pass Criteria:	The test passes if the SUT moves from AC+DC power to AC-only power.	

ID:	Check G3 State	
Title:	S0/CM0 to G3/CM-Off via Power loss (AC+DC, AC-only/PP1)	
Requirement:	Optional	
Method:	Automated by Intel® PETS	
Objective:	This test checks the SUT power flow from S0/CM0 to G3/CM-Off via Power loss with the parameters outlined below.	
Configuration:	<p>Intel® AMT should be provisioned via manual mode.</p> <p>If Deep S5 and/or G3 are supported on the SUT, please confirm the following:</p> <ul style="list-style-type: none"> the SUT and/or BIOS are properly configured to permit Deep S5 or G3 entry. the correct Deep Sx policy is applied to the SUT profile in Intel® PETS. 	



ID:	Check G3 State	
Parameters:	System Power Source	AC+DC or AC-only
	Power States	Initial S0/MeOn (CM0, CM0-PG)
		Final G3/MeOff (CM-Off)
		Trigger Power loss
	Intel® AMT	Power Package PP1 (Intel® ME on in S0)
		WLAN Link Policy [Not applicable.]
Setup:	<ol style="list-style-type: none"> 1. Set the SUT power source to AC+DC where supported; otherwise AC-only. 2. Bring the SUT to the base state of S0/MeOn (CM0,CM0-PG), and confirm that the Host OS is available. 3. Set the active power package on the SUT to Power Package 1 (Intel® ME on in S0). 4. Ensure that the Host OS network device drivers are configured to not wake the SUT. This includes enabling ARP and/or NS Offload features where available to help prevent unexpected host wake events. 	
Procedure:	<ol style="list-style-type: none"> 1. Shutdown the SUT via the Host OS. 2. Verify that the SUT is in S5, Deep S5, G3/MeOff (CM-Off). 3. Remove power from the SUT via AC-detach, and if necessary also via DC-detach. Wait for 10 seconds before continuing to allow full power drain from the SUT. 4. Verify that the SUT is in G3/MeOff (CM-Off). 	
Pass Criteria:	The test passes if the SUT moves to G3, and the Intel® CSME moves to MeOff (CM-Off).	

12.3 Test Coverage Summary

Test Requirements:

In general, all **applicable** tests are considered Mandatory in this section except for those specifically described as Optional or those which meet an Exemption. Refer the test Requirement section for details on test applicability.

Form Factor:

Mobile designs are most broadly covered by the tests in this chapter, Desktop, All-in-One, and Workstation designs are Exempted where classified as Non-Mobile (AC-only) systems. Refer the test Requirement section for Exemption details.

System Power Model:

Tests which involve S3 flows would not support Modern Standby or Microsoft* Windows* InstantGo. Refer the test Requirement section for Exemption details.

Network Configuration:

In general, all tests may be run on systems with any combination of LAN and/or WLAN network interface support. For tests that work with a subset of configurations, like LAN-only or LAN+WLAN, refer the test Configuration section for details.

Test ID	Test Case Title	Test Method
ME_PM_1	S0/CM0 to S3/CM-Off	Intel® PETS Package: Compliance_Power_G3-S5.xml
ME_PM_2	S0/CM0 to S3/CM-Off	Intel® PETS Package: Compliance_Power_G3-S5.xml Compliance_Power_Network_Wake.xml
ME_PM_3	S0/CM0 to S3/CM3	Intel® PETS Package: Compliance_Power_G3-S5.xml
ME_PM_4	S3/CM3 to S0/CM0	Intel® PETS Package: Compliance_Power_G3-S5.xml Compliance_Power_Network_Wake.xml
ME_PM_5	S3/CM3 to S3/CM-Off (without Intel® CSME Wake)	Intel® PETS Package: Compliance_Power_G3-S5.xml
ME_PM_6	S3/CM3 to S3/CM-Off (with Intel® ME Wake)	Intel® PETS Package: Compliance_Power_G3-S5.xml



Test ID	Test Case Title	Test Method
ME_PM_7	S3/CM-Off to S3/CM3	Intel® PETS Package: Compliance_Power_G3-S5.xml
ME_PM_8	S0/CM0 to S3/CM-Off	Intel® PETS Package: Compliance_Power_G3-S5.xml
ME_PM_9	G3 or S4-S5/CM-Off (Suspend Well Off) to S0/CM0	Intel® PETS Package: Compliance_Power_G3-S0.xml Compliance_Power_G3-S5.xml
ME_PM_10	S4/CM-Off (Suspend Well On) to S0/CM0	Intel® PETS Package: Compliance_Power_G3-S5.xml Compliance_Power_Network_Wake.xml
ME_PM_11	S0/CM0 to S4,S5/CM3	Intel® PETS Package: Compliance_Power_G3-S5.xml
ME_PM_12	S4-S5/CM3 to S0/CM0	Intel® PETS Package: Compliance_Power_G3-S5.xml
ME_PM_13	S4-S5/CM3 to S4-S5/CM-Off (without Intel® ME Wake)	Intel® PETS Package: Compliance_Power_G3-S5.xml
ME_PM_14	S4-S5/CM3 to S4-S5/CM-Off (with Intel® ME Wake)	Intel® PETS Package: Compliance_Power_G3-S5.xml
ME_PM_15	G3 or S4-S5/CM-Off (Suspend Well Off) to S4-S5/CM3	Intel® PETS Package: Compliance_Power_G3-S5.xml
ME_PM_16	S4-S5/CM-Off (Suspend Well On) to S4-S5/CM3	Intel® PETS Package: Compliance_Power_G3-S5.xml
ME_PM_17	Cold Reset	Intel® PETS Package: Compliance_Power_RST.xml
ME_PM_18	Global Reset	Intel® PETS Package: Compliance_Power_RST.xml
ME_PM_19	Straight-to-S5, Intel® CSME Power Policy is S0 Only	Intel® PETS Package: Compliance_Power_G3-S5.xml Compliance_Power_RST.xml
ME_PM_20	Straight-to-S5 via Power Button Override	Intel® PETS Package: Compliance_Power_G3-S5.xml Compliance_Power_RST.xml
ME_PM_21	S3/CM-Off (w/ Intel® ME Wake) to S3/CM-Off (w/o Intel® ME Wake)	Intel® PETS Package: Compliance_Power_G3-S5.xml
ME_PM_22	S3/CM3-PG (w/ Intel® ME Wake) to S3/CM-Off (w/o Intel® ME Wake)	Intel® PETS Package: Compliance_Power_G3-S5.xml
ME_PM_23	G3 or S4-S5/CM-Off (w/o Intel® ME Wake) to S4-S5/CM-Off (w/ Intel® ME Wake)	Intel® PETS Package: Compliance_Power_G3-S5.xml
ME_PM_24	S4-S5/CM-Off (w/ Intel® ME Wake) to S4-S5/CM-Off (w/o Intel® ME Wake)	Intel® PETS Package: Compliance_Power_G3-S5.xml
ME_PM_25	S4-S5/CM-Off (Suspend Well Off) to S4-S5/CM-Off (w/ Host WoL) to S0/CM0 via Host WoL/WoWLAN	Intel® PETS Package: Compliance_Power_Network_Wake.xml
ME_PM_26	Warm Reset	Intel® PETS Package: Compliance_Power_G3-S5.xml Compliance_Power_RST.xml
ME_PM_27	S0/CM0 or Sx/Mx to G3	Intel® PETS Package: Compliance_Power_G3-S0.xml Compliance_Power_RST.xml
ME_PM_44	S0/CM0-PG, CM0 to S4-S5/CM-Off	Intel® PETS Package: Compliance_ME_Power_Gating.xml
ME_PM_45	G3 or S4-S5/CM-Off to S0/CM0_PG, CM0	Intel® PETS Package: Compliance_ME_Power_Gating.xml Compliance_ME_Power_Gating_Network_Wake.xml
ME_PM_46	S0/CM0-PG, CM0 to S0/CM0-PG, CM0	Intel® PETS Package: Compliance_ME_Power_Gating.xml Compliance_Power_RST.xml
ME_PM_50	S0/CM0 to Sx (Cm3 or CM-Off) to S0/CM0 via AC Attach	Intel (R) PETS Package: Compliance_Power_G3-S5.xml Compliance_Power_G3-S5_UnProvision.xml
ME_PM_51	S0/CM0 to Sx/CM-Off to S0/CM0 via AC Detach in Sx State	Intel (R) PETS Package: Compliance_Power_G3-S5.xml

Notes:



1. All the tests which use wake on LAN (WOL) as a trigger require SUSPEND well (SUS well) to be powered up. Hence platforms which implement and support DeepSx cannot run WOL tests. PETS includes all the WOL tests under a single package named Compliance_Power_WOL.xml.
2. Some tests defined in this chapter perform a non-graceful system shutdown or restart. In cases where the Host OS used on the SUT during the test is Microsoft* Windows*, the test may cause the Host OS to enter into recovery mode due to non-graceful power state transition. **Test operators should be aware of the Host OS boot state during these tests to avoid impact to the Host OS on the SUT or invalid test result collection.** The following is a list of tests which may have impact on subsequent Host OS boot: ME_PM_17.6, ME_PM_18.1 through ME_PM_18.4, ME_PM_19.1/2, ME_PM_20.1/2, ME_PM_20.21, ME_PM_26.5 through ME_PM_26.8, ME_PM_26.13, ME_PM_27.1/2, and ME_PM_46.3 through ME_PM_46.6.

12.4 ME_PM_1: S0/CM0 to S3/CM-Off

ID:	ME_PM_1.1		
Title:	S0/CM0 to S3/CM-Off via Host OS suspend (DC-only/PP1/LP3)		
Requirement:	Mandatory	Exemptions	<input checked="" type="checkbox"/> Non-Mobile (AC-only) systems <input checked="" type="checkbox"/> Modern Standby and InstantGo* systems
Method:	Automated by Intel® PETS		
Objective:	This test checks the SUT power flow from S0/CM0 to S3/CM-Off via Host OS suspend with the parameters outlined below.		
Configuration:	This test assumes that either LAN-only, WLAN-only, or both LAN and WLAN network interfaces are available on the SUT.		
Parameters:	System Power Source		DC-only
	Power States	Initial	S0/MeOn (CM0, CM0-PG)
		Final	S3/MeOff (CM-Off)
		Trigger	Host OS suspend
	Intel® AMT	Power Package	PP1 (Intel® ME on in S0)
		WLAN Link Policy	LP3 (Enabled in S0, Sx/AC) where available
Setup:	<ol style="list-style-type: none"> 1. Set the SUT power source to AC+DC. 2. Bring the SUT to the base state of S0/MeOn (CM0,CM0-PG), and confirm that the Host OS is available. 3. Verify that a DC battery is connected to the SUT, and that it is charged. 4. Set the SUT power source to DC-only. 5. Set the active power package on the SUT to Power Package 1 (Intel® ME on in S0). 6. Set the Intel® AMT WLAN link policy on the SUT to Link Policy 3 (Enabled in S0, Sx/AC), if the WLAN network interface is available. 7. Ensure that the Host OS network device drivers are configured to not wake the SUT. This includes enabling ARP and/or NS Offload features where available to help prevent unexpected host wake events. Most especially, ensure that the Host OS Wireless Wake on LAN driver setting on the SUT is disabled, if the WLAN network interface is available. 8. Ensure that Intel® RMT is disabled, if running on an All-in-One (AIO) SUT with feature support. 9. Verify that Intel® AMT on the SUT responds to version queries via all available network interfaces. 		
Procedure:	<ol style="list-style-type: none"> 1. Suspend the SUT via the Host OS. 2. Verify that the SUT is in S3/MeOff (CM-Off) 		
Pass Criteria:	The test passes if the SUT moves to S3, and the Intel® CSME moves to MeOff (CM-Off).		

ID:	ME_PM_1.2		
Title:	S0/CM0 to S3/CM-Off via Host OS suspend (AC+DC, AC-only/PP1/LP3)		
Requirement:	Mandatory	Exemptions	<input checked="" type="checkbox"/> Modern Standby and InstantGo* systems
Method:	Automated by Intel® PETS		
Objective:	This test checks the SUT power flow from S0/CM0 to S3/CM-Off via Host OS suspend with the parameters outlined below.		
Configuration:	This test assumes that either LAN-only, WLAN-only, or both LAN and WLAN network interfaces are available on the SUT.		



ID:	ME_PM_1.2		
Parameters:	System Power Source		AC+DC or AC-only
	Power States	Initial	S0/MeOn (CM0, CM0-PG)
		Final	S3/MeOff (CM-Off)
		Trigger	Host OS suspend
	Intel® AMT	Power Package	PP1 (Intel® ME on in S0)
		WLAN Link Policy	LP3 (Enabled in S0, Sx/AC) where available
Setup:	<ol style="list-style-type: none"> 1. Set the SUT power source to AC+DC where supported; otherwise AC-only. 2. Bring the SUT to the base state of S0/MeOn (CM0,CM0-PG), and confirm that the Host OS is available. 3. Set the active power package on the SUT to Power Package 1 (Intel® ME on in S0). 4. Set the Intel® AMT WLAN link policy on the SUT to Link Policy 3 (Enabled in S0, Sx/AC), if the WLAN network interface is available. 5. Ensure that the Host OS network device drivers are configured to not wake the SUT. This includes enabling ARP and/or NS Offload features where available to help prevent unexpected host wake events. Most especially, ensure that the Host OS Wireless Wake on LAN driver setting on the SUT is disabled, if the WLAN network interface is available. 6. Ensure that Intel® RMT is disabled, if running on a Desktop or All-in-One (AIO) SUT with feature support. 7. Verify that Intel® AMT on the SUT responds to version queries via all available network interfaces. 		
Procedure:	<ol style="list-style-type: none"> 1. Suspend the SUT via the Host OS. 2. Verify that the SUT is in S3/MeOff (CM-Off). 		
Pass Criteria:	The test passes if the SUT moves to S3, and the Intel® CSME moves to MeOff (CM-Off).		

ID:	ME_PM_1.3		
Title:	S0/CM0 to S3/CM3-PG with AC Wake via Host OS suspend (DC-only/PP2/LP3)		
Requirement:	Mandatory	Exemptions	<input checked="" type="checkbox"/> Non-Mobile (AC-only) systems
			<input checked="" type="checkbox"/> Modern Standby and InstantGo* systems
Method:	Automated by Intel® PETS		
Objective:	This test checks the SUT power flow from S0/CM0 to S3/CM3-PGwith AC Wake via Host OS suspend with the parameters outlined below.		
Configuration:	This test assumes that either LAN-only, WLAN-only, or both LAN and WLAN network interfaces are available on the SUT.		
Parameters:	System Power Source		DC-only
	Power States	Initial	S0/MeOn (CM0, CM0-PG)
		Final	S3/CM3-PG
		Trigger	Host OS suspend
	Intel® AMT	Power Package	PP2 (Intel® ME on in S0, wake in Sx/AC)
		WLAN Link Policy	LP3 (Enabled in S0, Sx/AC) where available
Setup:	1. Set the SUT power source to AC+DC.		
	2. Bring the SUT to the base state of S0/MeOn (CM0,CM0-PG), and confirm that the Host OS is available.		
	3. Verify that a DC battery is connected to the SUT, and that it is charged.		
	4. Set the SUT power source to DC-only .		
	5. Set the active power package on the SUT to Power Package 2 (Intel® ME on in S0, wake in Sx/AC).		
	6. Set the Intel® AMT WLAN link policy on the SUT to Link Policy 3 (Enabled in S0, Sx/AC), if the WLAN network interface is available.		
	7. Ensure that the Host OS network device drivers are configured to not wake the SUT. This includes enabling ARP and/or NS Offload features where available to help prevent unexpected host wake events. Most especially, ensure that the Host OS Wireless Wake on LAN driver setting on the SUT is disabled , if the WLAN network interface is available.		
	8. Ensure that Intel® RMT is disabled , if running on a Desktop or All-in-One (AIO) SUT with feature support.		
	9. Verify that Intel® AMT on the SUT responds to version queries via all available network interfaces.		



ID:	ME_PM_1.3
Procedure:	1. Suspend the SUT via the Host OS. 2. Verify that the SUT is in S3/(CM3-PG).
Pass Criteria:	The test passes if the SUT moves to S3, and the Intel® CSME moves to CM3-PG.

12.5 ME_PM_2: S3/CM-Off to S0/CM0

ID:	ME_PM_2.1																	
Title:	S3/CM-Off to S0/CM0 via magic packet (AC+DC, AC-only/PP1/LP3)																	
Requirement:	Mandatory	Exemptions	<input checked="" type="checkbox"/> Systems without WoL and/or WoWLAN support <input checked="" type="checkbox"/> Modern Standby and InstantGo* systems															
Method:	Automated by Intel® PETS																	
Objective:	This test checks the SUT power flow from S3/CM-Off to S0/CM0 via magic packet with the parameters outlined below.																	
Configuration:	This test assumes that either LAN-only, WLAN-only, or both LAN and WLAN network interfaces are available on the SUT. Where both network interfaces are available, LAN is the initial active network interface in the test, and WLAN is the secondary network interface.																	
Parameters:	<table><tr><td colspan="2">System Power Source</td><td>AC+DC or AC-only</td></tr><tr><td rowspan="3">Power States</td><td>Initial</td><td>S3/MeOff (CM-Off)</td></tr><tr><td>Final</td><td>S0/MeOn (CM0, CM0-PG)</td></tr><tr><td>Trigger</td><td>Magic Packet receipt</td></tr><tr><td rowspan="2">Intel® AMT</td><td>Power Package</td><td>PP1 (Intel® ME on in S0)</td></tr><tr><td>WLAN Link Policy</td><td>LP3 (Enabled in S0, Sx/AC) where available</td></tr></table>			System Power Source		AC+DC or AC-only	Power States	Initial	S3/MeOff (CM-Off)	Final	S0/MeOn (CM0, CM0-PG)	Trigger	Magic Packet receipt	Intel® AMT	Power Package	PP1 (Intel® ME on in S0)	WLAN Link Policy	LP3 (Enabled in S0, Sx/AC) where available
System Power Source		AC+DC or AC-only																
Power States	Initial	S3/MeOff (CM-Off)																
	Final	S0/MeOn (CM0, CM0-PG)																
	Trigger	Magic Packet receipt																
Intel® AMT	Power Package	PP1 (Intel® ME on in S0)																
	WLAN Link Policy	LP3 (Enabled in S0, Sx/AC) where available																
Setup:	<ol style="list-style-type: none">Set the SUT power source to AC+DC where supported; otherwise AC-only.Bring the SUT to the base state of S0/MeOn (CM0,CM0-PG), and confirm that the Host OS is available.Set the active power package on the SUT to Power Package 1 (Intel® ME on in S0).Set the Intel® AMT WLAN link policy on the SUT to Link Policy 3 (Enabled in S0, Sx/AC), if the WLAN network interface is available.Ensure that, where available, only the Host OS Wake on LAN and/or Wake on Wireless LAN driver setting(s) are enabled on the SUT. All other network wake sources must be disabled. This includes enabling ARP and/or NS Offload features where available to help prevent unexpected host wake events.Ensure that Intel® RMT is disabled, if running on a Desktop or All-in-One (AIO) SUT with feature support.Record the Host OS last boot time on the SUT (to verify successful return from S3).Verify that Intel® AMT on the SUT responds to version queries via all available network interfaces.Ensure yellow bang is not seen on Drivers in Device Manager																	
Procedure:	<ol style="list-style-type: none">Suspend the SUT via the Host OS.Verify that the SUT is in S3/MeOff (CM-Off).Send three magic packets, at 2 second intervals, by means of the active network interface.Verify that the SUT is in S0/MeOn (CM0,CM0-PG).Verify that the Host OS on the SUT is available.Verify that Intel® AMT on the SUT responds to version queries via all available network interfaces.Verify the Host OS last boot time on the SUT matches the boot time recorded before entry into S3.Verify that the second nibble of the FWSTS2 register on the SUT have a value of 0x60xxxxxx.Ensure yellow bang is not seen on Drivers in Device Manager <p>If both LAN and WLAN network interfaces are available, repeat this test procedure with the WLAN interface set as the active network interface.</p>																	



ID:	ME_PM_2.1
Pass Criteria:	<p>The test passes if:</p> <ul style="list-style-type: none"> the SUT moves from S3 to S0. the Intel® CSME moves to MeOn (CM0, CM0-PG). Intel® AMT responds to version queries via all available network interfaces. the Host OS last boot time has not changed.

ID:	ME_PM_2.2		
Title:	S3/CM-Off to S0/CM0 via Power Button press (DC-only/PP1/LP3)		
Requirement:	Mandatory	Exemptions	<input checked="" type="checkbox"/> Non-Mobile (AC-only) systems <input checked="" type="checkbox"/> Modern Standby and InstantGo* systems
Method:	Automated by Intel® PETS		
Objective:	This test checks the SUT power flow from S3/CM-Off to S0/CM0 via Power Button press with the parameters outlined below.		
Configuration:	This test assumes that either LAN-only, WLAN-only, or both LAN and WLAN network interfaces are available on the SUT.		
Parameters:	System Power Source		DC-only
	Power States	Initial	S3/MeOff (CM-Off)
		Final	S0/MeOn (CM0, CM0-PG)
		Trigger	Power Button press
	Intel® AMT	Power Package	PP1 (Intel® ME on in S0)
		WLAN Link Policy	LP3 (Enabled in S0, Sx/AC) where available
Setup:	<ol style="list-style-type: none"> Set the SUT power source to AC+DC. Bring the SUT to the base state of S0/MeOn (CM0,CM0-PG), and confirm that the Host OS is available. Verify that a DC battery is connected to the SUT, and that it is charged. Set the SUT power source to DC-only. Set the active power package on the SUT to Power Package 1 (Intel® ME on in S0). Set the Intel® AMT WLAN link policy on the SUT to Link Policy 3 (Enabled in S0, Sx/AC), if the WLAN network interface is available. Ensure that the Host OS network device drivers are configured to not wake the SUT. This includes enabling ARP and/or NS Offload features where available to help prevent unexpected host wake events. Most especially, ensure that the Host OS Wireless Wake on LAN driver setting on the SUT is disabled, if the WLAN network interface is available. Ensure that Intel® RMT is disabled, if running on an All-in-One (AIO) SUT with feature support. Record the Host OS last boot time on the SUT (to verify successful return from S3). Verify that Intel® AMT on the SUT responds to version queries via all available network interfaces. Ensure yellow bang is not seen on Drivers in Device Manager Suspend the SUT via the Host OS. Verify that the SUT is in S3/MeOff (CM-Off). 		
Procedure:	<ol style="list-style-type: none"> Briefly press the Power Button on the SUT. Verify that the SUT is in S0/MeOn (CM0,CM0-PG). Verify that the Host OS on the SUT is available. Verify that Intel® AMT on the SUT responds to version queries via all available network interfaces. Verify the Host OS last boot time on the SUT matches the boot time recorded before entry into S3. Verify that the second nibble of the FWSTS2 register on the SUT have a value of 0x60xxxxxx. Ensure yellow bang is not seen on Drivers in Device Manager 		
Pass Criteria:	<p>The test passes if:</p> <ul style="list-style-type: none"> the SUT moves from S3 to S0. the Intel® CSME moves to MeOn (CM0, CM0-PG). Intel® AMT responds to version queries via all available network interfaces. the Host OS last boot time has not changed. 		



ID:	ME_PM_2.3		
Title:	S3/CM-Off to S0/CM0 via Power Button press (AC+DC, AC-only/PP1/LP3)		
Requirement:	Mandatory	Exemptions	<input checked="" type="checkbox"/> Modern Standby and InstantGo* systems
Method:	Automated by Intel® PETS		
Objective:	This test checks the SUT power flow from S3/CM-Off to S0/CM0 via Power Button press with the parameters outlined below.		
Configuration:	This test assumes that either LAN-only, WLAN-only, or both LAN and WLAN network interfaces are available on the SUT.		
Parameters:	System Power Source		AC+DC or AC-only
	Power States	Initial	S3/MeOff (CM-Off)
		Final	S0/MeOn (CM0, CM0-PG)
		Trigger	Power Button press
	Intel® AMT	Power Package	PP1 (Intel® ME on in S0)
WLAN Link Policy		LP3 (Enabled in S0, Sx/AC) where available	
Setup:	<div>1. Set the SUT power source to AC+DC where supported; otherwise AC-only.</div> <div>2. Bring the SUT to the base state of S0/MeOn (CM0,CM0-PG), and confirm that the Host OS is available.</div> <div>3. Set the active power package on the SUT to Power Package 1 (Intel® ME on in S0).</div> <div>4. Set the Intel® AMT WLAN link policy on the SUT to Link Policy 3 (Enabled in S0, Sx/AC), if the WLAN network interface is available.</div> <div>5. Ensure that the Host OS network device drivers are configured to not wake the SUT. This includes enabling ARP and/or NS Offload features where available to help prevent unexpected host wake events. Most especially, ensure that the Host OS Wireless Wake on LAN driver setting on the SUT is disabled, if the WLAN network interface is available.</div> <div>6. Ensure that Intel® RMT is disabled, if running on a Desktop or All-in-One (AIO) SUT with feature support.</div> <div>7. Record the Host OS last boot time on the SUT (to verify successful return from S3).</div> <div>8. Verify that Intel® AMT on the SUT responds to version queries via all available network interfaces.</div> <div>9. Ensure yellow bang is not seen on Drivers in Device Manager</div> <div>10. Suspend the SUT via the Host OS.</div> <div>11. Verify that the SUT is in S3/MeOff (CM-Off).</div>		
Procedure:	<div>1. Briefly press the Power Button on the SUT.</div> <div>2. Verify that the SUT is in S0/MeOn (CM0,CM0-PG).</div> <div>3. Verify that the Host OS on the SUT is available.</div> <div>4. Verify that Intel® AMT on the SUT responds to version queries via all available network interfaces.</div> <div>5. Verify the Host OS last boot time on the SUT matches the boot time recorded before entry into S3.</div> <div>6. Verify that the second nibble of the FWSTS2 register on the SUT have a value of 0x60xxxxxx.</div> <div>7. Ensure yellow bang is not seen on Drivers in Device Manager</div>		
Pass Criteria:	<div>The test passes if:</div> <div><ul style="list-style-type: none">the SUT moves from S3 to S0.the Intel® CSME moves to MeOn (CM0, CM0-PG).Intel® AMT responds to version queries via all available network interfaces.the Host OS last boot time has not changed.</div>		

ID:	ME_PM_2.4	
Title:	S3/CM3-PG to S0/CM0 via magic packet (AC+DC, AC-only/PP2/LP3)	
Requirement:	Mandatory	Exemptions <input checked="" type="checkbox"/> Systems without WoL and/or WoWLAN support <input checked="" type="checkbox"/> Modern Standby and InstantGo* systems
Method:	Automated by Intel® PETS	
Objective:	This test checks the SUT power flow from S3/CM-Off to S0/CM0 via magic packet with the parameters outlined below.	



ID:	ME_PM_2.4																
Configuration:	Intel® AMT should be provisioned via manual mode. This test assumes that either LAN-only, WLAN-only, or both LAN and WLAN network interfaces are available on the SUT. Where both network interfaces are available, LAN is the initial active network interface in the test, and WLAN is the secondary network interface.																
Parameters:	<table> <tr> <td colspan="2">System Power Source</td><td>AC+DC or AC-only</td></tr> <tr> <td rowspan="3">Power States</td><td>Initial</td><td>S3/CM3-PG</td></tr> <tr> <td>Final</td><td>S0/MeOn (CM0, CM0-PG)</td></tr> <tr> <td>Trigger</td><td>Magic Packet receipt</td></tr> <tr> <td rowspan="2">Intel® AMT</td><td>Power Package</td><td>PP2 (Intel® ME on in S0, wake in Sx/AC)</td></tr> <tr> <td>WLAN Link Policy</td><td>LP3 (Enabled in S0, Sx/AC) where available</td></tr> </table>	System Power Source		AC+DC or AC-only	Power States	Initial	S3/CM3-PG	Final	S0/MeOn (CM0, CM0-PG)	Trigger	Magic Packet receipt	Intel® AMT	Power Package	PP2 (Intel® ME on in S0, wake in Sx/AC)	WLAN Link Policy	LP3 (Enabled in S0, Sx/AC) where available	
System Power Source		AC+DC or AC-only															
Power States	Initial	S3/CM3-PG															
	Final	S0/MeOn (CM0, CM0-PG)															
	Trigger	Magic Packet receipt															
Intel® AMT	Power Package	PP2 (Intel® ME on in S0, wake in Sx/AC)															
	WLAN Link Policy	LP3 (Enabled in S0, Sx/AC) where available															
Setup:	<ol style="list-style-type: none"> Set the SUT power source to AC+DC where supported; otherwise AC-only. Bring the SUT to the base state of S0/MeOn (CM0,CM0-PG), and confirm that the Host OS is available. Set the active power package on the SUT to Power Package 2 (Intel® ME on in S0, wake in Sx/AC). Set the Intel® AMT WLAN link policy on the SUT to Link Policy 3 (Enabled in S0, Sx/AC), if the WLAN network interface is available. Ensure the Intel® AMT idle timeout on the SUT is set to 1 minute. Ensure that, where available, only the Host OS Wake on LAN and/or Wake on Wireless LAN driver setting(s) are enabled on the SUT. All other network wake sources must be disabled. This includes enabling ARP and/or NS Offload features where available to help prevent unexpected host wake events. Ensure that Intel® RMT is disabled, if running on a Desktop or All-in-One (AIO) SUT with feature support. Record the Host OS last boot time on the SUT (to verify successful return from S3). Verify that Intel® AMT on the SUT responds to version queries via all available network interfaces. Ensure yellow bang is not seen on Drivers in Device Manager 																
Procedure:	<ol style="list-style-type: none"> Suspend the SUT via the Host OS. Verify that the SUT is in S3/MeOn (CM3). Verify that Intel® AMT on the SUT responds to version query via the LAN network interface. Wait for 3 minutes to allow the Intel® ME on the SUT to move to CM3-PG after Intel® AMT idle timeout. Verify that the Intel® ME on the SUT is in CM3-PG. Send three magic packets, at 2 second intervals, by means of the active network interface. Verify that the SUT is in S0/MeOn (CM0,CM0-PG). Verify that the Host OS on the SUT is available. Verify that Intel® AMT on the SUT responds to version queries via all available network interfaces. Verify the Host OS last boot time on the SUT matches the boot time recorded before entry into S3. Verify that the second nibble of the FWSTS2 register on the SUT have a value of 0x60xxxxxx. Ensure yellow bang is not seen on Drivers in Device Manager <p>If both LAN and WLAN network interfaces are available, repeat this test procedure with the WLAN interface set as the active network interface.</p>																
Pass Criteria:	<p>The test passes if:</p> <ul style="list-style-type: none"> the SUT moves from S3 to S0. the Intel® CSME is in MeOn (CM0, CM0-PG). Intel® AMT responds to version queries via all available network interfaces. the Host OS last boot time has not changed. 																

ID:	ME_PM_2.5		
Title:	S3/CM3-PG with AC Wake to S0/CM0 via Power Button press (DC-only/PP2/LP3)		
Requirement:	Mandatory	Exemptions	<input checked="" type="checkbox"/> Non-Mobile (AC-only) systems
			<input checked="" type="checkbox"/> Modern Standby and InstantGo* systems



ID:	ME_PM_2.5		
Method:	Automated by Intel® PETS		
Objective:	This test checks the SUT power flow from S3/CM3-PG with AC Wake to S0/CM0 via Power Button press with the parameters outlined below.		
Configuration:	This test assumes that either LAN-only, WLAN-only, or both LAN and WLAN network interfaces are available on the SUT.		
Parameters:	System Power Source		DC-only
	Power States	Initial	S3/CM3-PG with AC Wake
		Final	S0/MeOn (CM0, CM0-PG)
		Trigger	Power Button press
	Intel® AMT	Power Package	PP2 (Intel® ME on in S0, wake in Sx/AC)
WLAN Link Policy		LP3 (Enabled in S0, Sx/AC) where available	
Setup:	<div>1. Set the SUT power source to AC+DC.</div> <div>2. Bring the SUT to the base state of S0/MeOn (CM0,CM0-PG), and confirm that the Host OS is available.</div> <div>3. Verify that a DC battery is connected to the SUT, and that it is charged.</div> <div>4. Set the SUT power source to DC-only.</div> <div>5. Set the active power package on the SUT to Power Package 2 (Intel® ME on in S0, wake in Sx/AC).</div> <div>6. Set the Intel® AMT WLAN link policy on the SUT to Link Policy 3 (Enabled in S0, Sx/AC), if the WLAN network interface is available.</div> <div>7. Ensure that the Host OS network device drivers are configured to not wake the SUT. This includes enabling ARP and/or NS Offload features where available to help prevent unexpected host wake events. Most especially, ensure that the Host OS Wireless Wake on LAN driver setting on the SUT is disabled, if the WLAN network interface is available.</div> <div>8. Ensure that Intel® RMT is disabled, if running on an All-in-One (AIO) SUT with feature support.</div> <div>9. Record the Host OS last boot time on the SUT (to verify successful return from S3).</div> <div>10. Verify that Intel® AMT on the SUT responds to version queries via all available network interfaces.</div> <div>11. Ensure yellow bang is not seen on Drivers in Device Manager</div> <div>12. Suspend the SUT via the Host OS.</div> <div>13. Verify that the SUT is in S3/CM3-PG with AC Wake</div>		
Procedure:	<div>1. Briefly press the Power Button on the SUT.</div> <div>2. Verify that the SUT is in S0/MeOn (CM0,CM0-PG).</div> <div>3. Verify that the Host OS on the SUT is available.</div> <div>4. Verify that Intel® AMT on the SUT responds to version queries via all available network interfaces.</div> <div>5. Verify the Host OS last boot time on the SUT matches the boot time recorded before entry into S3.</div> <div>6. Verify that the second nibble of the FWSTS2 register on the SUT have a value of 0x60xxxxxx.</div> <div>7. Ensure yellow bang is not seen on Drivers in Device Manager</div>		
Pass Criteria:	<div>The test passes if:</div> <div><ul style="list-style-type: none">the SUT moves from S3 to S0.the Intel® CSME moves to MeOn (CM0, CM0-PG).Intel® AMT responds to version queries via all available network interfaces.the Host OS last boot time has not changed.</div>		

ID:	ME_PM_2.6
Title:	S3/CM3-PG to S0/CM0 via Power Button press (AC+DC, AC-only/PP2/LP3)
Requirement:	Mandatory Exemptions <input checked="" type="checkbox"/> Modern Standby and InstantGo* systems
Method:	Automated by Intel® PETS
Objective:	This test checks the SUT power flow from S3/CM3-PG to S0/CM0 via Power Button press with the parameters outlined below.
Configuration:	<p>Intel® AMT should be provisioned via manual mode.</p> <p>This test assumes that either LAN-only, WLAN-only, or both LAN and WLAN network interfaces are available on the SUT.</p>



ID:	ME_PM_2.6	
Parameters:	System Power Source AC+DC or AC-only	
	Power States	Initial S3/CM3-PG
		Final S0/MeOn (CM0, CM0-PG)
		Trigger Power Button press
	Intel® AMT	Power Package PP2 (Intel® ME on in S0, wake in Sx/AC)
		WLAN Link Policy LP3 (Enabled in S0, Sx/AC) where available
Setup:	<ol style="list-style-type: none"> 1. Set the SUT power source to AC+DC where supported; otherwise AC-only. 2. Bring the SUT to the base state of S0/MeOn (CM0,CM0-PG), and confirm that the Host OS is available. 3. Set the active power package on the SUT to Power Package 2 (Intel® ME on in S0, wake in Sx/AC). 4. Set the Intel® AMT WLAN link policy on the SUT to Link Policy 3 (Enabled in S0, Sx/AC), if the WLAN network interface is available. 5. Ensure the Intel® AMT idle timeout on the SUT is set to 1 minute. 6. Ensure that the Host OS network device drivers are configured to not wake the SUT. This includes enabling ARP and/or NS Offload features where available to help prevent unexpected host wake events. Most especially, ensure that the Host OS Wireless Wake on LAN driver setting on the SUT is disabled, if the WLAN network interface is available. 7. Ensure that Intel® RMT is disabled, if running on a Desktop or All-in-One (AIO) SUT with feature support. 8. Record the Host OS last boot time on the SUT (to verify successful return from S3). 9. Verify that Intel® AMT on the SUT responds to version queries via all available network interfaces. 10. Ensure yellow bang is not seen on Drivers in Device Manager 11. Suspend the SUT via the Host OS. 12. Verify that the SUT is in S3/MeOn (CM3). 13. Verify that Intel® AMT on the SUT responds to version queries via all available network interfaces. 	
Procedure:	<ol style="list-style-type: none"> 1. Wait for 3 minutes to allow the Intel® ME on the SUT to move to CM3-PG after Intel® AMT idle timeout. 2. Verify that the Intel® ME on the SUT is in CM3-PG. 3. Briefly press the Power Button on the SUT. 4. Verify that the SUT is in S0/MeOn (CM0,CM0-PG). 5. Verify that the Host OS on the SUT is available. 6. Verify that Intel® AMT on the SUT responds to version queries via all available network interfaces. 7. Verify the Host OS last boot time on the SUT matches the boot time recorded before entry into S3. 8. Verify that the second nibble of the FWSTS2 register on the SUT have a value of 0x60xxxxxx. 9. Ensure yellow bang is not seen on Drivers in Device Manager 	
Pass Criteria:	<p>The test passes if:</p> <ul style="list-style-type: none"> • the SUT moves from S3 to S0. • the Intel® CSME moves to MeOn (CM0, CM0-PG). • Intel® AMT responds to version queries via all available network interfaces. • the Host OS last boot time has not changed. 	

ID:	ME_PM_2.7	
Title:	S3/CM-Off with AC Wake to S0/CM0 via magic packet (DC-only/PP1/LP3)	
Requirement:	Optional Non-Support	<input checked="" type="checkbox"/> Non-Mobile (AC-only) systems
		<input checked="" type="checkbox"/> Systems without WoL and/or WoWLAN support
		<input checked="" type="checkbox"/> Modern Standby and InstantGo* systems
Method:	Automated by Intel® PETS	
Objective:	This test checks the SUT power flow from S3/CM3-PG with AC Wake to S0/CM0 via magic packet with the parameters outlined below.	
Configuration:	This test assumes that either LAN-only, WLAN-only, or both LAN and WLAN network interfaces are available on the SUT. Where both network interfaces are available, LAN is the initial active network interface in the test, and WLAN is the secondary network interface.	



ID:	ME_PM_2.7	
Parameters:	System Power Source	
	DC-only	
	Power States	Initial
		S3/CM3-PG with AC Wake
	Intel® AMT	Final
		S0/MeOn (CM0, CM0-PG)
		Trigger
		Magic Packet receipt
		Power Package
		PP1 (Intel® ME on in S0)
		WLAN Link Policy
		LP3 (Enabled in S0, Sx/AC) where available
Setup:	<ol style="list-style-type: none"> Set the SUT power source to AC+DC. Bring the SUT to the base state of S0/MeOn (CM0,CM0-PG), and confirm that the Host OS is available. Verify that a DC battery is connected to the SUT, and that it is charged. Set the SUT power source to DC-only. Set the active power package on the SUT to Power Package 1 (Intel® ME on in S0). Set the Intel® AMT WLAN link policy on the SUT to Link Policy 3 (Enabled in S0, Sx/AC), if the WLAN network interface is available. Ensure that, where available, only the Host OS Wake on LAN and/or Wake on Wireless LAN driver setting(s) are enabled on the SUT. All other network wake sources must be disabled. This includes enabling ARP and/or NS Offload features where available to help prevent unexpected host wake events. Ensure that Intel® RMT is disabled, if running on an All-in-One (AIO) SUT with feature support. Record the Host OS last boot time on the SUT (to verify successful return from S3). Verify that Intel® AMT on the SUT responds to version queries via all available network interfaces. Ensure yellow bang is not seen on Drivers in Device Manager 	
Procedure:	<ol style="list-style-type: none"> Suspend the SUT via the Host OS. Verify that the SUT is in S3/CM3-PG with AC Wake. Send three magic packets, at 2 second intervals, by means of the active network interface. Verify that the SUT is in S0/MeOn (CM0,CM0-PG). Verify that the Host OS on the SUT is available. Verify that Intel® AMT on the SUT responds to version queries via all available network interfaces. Verify the Host OS last boot time on the SUT matches the boot time recorded before entry into S3. Verify that the second nibble of the FWSTS2 register on the SUT have a value of 0x60xxxxxx. Ensure yellow bang is not seen on Drivers in Device Manager <p>If both LAN and WLAN network interfaces are available, repeat this test procedure with the WLAN interface set as the active network interface.</p>	
Pass Criteria:	<p>The test passes if:</p> <ul style="list-style-type: none"> the SUT moves from S3 to S0. the Intel® CSME moves to MeOn (CM0, CM0-PG). Intel® AMT responds to version queries via all available network interfaces. the Host OS last boot time has not changed. 	

ID:	ME_PM_2.8	
Title:	S3/CM3-PG with AC Wake to S0/CM0 via magic packet (DC-only/PP2/LP3)	
Requirement:	Optional Non-Support	<input checked="" type="checkbox"/> Non-Mobile (AC-only) systems
		<input checked="" type="checkbox"/> Systems without WoL and/or WoWLAN support
		<input checked="" type="checkbox"/> Modern Standby and InstantGo* systems
Method:	Automated by Intel® PETS	
Objective:	This test checks the SUT power flow from S3/CM3-PG with AC Wake to S0/CM0 via magic packet with the parameters outlined below.	
Configuration:	This test assumes that either LAN-only, WLAN-only, or both LAN and WLAN network interfaces are available on the SUT. Where both network interfaces are available, LAN is the initial active network interface in the test, and WLAN is the secondary network interface.	



ID:	ME_PM_2.8		
Parameters:	System Power Source		DC-only
	Power States	Initial	S3/CM3-PG with AC Wake
		Final	S0/MeOn (CM0, CM0-PG)
		Trigger	Magic Packet receipt
	Intel® AMT	Power Package	PP2 (Intel® ME on in S0, wake in Sx/AC)
		WLAN Link Policy	LP3 (Enabled in S0, Sx/AC) where available
Setup:	<ol style="list-style-type: none"> Set the SUT power source to AC+DC. Bring the SUT to the base state of S0/MeOn (CM0,CM0-PG), and confirm that the Host OS is available. Verify that a DC battery is connected to the SUT, and that it is charged. Set the SUT power source to DC-only. Set the active power package on the SUT to Power Package 2 (Intel® ME on in S0, wake in Sx/AC). Set the Intel® AMT WLAN link policy on the SUT to Link Policy 3 (Enabled in S0, Sx/AC), if the WLAN network interface is available. Ensure that, where available, only the Host OS Wake on LAN and/or Wake on Wireless LAN driver setting(s) are enabled on the SUT. All other network wake sources must be disabled. This includes enabling ARP and/or NS Offload features where available to help prevent unexpected host wake events. Ensure that Intel® RMT is disabled, if running on an All-in-One (AIO) SUT with feature support. Record the Host OS last boot time on the SUT (to verify successful return from S3). Verify that Intel® AMT on the SUT responds to version queries via all available network interfaces. Ensure yellow bang is not seen on Drivers in Device Manager 		
Procedure:	<ol style="list-style-type: none"> Suspend the SUT via the Host OS. Verify that the Intel® ME on the SUT is in CM3-PG.with AC Wake. Send three magic packets, at 2 second intervals, by means of the active network interface. Verify that the SUT is in S0/MeOn (CM0,CM0-PG). Verify that the Host OS on the SUT is available. Verify that Intel® AMT on the SUT responds to version queries via all available network interfaces. Verify the Host OS last boot time on the SUT matches the boot time recorded before entry into S3. Verify that the second nibble of the FWSTS2 register on the SUT have a value of 0x60xxxxxx. Ensure yellow bang is not seen on Drivers in Device Manager <p>If both LAN and WLAN network interfaces are available, repeat this test procedure with the WLAN interface set as the active network interface.</p>		
Pass Criteria:	<p>The test passes if:</p> <ul style="list-style-type: none"> the SUT moves from S3 to S0. the Intel® CSME moves to MeOn (CM0, CM0-PG). Intel® AMT responds to version queries via all available network interfaces. the Host OS last boot time has not changed. 		

12.6 ME_PM_3: S0/CM0 to S3/CM3

ID:	ME_PM_3.1		
Title:	S0/CM0 to S3/CM3 via Host OS suspend (AC+DC, AC-only/PP2/LP3)		
Requirement:	Mandatory	Exemptions	<input checked="" type="checkbox"/> Modern Standby and InstantGo* systems
Method:	Automated by Intel® PETS		
Objective:	This test checks the SUT power flow from S0/CM0 to S3/CM3 via Host OS suspend with the parameters outlined below.		
Configuration:	<p>Intel® AMT should be provisioned via manual mode.</p> <p>This test assumes that either LAN-only, WLAN-only, or both LAN and WLAN network interfaces are available on the SUT.</p>		



ID:	ME_PM_3.1		
Parameters:	System Power Source		AC+DC or AC-only
	Power States	Initial	S0/MeOn (CM0, CM0-PG)
		Final	S3/MeOn (CM3)
		Trigger	Host OS suspend
	Intel® AMT	Power Package	PP2 (Intel® ME on in S0, wake in Sx/AC)
		WLAN Link Policy	LP3 (Enabled in S0, Sx/AC) where available
Setup:	<ol style="list-style-type: none"> Set the SUT power source to AC+DC where supported; otherwise AC-only. Bring the SUT to the base state of S0/MeOn (CM0,CM0-PG), and confirm that the Host OS is available. Set the active power package on the SUT to Power Package 2 (Intel® ME on in S0, wake in Sx/AC). Set the Intel® AMT WLAN link policy on the SUT to Link Policy 3 (Enabled in S0, Sx/AC), if the WLAN network interface is available. Ensure that the Host OS network device drivers are configured to not wake the SUT. This includes enabling ARP and/or NS Offload features where available to help prevent unexpected host wake events. Most especially, ensure that the Host OS Wireless Wake on LAN driver setting on the SUT is disabled, if the WLAN network interface is available. Ensure that Intel® RMT is disabled, if running on a Desktop or All-in-One (AIO) SUT with feature support. Verify that Intel® AMT on the SUT responds to version queries via all available network interfaces. 		
Procedure:	<ol style="list-style-type: none"> Suspend the SUT via the Host OS. Verify that the SUT is in S3/MeOn (CM3). Verify that Intel® AMT on the SUT responds to version queries via all available network interfaces. 		
Pass Criteria:	The test passes if the SUT moves to S3, and the Intel® CSME is in MeOn (CM3).		

ID:	ME_PM_3.21		
Title:	S0/CM0 to S3/CM3 via Host OS suspend (AC+DC, AC-only/PP2/LP2)		
Requirement:	Mandatory	Exemptions	<input checked="" type="checkbox"/> Modern Standby and InstantGo* systems <input checked="" type="checkbox"/> Systems with a LAN-only network interface
Method:	Automated by Intel® PETS		
Objective:	This test checks the SUT power flow from S0/CM0 to S3/CM3 via Host OS suspend with the parameters outlined below.		
Configuration:	Intel® AMT should be provisioned via manual mode. This test assumes that either WLAN-only, or both LAN and WLAN network interfaces are available on the SUT.		
Parameters:	System Power Source		AC+DC or AC-only
	Power States	Initial	S0/MeOn (CM0, CM0-PG)
		Final	S3/MeOn (CM3)
		Trigger	Host OS suspend
	Intel® AMT	Power Package	PP2 (Intel® ME on in S0, wake in Sx/AC)
		WLAN Link Policy	LP2 (Enabled in S0)



ID:	ME_PM_3.21
Setup:	<ol style="list-style-type: none"> 1. Set the SUT power source to AC+DC where supported; otherwise AC-only. 2. Bring the SUT to the base state of S0/MeOn (CM0,CM0-PG), and confirm that the Host OS is available. 3. Set the active power package on the SUT to Power Package 2 (Intel® ME on in S0, wake in Sx/AC). 4. Set the Intel® AMT WLAN link policy on the SUT to Link Policy 2 (Enabled in S0). 5. Ensure that the Host OS network device drivers are configured to not wake the SUT. This includes enabling ARP and/or NS Offload features where available to help prevent unexpected host wake events. Most especially, ensure that the Host OS Wireless Wake on LAN driver setting on the SUT is disabled. 6. Ensure that Intel® RMT is disabled, if running on a Desktop or All-in-One (AIO) SUT with feature support. 7. Verify that Intel® AMT on the SUT responds to version queries via all available network interfaces.
Procedure:	<ol style="list-style-type: none"> 1. Suspend the SUT via the Host OS. 2. Verify that the SUT is in S3/MeOn (CM3). 3. Verify that Intel® AMT on the SUT responds to version query via the LAN network interface, if available. 4. Verify that Intel® AMT on the SUT does not respond to version query via the WLAN network interface.
Pass Criteria:	<p>The test passes if:</p> <ul style="list-style-type: none"> • the SUT moves to S3. • the Intel® CSME is in MeOn (CM3). • when in S3: <ul style="list-style-type: none"> — Intel® AMT on the SUT does respond to version queries via the LAN network interface, if available. — Intel® AMT on the SUT does not respond to version queries the WLAN network interface.

12.7 ME_PM_4: S3/CM3 to S0/CM0

ID:	ME_PM_4.1	
Title:	S3/CM3 to S0/CM0 via magic packet (AC+DC, AC-only/PP2/LP3)	
Requirement:	Mandatory Exemptions	<input checked="" type="checkbox"/> Systems without WoL and/or WoWLAN support
		<input checked="" type="checkbox"/> Modern Standby and InstantGo* systems
Method:	Automated by Intel® PETS	
Objective:	This test checks the SUT power flow from S3/CM3 to S0/CM0 via magic packet with the parameters outlined below.	
Configuration:	<p>Intel® AMT should be provisioned via manual mode.</p> <p>This test assumes that either LAN-only, WLAN-only, or both LAN and WLAN network interfaces are available on the SUT. Where both network interfaces are available, LAN is the initial active network interface in the test, and WLAN is the secondary network interface.</p>	
Parameters:	System Power Source	
	Power States	Initial S3/MeOn (CM3)
		Final S0/MeOn (CM0, CM0-PG)
		Trigger Magic Packet receipt
	Intel® AMT	Power Package PP2 (Intel® ME on in S0, wake in Sx/AC)
		WLAN Link Policy LP3 (Enabled in S0, Sx/AC) where available



ID:	ME_PM_4.1
Setup:	<ol style="list-style-type: none"> 1. Set the SUT power source to AC+DC where supported; otherwise AC-only. 2. Bring the SUT to the base state of S0/MeOn (CM0,CM0-PG), and confirm that the Host OS is available. 3. Set the active power package on the SUT to Power Package 2 (Intel® ME on in S0, wake in Sx/AC). 4. Set the Intel® AMT WLAN link policy on the SUT to Link Policy 3 (Enabled in S0, Sx/AC), if the WLAN network interface is available. 5. Ensure that, where available, only the Host OS Wake on LAN and/or Wake on Wireless LAN driver setting(s) are enabled on the SUT. All other network wake sources must be disabled. This includes enabling ARP and/or NS Offload features where available to help prevent unexpected host wake events. 6. Ensure that Intel® RMT is disabled, if running on a Desktop or All-in-One (AIO) SUT with feature support. 7. Record the Host OS last boot time on the SUT (to verify successful return from S3). 8. Verify that Intel® AMT on the SUT responds to version queries via all available network interfaces. 9. Ensure yellow bang is not seen on Drivers in Device Manager
Procedure:	<ol style="list-style-type: none"> 1. Suspend the SUT via the Host OS. 2. Verify that the SUT is in S3/MeOn (CM3). 3. Verify that Intel® AMT on the SUT responds to version query via the LAN network interface. 4. Send three magic packets, at 2 second intervals, by means of the active network interface. 5. Verify that the SUT is in S0/MeOn (CM0,CM0-PG). 6. Verify that the Host OS on the SUT is available. 7. Verify that Intel® AMT on the SUT responds to version queries via all available network interfaces. 8. Verify the Host OS last boot time on the SUT matches the boot time recorded before entry into S3. 9. Verify that the second nibble of the FWSTS2 register on the SUT have a value of 0x68xxxxxx. 10. Ensure yellow bang is not seen on Drivers in Device Manager <p>If both LAN and WLAN network interfaces are available, repeat this test procedure with the WLAN interface set as the active network interface.</p>
Pass Criteria:	<p>The test passes if:</p> <ul style="list-style-type: none"> • the SUT moves from S3 to S0. • the Intel® CSME is in MeOn (CM0, CM0-PG). • Intel® AMT responds to version queries via all available network interfaces. • the Host OS last boot time has not changed.

ID:	ME_PM_4.2		
Title:	S3/CM3 to S0/CM0 via Power Button press (AC+DC, AC-only/PP2/LP3)		
Requirement:	Mandatory	Exemptions	<input checked="" type="checkbox"/> Modern Standby and InstantGo* systems
Method:	Automated by Intel® PETS		
Objective:	This test checks the SUT power flow from S3/CM3 to S0/CM0 via Power Button press with the parameters outlined below.		
Configuration:	Intel® AMT should be provisioned via manual mode. This test assumes that either LAN-only, WLAN-only, or both LAN and WLAN network interfaces are available on the SUT.		
Parameters:	System Power Source		AC+DC or AC-only
	Power States	Initial	S3/MeOn (CM3)
		Final	S0/MeOn (CM0, CM0-PG)
		Trigger	Power Button press
	Intel® AMT	Power Package	PP2 (Intel® ME on in S0, wake in Sx/AC)
		WLAN Link Policy	LP3 (Enabled in S0, Sx/AC) where available



ID:	ME_PM_4.2
Setup:	<ol style="list-style-type: none"> 1. Set the SUT power source to AC+DC where supported; otherwise AC-only. 2. Bring the SUT to the base state of S0/MeOn (CM0,CM0-PG), and confirm that the Host OS is available. 3. Set the active power package on the SUT to Power Package 2 (Intel® ME on in S0, wake in Sx/AC). 4. Set the Intel® AMT WLAN link policy on the SUT to Link Policy 3 (Enabled in S0, Sx/AC), if the WLAN network interface is available. 5. Ensure that the Host OS network device drivers are configured to not wake the SUT. This includes enabling ARP and/or NS Offload features where available to help prevent unexpected host wake events. Most especially, ensure that the Host OS Wireless Wake on LAN driver setting on the SUT is disabled, if the WLAN network interface is available. 6. Ensure that Intel® RMT is disabled, if running on a Desktop or All-in-One (AIO) SUT with feature support. 7. Record the Host OS last boot time on the SUT (to verify successful return from S3). 8. Verify that Intel® AMT on the SUT responds to version queries via all available network interfaces. 9. Ensure yellow bang is not seen on Drivers in Device Manager 10. Suspend the SUT via the Host OS. 11. Verify that the SUT is in S3/MeOn (CM3). 12. Verify that Intel® AMT on the SUT responds to version queries via all available network interfaces.
Procedure:	<ol style="list-style-type: none"> 1. Briefly press the Power Button on the SUT. 2. Verify that the SUT is in S0/MeOn (CM0,CM0-PG). 3. Verify that the Host OS on the SUT is available. 4. Verify that Intel® AMT on the SUT responds to version queries via all available network interfaces. 5. Verify the Host OS last boot time on the SUT matches the boot time recorded before entry into S3. 6. Verify that the second nibble of the FWSTS2 register on the SUT have a value of 0x68xxxxxx. 7. Ensure yellow bang is not seen on Drivers in Device Manager
Pass Criteria:	<p>The test passes if:</p> <ul style="list-style-type: none"> • the SUT moves from S3 to S0. • the Intel® CSME is in MeOn (CM0, CM0-PG). • Intel® AMT responds to version queries via all available network interfaces. • the Host OS last boot time has not changed.

ID:	ME_PM_4.21		
Title:	S3/CM3 to S0/CM0 via magic packet (AC+DC, AC-only/PP2/LP2)		
Requirement:	Mandatory	Exemptions	<div><input checked="" type="checkbox"/> Systems without WoL and/or WoWLAN support</div> <div><input checked="" type="checkbox"/> Modern Standby and InstantGo* systems</div>
Method:	Automated by Intel® PETS		
Objective:	This test checks the SUT power flow from S3/CM3 to S0/CM0 via magic packet with the parameters outlined below.		
Configuration:	Intel® AMT should be provisioned via manual mode. This test assumes that either LAN-only, WLAN-only, or both LAN and WLAN network interfaces are available on the SUT. Where both network interfaces are available, LAN is the initial active network interface in the test, and WLAN is the secondary network interface.		
Parameters:	System Power Source		AC+DC or AC-only
	Power States	Initial	S3/MeOn (CM3)
		Final	S0/MeOn (CM0, CM0-PG)
		Trigger	Magic Packet receipt
	Intel® AMT	Power Package	PP2 (Intel® ME on in S0, wake in Sx/AC)
		WLAN Link Policy	LP2 (Enabled in S0) where available



ID:	ME_PM_4.21
Setup:	<ol style="list-style-type: none"> 1. Set the SUT power source to AC+DC where supported; otherwise AC-only. 2. Bring the SUT to the base state of S0/MeOn (CM0,CM0-PG), and confirm that the Host OS is available. 3. Set the active power package on the SUT to Power Package 2 (Intel® ME on in S0, wake in Sx/AC). 4. Set the Intel® AMT WLAN link policy on the SUT to Link Policy 2 (Enabled in S0), if the WLAN network interface is available. 5. Ensure that, where available, only the Host OS Wake on LAN and/or Wake on Wireless LAN driver setting(s) are enabled on the SUT. All other network wake sources must be disabled. This includes enabling ARP and/or NS Offload features where available to help prevent unexpected host wake events. 6. Ensure that Intel® RMT is disabled, if running on a Desktop or All-in-One (AIO) SUT with feature support. 7. Record the Host OS last boot time on the SUT (to verify successful return from S3). 8. Verify that Intel® AMT on the SUT responds to version queries via all available network interfaces. 9. Ensure yellow bang is not seen on Drivers in Device Manager
Procedure:	<ol style="list-style-type: none"> 1. Suspend the SUT via the Host OS. 2. Verify that the SUT is in S3/MeOn (CM3). 3. Verify that Intel® AMT on the SUT responds to version query via the LAN network interface. 4. Send three magic packets, at 2 second intervals, by means of the active network interface. 5. Verify that the SUT is in S0/MeOn (CM0,CM0-PG). 6. Verify that the Host OS on the SUT is available. 7. Verify that Intel® AMT on the SUT responds to version queries via all available network interfaces. 8. Verify the Host OS last boot time on the SUT matches the boot time recorded before entry into S3. 9. Verify that the second nibble of the FWSTS2 register on the SUT have a value of 0x68xxxxxx. 10. Ensure yellow bang is not seen on Drivers in Device Manager <p>If both LAN and WLAN network interfaces are available, repeat this test procedure with the WLAN interface set as the active network interface.</p>
Pass Criteria:	<p>The test passes if:</p> <ul style="list-style-type: none"> • the SUT moves from S3 to S0. • the Intel® CSME is in MeOn (CM0, CM0-PG). • Intel® AMT responds to version queries via all available network interfaces. • the Host OS last boot time has not changed.

ID:	ME_PM_4.22		
Title:	S3/CM3 to S0/CM0 via Power Button press (AC+DC, AC-only/PP2/LP2)		
Requirement:	Mandatory	Exemptions	<input checked="" type="checkbox"/> Modern Standby and InstantGo* systems
			<input checked="" type="checkbox"/> Systems with a LAN-only network interface
Method:	Automated by Intel® PETS		
Objective:	This test checks the SUT power flow from S3/CM3 to S0/CM0 via Power Button press with the parameters outlined below.		
Configuration:	Intel® AMT should be provisioned via manual mode. This test assumes that either WLAN-only, or both LAN and WLAN network interfaces are available on the SUT.		
Parameters:	System Power Source		AC+DC or AC-only
	Power States	Initial	S3/MeOn (CM3)
		Final	S0/MeOn (CM0, CM0-PG)
		Trigger	Power Button press
	Intel® AMT	Power Package	PP2 (Intel® ME on in S0, wake in Sx/AC)
		WLAN Link Policy	LP2 (Enabled in S0)



ID:	ME_PM_4.22
Setup:	<ol style="list-style-type: none"> Set the SUT power source to AC+DC where supported; otherwise AC-only. Bring the SUT to the base state of S0/MeOn (CM0,CM0-PG), and confirm that the Host OS is available. Set the active power package on the SUT to Power Package 2 (Intel® ME on in S0, wake in Sx/AC). Set the Intel® AMT WLAN link policy on the SUT to Link Policy 2 (Enabled in S0). Ensure that the Host OS network device drivers are configured to not wake the SUT. This includes enabling ARP and/or NS Offload features where available to help prevent unexpected host wake events. Most especially, ensure that the Host OS Wireless Wake on LAN driver setting on the SUT is disabled. Ensure that Intel® RMT is disabled, if running on a Desktop or All-in-One (AIO) SUT with feature support. Record the Host OS last boot time on the SUT (to verify successful return from S3). Verify that Intel® AMT on the SUT responds to version queries via all available network interfaces. Ensure yellow bang is not seen on Drivers in Device Manager Suspend the SUT via the Host OS. Verify that the SUT is in S3/MeOn (CM3). Verify that Intel® AMT on the SUT responds to version query via the LAN network interface, if available. Verify that Intel® AMT on the SUT does not respond to version query via the WLAN network interface.
Procedure:	<ol style="list-style-type: none"> Briefly press the Power Button on the SUT. Verify that the SUT is in S0/MeOn (CM0,CM0-PG). Verify that the Host OS on the SUT is available. Verify that Intel® AMT on the SUT responds to version queries via all available network interfaces. Verify the Host OS last boot time on the SUT matches the boot time recorded before entry into S3. Verify that the second nibble of the FWSTS2 register on the SUT have a value of 0x68xxxxxx. Ensure yellow bang is not seen on Drivers in Device Manager
Pass Criteria:	<p>The test passes if:</p> <ul style="list-style-type: none"> the SUT moves from S3 to S0. the Intel® CSME is in MeOn (CM0, CM0-PG). Intel® AMT responds to version queries via all available network interfaces. the Host OS last boot time has not changed.

12.8 ME_PM_5: S3/CM3 to S3/CM-Off (Without Intel® ME Wake)

ID:	ME_PM_5.1	
Title:	S3/CM3 to S3/CM3-PG with AC wake via AC-detach (AC+DC/PP2/LP3)	
Requirement:	Mandatory Exemptions	<input checked="" type="checkbox"/> Non-Mobile (AC-only) systems
		<input checked="" type="checkbox"/> Modern Standby and InstantGo* systems
Method:	Automated by Intel® PETS	
Objective:	This test checks the SUT power flow from S3/CM3 to S3/CM3-PG with AC Wake via AC-detach with the parameters outlined below.	
Configuration:	This test assumes that either LAN-only, WLAN-only, or both LAN and WLAN network interfaces are available on the SUT.	
Parameters:	System Power Source AC+DC	
	Power States	Initial S3/MeOn (CM3)
		Final S3/CM3-PG with AC Wake
		Trigger AC-detach
	Intel® AMT	Power Package PP2 (Intel® ME on in S0, wake in Sx/AC)
		WLAN Link Policy LP3 (Enabled in S0, Sx/AC) where available



ID:	ME_PM_5.1
Setup:	<ol style="list-style-type: none"> 1. Set the SUT power source to AC+DC. 2. Bring the SUT to the base state of S0/MeOn (CM0,CM0-PG), and confirm that the Host OS is available. 3. Verify that a DC battery is connected to the SUT, and that it is charged. 4. Set the active power package on the SUT to Power Package 2 (Intel® ME on in S0, wake in Sx/AC). 5. Set the Intel® AMT WLAN link policy on the SUT to Link Policy 3 (Enabled in S0, Sx/AC), if the WLAN network interface is available. 6. Ensure that the Host OS network device drivers are configured to not wake the SUT. This includes enabling ARP and/or NS Offload features where available to help prevent unexpected host wake events. Most especially, ensure that the Host OS Wireless Wake on LAN driver setting on the SUT is disabled, if the WLAN network interface is available. 7. Ensure that Intel® RMT is disabled, if running on an All-in-One (AIO) SUT with feature support. 8. Verify that Intel® AMT on the SUT responds to version queries via all available network interfaces. 9. Suspend the SUT via the Host OS. 10. Verify that the SUT is in S3/MeOn (CM3). 11. Verify that Intel® AMT on the SUT responds to version queries via all available network interfaces.
Procedure:	<ol style="list-style-type: none"> 1. Set the SUT power source to DC-only. 2. Verify that the SUT is in S3/(CM3-PG) with AC Wake.
Pass Criteria:	The test passes if the SUT remains in S3 and the Intel® CSME moves to CM3-PG.

ID:	ME_PM_5.2		
Title:	S3/CM3 to S3/CM-Off via Intel® AMT Power Package change (AC+DC, AC-only/PP2/LP3)		
Requirement:	Mandatory	Exemptions	<input checked="" type="checkbox"/> Modern Standby and InstantGo* systems
Method:	Automated by Intel® PETS		
Objective:	This test checks the SUT power flow from S3/CM3 to S3/CM-Off via Intel® AMT Power Package change with the parameters outlined below.		
Configuration:	This test assumes that either LAN-only, WLAN-only, or both LAN and WLAN network interfaces are available on the SUT.		
Parameters:	System Power Source		AC+DC or AC-only
	Power States	Initial	S3/MeOn (CM3)
		Final	S3/MeOff (CM-Off)
		Trigger	Set Intel® AMT PP1 (Intel® ME on in S0)
	Intel® AMT	Power Package	PP2 (Intel® ME on in S0, wake in Sx/AC)
WLAN Link Policy		LP3 (Enabled in S0, Sx/AC) where available	
Setup:	<div>1. Set the SUT power source to AC+DC where supported; otherwise AC-only.</div> <div>2. Bring the SUT to the base state of S0/MeOn (CM0,CM0-PG), and confirm that the Host OS is available.</div> <div>3. Set the active power package on the SUT to Power Package 2 (Intel® ME on in S0, wake in Sx/AC).</div> <div>4. Set the Intel® AMT WLAN link policy on the SUT to Link Policy 3 (Enabled in S0, Sx/AC), if the WLAN network interface is available.</div> <div>5. Ensure that the Host OS network device drivers are configured to not wake the SUT. This includes enabling ARP and/or NS Offload features where available to help prevent unexpected host wake events. Most especially, ensure that the Host OS Wireless Wake on LAN driver setting on the SUT is disabled, if the WLAN network interface is available.</div> <div>6. Ensure that Intel® RMT is disabled, if running on a Desktop or All-in-One (AIO) SUT with feature support.</div> <div>7. Verify that Intel® AMT on the SUT responds to version queries via all available network interfaces.</div> <div>8. Suspend the SUT via the Host OS.</div> <div>9. Verify that the SUT is in S3/MeOn (CM3).</div> <div>10. Verify that Intel® AMT on the SUT responds to version queries via all available network interfaces.</div>		
Procedure:	<div>1. Set the active power package on the SUT to Power Package 1 (Intel® ME on in S0).</div> <div>2. Verify that the SUT is in S3, Deep S3/MeOff (CM-Off).</div>		



ID:	ME_PM_5.2
Pass Criteria:	The test passes if the SUT remains in S3, and the Intel® CSME moves to MeOff (CM-Off).

ID:	ME_PM_5.21		
Title:	S3/CM3 to S3/CM3-PG with AC Wake via AC-detach (AC+DC/PP2/LP2)		
Requirement:	Mandatory	Exemptions	<input checked="" type="checkbox"/> Non-Mobile (AC-only) systems <input checked="" type="checkbox"/> Modern Standby and InstantGo* systems <input checked="" type="checkbox"/> Systems with a LAN-only network interface
Method:	Automated by Intel® PETS		
Objective:	This test checks the SUT power flow from S3/CM3 to S3/CM3-PG with AC Wake via AC-detach with the parameters outlined below.		
Configuration:	This test assumes that either WLAN-only, or both LAN and WLAN network interfaces are available on the SUT.		
Parameters:	System Power Source		AC+DC
	Power States	Initial	S3/MeOn (CM3)
		Final	S3/CM3-PG with Ac Wake
		Trigger	AC-detach
	Intel® AMT	Power Package	PP2 (Intel® ME on in S0, wake in Sx/AC)
		WLAN Link Policy	LP2 (Enabled in S0)
Setup:	<ol style="list-style-type: none"> Set the SUT power source to AC+DC. Bring the SUT to the base state of S0/MeOn (CM0,CM0-PG), and confirm that the Host OS is available. Verify that a DC battery is connected to the SUT, and that it is charged. Set the active power package on the SUT to Power Package 2 (Intel® ME on in S0, wake in Sx/AC). Set the Intel® AMT WLAN link policy on the SUT to Link Policy 2 (Enabled in S0). Ensure that the Host OS network device drivers are configured to not wake the SUT. This includes enabling ARP and/or NS Offload features where available to help prevent unexpected host wake events. Most especially, ensure that the Host OS Wireless Wake on LAN driver setting on the SUT is disabled. Ensure that Intel® RMT is disabled, if running on an All-in-One (AIO) SUT with feature support. Verify that Intel® AMT on the SUT responds to version queries via all available network interfaces. Suspend the SUT via the Host OS. Verify that the SUT is in S3/MeOn (CM3). Verify that Intel® AMT on the SUT responds to version query via the LAN network interface, if available. Verify that Intel® AMT on the SUT does not respond to version query via the WLAN network interface. 		
Procedure:	<ol style="list-style-type: none"> Set the SUT power source to DC-only. Verify that the SUT is in S3/(CM3-PG) with AC Wake 		
Pass Criteria:	The test passes if the SUT remains in S3, and the Intel® CSME moves to CM3-PG with AC Wake.		

ID:	ME_PM_5.22		
Title:	S3/CM3 to S3/CM-Off via Intel® AMT Power Package change (AC+DC, AC-only/PP2/LP2)		
Requirement:	Mandatory	Exemptions	<input checked="" type="checkbox"/> Modern Standby and InstantGo* systems <input checked="" type="checkbox"/> Systems with a single network interface (not LAN+WLAN)
Method:	Automated by Intel® PETS		
Objective:	This test checks the SUT power flow from S3/CM3 to S3/CM-Off via Intel® AMT Power Package change with the parameters outlined below.		



ID:	ME_PM_5.22	
Configuration:	This test assumes that both LAN and WLAN network interfaces are available on the SUT.	
Parameters:	System Power Source	AC+DC or AC-only
	Power States	Initial S3/MeOn (CM3)
		Final S3/CM3-PG
		Trigger Set Intel® AMT PP1 (Intel® ME on in S0)
	Intel® AMT	Power Package PP2 (Intel® ME on in S0, wake in Sx/AC)
		WLAN Link Policy LP2 (Enabled in S0)
Setup:	<ol style="list-style-type: none"> Set the SUT power source to AC+DC where supported; otherwise AC-only. Bring the SUT to the base state of S0/MeOn (CM0), and confirm that the Host OS is available. Set the active power package on the SUT to Power Package 2 (Intel® ME on in S0, wake in Sx/AC). Set the Intel® AMT WLAN link policy on the SUT to Link Policy 2 (Enabled in S0). Ensure that the Host OS network device drivers are configured to not wake the SUT. This includes enabling ARP and/or NS Offload features where available to help prevent unexpected host wake events. Most especially, ensure that the Host OS Wireless Wake on LAN driver setting on the SUT is disabled. Ensure that Intel® RMT is disabled, if running on a Desktop or All-in-One (AIO) SUT with feature support. Verify that Intel® AMT on the SUT responds to version queries via all available network interfaces. Suspend the SUT via the Host OS. Verify that the SUT is in S3/MeOn (CM3). Verify that Intel® AMT on the SUT responds to version query via the LAN network interface. Verify that Intel® AMT on the SUT does not respond to version query via the WLAN network interface. 	
Procedure:	<ol style="list-style-type: none"> Set the active power package on the SUT to Power Package 1 (Intel® ME on in S0). Verify that the SUT is in S3/MeOff (CM-Off). 	
Pass Criteria:	The test passes if the SUT remains in S3, and the Intel® CSME moves to MeOff (CM-Off).	

12.9 ME_PM_6: S3/CM3 to S3/CM-Off (with Intel® ME Wake)

ID:	ME_PM_6.1	
Title:	S3/CM3 to S3/CM3-PG via Intel® AMT idle timeout (AC+DC, AC-only/PP2/LP3)	
Requirement:	Mandatory	Exemptions <input checked="" type="checkbox"/> Modern Standby and InstantGo* systems
Method:	Automated by Intel® PETS	
Objective:	This test checks the SUT power flow from S3/CM3 to S3/CM-Off via Intel® AMT idle timeout with the parameters outlined below.	
Configuration:	Intel® AMT should be provisioned via manual mode. This test assumes that either LAN-only, WLAN-only, or both LAN and WLAN network interfaces are available on the SUT.	
Parameters:	System Power Source	AC+DC or AC-only
	Power States	Initial S3/MeOn (CM3)
		Final S3/CM3-PG
		Trigger Intel® AMT idle timeout
	Intel® AMT	Power Package PP2 (Intel® ME on in S0, wake in Sx/AC)
		WLAN Link Policy LP3 (Enabled in S0, Sx/AC) where available



ID:	ME_PM_6.1
Setup:	<ol style="list-style-type: none"> 1. Set the SUT power source to AC+DC where supported; otherwise AC-only. 2. Bring the SUT to the base state of S0/MeOn (CM0,CM0-PG), and confirm that the Host OS is available. 3. Set the active power package on the SUT to Power Package 2 (Intel® ME on in S0, wake in Sx/AC). 4. Set the Intel® AMT WLAN link policy on the SUT to Link Policy 3 (Enabled in S0, Sx/AC), if the WLAN network interface is available. 5. Ensure the Intel® AMT idle timeout on the SUT is set to 1 minute. 6. Ensure that the Host OS network device drivers are configured to not wake the SUT. This includes enabling ARP and/or NS Offload features where available to help prevent unexpected host wake events. Most especially, ensure that the Host OS Wireless Wake on LAN driver setting on the SUT is disabled, if the WLAN network interface is available. 7. Ensure that Intel® RMT is disabled, if running on a Desktop or All-in-One (AIO) SUT with feature support. 8. Verify that Intel® AMT on the SUT responds to version queries via all available network interfaces. 9. Suspend the SUT via the Host OS. 10. Verify that the SUT is in S3/MeOn (CM3). 11. Verify that Intel® AMT on the SUT responds to version queries via all available network interfaces.
Procedure:	<ol style="list-style-type: none"> 1. Wait for 3 minutes to allow the Intel® ME on the SUT to move to CM3-PG after Intel® AMT idle timeout. 2. Verify that the SUT is in S3/CM3-PG.
Pass Criteria:	The test passes if the SUT remains in S3, and the Intel® CSME moves to CM3-PG.

ID:	ME_PM_6.21	
Title:	S3/CM3 to S3/CM3-PG via Intel® AMT idle timeout (AC+DC, AC-only/PP2/LP2)	
Requirement:	Mandatory	Exemptions <ul style="list-style-type: none"> <input checked="" type="checkbox"/> Modern Standby and InstantGo* systems <input checked="" type="checkbox"/> Systems with a single network interface (not LAN+WLAN)
Method:	Automated by Intel® PETS	
Objective:	This test checks the SUT power flow from S3/CM3 to S3/CM-Off via Intel® AMT idle timeout with the parameters outlined below.	
Configuration:	Intel® AMT should be provisioned via manual mode. This test assumes that both LAN and WLAN network interfaces are available on the SUT.	
Parameters:	System Power Source	
	Power States	Initial S3/MeOn (CM3)
		Final S3/CM3-PG
		Trigger Intel® AMT idle timeout
	Intel® AMT	Power Package PP2 (Intel® ME on in S0, wake in Sx/AC)
		WLAN Link Policy LP2 (Enabled in S0)



ID:	ME_PM_6.21
Setup:	<ol style="list-style-type: none"> 1. Set the SUT power source to AC+DC where supported; otherwise AC-only. 2. Bring the SUT to the base state of S0/MeOn (CM0), and confirm that the Host OS is available. 3. Set the active power package on the SUT to Power Package 2 (Intel® ME on in S0, wake in Sx/AC). 4. Set the Intel® AMT WLAN link policy on the SUT to Link Policy 2 (Enabled in S0). 5. Ensure the Intel® AMT idle timeout on the SUT is set to 1 minute. 6. Ensure that the Host OS network device drivers are configured to not wake the SUT. This includes enabling ARP and/or NS Offload features where available to help prevent unexpected host wake events. Most especially, ensure that the Host OS Wireless Wake on LAN driver setting on the SUT is disabled. 7. Ensure that Intel® RMT is disabled, if running on a Desktop or All-in-One (AIO) SUT with feature support. 8. Verify that Intel® AMT on the SUT responds to version queries via all available network interfaces. 9. Suspend the SUT via the Host OS. 10. Verify that the SUT is in S3/MeOn (CM3). 11. Verify that Intel® AMT on the SUT responds to version query via the LAN network interface. 12. Verify that Intel® AMT on the SUT does not respond to version query via the WLAN network interface.
Procedure:	<ol style="list-style-type: none"> 1. Wait for 3 minutes to allow the Intel® ME on the SUT to move to CM3-PG after Intel® AMT idle timeout. 2. Verify that the SUT is in S3/CM3-PG.
Pass Criteria:	The test passes if the SUT remains in S3, and the Intel® CSME moves to CM3-PG.

12.10 ME_PM_7: S3/CM-Off to S3/CM3

ID:	ME_PM_7.1		
Title:	S3/CM3-PG to S3/CM3 via Intel® AMT network access (AC+DC, AC-only/PP2/LP3)		
Requirement:	Mandatory	Exemptions	<input checked="" type="checkbox"/> Modern Standby and InstantGo* systems
Method:	Automated by Intel® PETS		
Objective:	This test checks the SUT power flow from S3/CM3-PG to S3/CM3 via Intel® AMT network access with the parameters outlined below.		
Configuration:	Intel® AMT should be provisioned via manual mode. This test assumes that either LAN-only, WLAN-only, or both LAN and WLAN network interfaces are available on the SUT. Where both network interfaces are available, LAN is the initial active network interface in the test, and WLAN is the secondary network interface.		
Parameters:	System Power Source		AC+DC or AC-only
	Power States	Initial	S3/CM3-PG
		Final	S3/MeOn (CM3)
		Trigger	Intel® AMT network access
	Intel® AMT	Power Package	PP2 (Intel® ME on in S0, wake in Sx/AC)
		WLAN Link Policy	LP3 (Enabled in S0, Sx/AC) where available



ID:	ME_PM_7.1
Setup:	<ol style="list-style-type: none"> 1. Set the SUT power source to AC+DC where supported; otherwise AC-only. 2. Bring the SUT to the base state of S0/MeOn (CM0,CM0-PG), and confirm that the Host OS is available. 3. Set the active power package on the SUT to Power Package 2 (Intel® ME on in S0, wake in Sx/AC). 4. Set the Intel® AMT WLAN link policy on the SUT to Link Policy 3 (Enabled in S0, Sx/AC), if the WLAN network interface is available. 5. Ensure the Intel® AMT idle timeout on the SUT is set to 1 minute. 6. Ensure that the Host OS network device drivers are configured to not wake the SUT. This includes enabling ARP and/or NS Offload features where available to help prevent unexpected host wake events. Most especially, ensure that the Host OS Wireless Wake on LAN driver setting on the SUT is disabled, if the WLAN network interface is available. 7. Ensure that Intel® RMT is disabled, if running on a Desktop or All-in-One (AIO) SUT with feature support. 8. Verify that Intel® AMT on the SUT responds to version queries via all available network interfaces. 9. Suspend the SUT via the Host OS. 10. Verify that the SUT is in S3/MeOn (CM3). 11. Verify that Intel® AMT on the SUT responds to version queries via all available network interfaces.
Procedure:	<ol style="list-style-type: none"> 1. Wait for 3 minutes to allow the Intel® ME on the SUT to move to CM3-PG after Intel® AMT idle timeout. 2. Verify that the Intel® ME on the SUT is in CM3-PG. 3. Verify that Intel® AMT on the SUT responds to version query by means of the active network interface. 4. Verify that the Intel® ME on the SUT is on. <p>If both LAN and WLAN network interfaces are available, repeat this test procedure with the WLAN interface set as the active network interface.</p>
Pass Criteria:	<p>The test passes if:</p> <ul style="list-style-type: none"> • Intel® AMT responds to version queries via all available network interfaces. • the SUT remains in S3. • the Intel® CSME moves to MeOn (CM3).

ID:	ME_PM_7.2		
Title:	S3/CM3-PG with AC Wake to S3/CM3 via AC-attach (DC-only/PP2/LP3)		
Requirement:	Mandatory	Exemptions	<input checked="" type="checkbox"/> Non-Mobile (AC-only) systems <input checked="" type="checkbox"/> Modern Standby and InstantGo* systems
Method:	Automated by Intel® PETS		
Objective:	This test checks the SUT power flow from S3/CM3-PG with Ac Wake to S3/CM3 via AC-attach with the parameters outlined below.		
Configuration:	This test assumes that either LAN-only, WLAN-only, or both LAN and WLAN network interfaces are available on the SUT.		
Parameters:	System Power Source		DC-only
	Power States	Initial	S3/CM3-PG with AC Wake
		Final	S3/MeOn (CM3)
		Trigger	AC-attach
	Intel® AMT	Power Package	PP2 (Intel® ME on in S0, wake in Sx/AC)
		WLAN Link Policy	LP3 (Enabled in S0, Sx/AC) where available



ID:	ME_PM_7.2
Setup:	<ol style="list-style-type: none"> 1. Set the SUT power source to AC+DC. 2. Bring the SUT to the base state of S0/MeOn (CM0,CM0-PG), and confirm that the Host OS is available. 3. Verify that a DC battery is connected to the SUT, and that it is charged. 4. Set the SUT power source to DC-only. 5. Set the active power package on the SUT to Power Package 2 (Intel® ME on in S0, wake in Sx/AC). 6. Set the Intel® AMT WLAN link policy on the SUT to Link Policy 3 (Enabled in S0, Sx/AC), if the WLAN network interface is available. 7. Ensure that the Host OS network device drivers are configured to not wake the SUT. This includes enabling ARP and/or NS Offload features where available to help prevent unexpected host wake events. Most especially, ensure that the Host OS Wireless Wake on LAN driver setting on the SUT is disabled, if the WLAN network interface is available. 8. Ensure that Intel® RMT is disabled, if running on an All-in-One (AIO) SUT with feature support. 9. Verify that Intel® AMT on the SUT responds to version queries via all available network interfaces. 10. Suspend the SUT via the Host OS. 11. Verify that the SUT is in S3/(CM3-PG) with AC Wake
Procedure:	<ol style="list-style-type: none"> 1. Set the SUT power source to AC+DC. 2. Verify that Intel® AMT on the SUT responds to version queries via all available network interfaces. 3. Verify that the SUT is in S3/MeOn (CM3).
Pass Criteria:	<p>The test passes if:</p> <ul style="list-style-type: none"> • the SUT remains in S3. • the Intel® CSME moves to MeOn (CM3). • Intel® AMT responds to version queries via all available network interfaces.

ID:	ME_PM_7.21		
Title:	S3/CM3-PG to S3/CM3 via Intel® AMT network access (AC+DC, AC-only/PP2/LP2)		
Requirement:	Mandatory	Exemptions	<div><input checked="" type="checkbox"/> Modern Standby and InstantGo* systems</div> <div><input checked="" type="checkbox"/> Systems with a single network interface (not LAN+WLAN)</div>
Method:	Automated by Intel® PETS		
Objective:	This test checks the SUT power flow from S3/CM-Off to S3/CM3 via Intel® AMT network access with the parameters outlined below.		
Configuration:	Intel® AMT should be provisioned via manual mode. This test assumes that both LAN and WLAN network interfaces are available on the SUT.		
Parameters:	System Power Source		AC+DC or AC-only
	Power States	Initial	S3/CM3-PG
		Final	S3/MeOn (CM3)
		Trigger	Intel® AMT network access
	Intel® AMT	Power Package	PP2 (Intel® ME on in S0, wake in Sx/AC)
WLAN Link Policy		LP2 (Enabled in S0)	



ID:	ME_PM_7.21
Setup:	<ol style="list-style-type: none"> 1. Set the SUT power source to AC+DC where supported; otherwise AC-only. 2. Bring the SUT to the base state of S0/MeOn (CM0), and confirm that the Host OS is available. 3. Set the active power package on the SUT to Power Package 2 (Intel® ME on in S0, wake in Sx/AC). 4. Set the Intel® AMT WLAN link policy on the SUT to Link Policy 2 (Enabled in S0). 5. Ensure the Intel® AMT idle timeout on the SUT is set to 1 minute. 6. Ensure that the Host OS network device drivers are configured to not wake the SUT. This includes enabling ARP and/or NS Offload features where available to help prevent unexpected host wake events. Most especially, ensure that the Host OS Wireless Wake on LAN driver setting on the SUT is disabled. 7. Ensure that Intel® RMT is disabled, if running on a Desktop or All-in-One (AIO) SUT with feature support. 8. Verify that Intel® AMT on the SUT responds to version queries via all available network interfaces. 9. Suspend the SUT via the Host OS. 10. Verify that the SUT is in S3/MeOn (CM3). 11. Verify that Intel® AMT on the SUT responds to version query via the LAN network interface. 12. Verify that Intel® AMT on the SUT does not respond to version query via the WLAN network interface.
Procedure:	<ol style="list-style-type: none"> 1. Wait for 3 minutes to allow the Intel® ME on the SUT to move to CM3-PG after Intel® AMT idle timeout. 2. Verify that the Intel® ME on the SUT is in CM3-PG. 3. Verify that Intel® AMT on the SUT responds to version query via the LAN network interface. 4. Verify that Intel® AMT on the SUT does not respond to version query via the WLAN network interface. 5. Verify that the Intel® ME on the SUT is on.
Pass Criteria:	<p>The test passes if:</p> <ul style="list-style-type: none"> • the SUT remains in S3. • the Intel® CSME moves to MeOn (CM3). • when in S3: <ul style="list-style-type: none"> – Intel® AMT on the SUT does respond to version queries via the LAN network interface. – Intel® AMT on the SUT does not respond to version queries the WLAN network interface.

ID:	ME_PM_7.22		
Title:	S3/CM3-PG with AC wake to S3/CM3 via AC-attach (DC-only/PP2/LP2)		
Requirement:	Mandatory	Exemptions	<div><input checked="" type="checkbox"/> Non-Mobile (AC-only) systems</div> <div><input checked="" type="checkbox"/> Modern Standby and InstantGo* systems</div> <div><input checked="" type="checkbox"/> Systems with a LAN-only network interface</div>
Method:	Automated by Intel® PETS		
Objective:	This test checks the SUT power flow from S3/CM3-PG with AC Wake to S3/CM3 via AC-attach with the parameters outlined below.		
Configuration:	This test assumes that either WLAN-only, or both LAN and WLAN network interfaces are available on the SUT.		
Parameters:	System Power Source		DC-only
	Power States	Initial	S3/CM3-PG
		Final	S3/MeOn (CM3)
		Trigger	AC-attach
	Intel® AMT	Power Package	PP2 (Intel® ME on in S0, wake in Sx/AC)
		WLAN Link Policy	LP2 (Enabled in S0)



ID:	ME_PM_7.22
Setup:	<ol style="list-style-type: none"> 1. Set the SUT power source to AC+DC. 2. Bring the SUT to the base state of S0/MeOn (CM0,CM0-PG), and confirm that the Host OS is available. 3. Verify that a DC battery is connected to the SUT, and that it is charged. 4. Set the SUT power source to DC-only. 5. Set the active power package on the SUT to Power Package 2 (Intel® ME on in S0, wake in Sx/AC). 6. Set the Intel® AMT WLAN link policy on the SUT to Link Policy 2 (Enabled in S0). 7. Ensure that the Host OS network device drivers are configured to not wake the SUT. This includes enabling ARP and/or NS Offload features where available to help prevent unexpected host wake events. Most especially, ensure that the Host OS Wireless Wake on LAN driver setting on the SUT is disabled. 8. Ensure that Intel® RMT is disabled, if running on an All-in-One (AIO) SUT with feature support. 9. Verify that Intel® AMT on the SUT responds to version queries via all available network interfaces. 10. Suspend the SUT via the Host OS. 11. Verify that the SUT is in S3/(CM3-PG) with AC Wake.
Procedure:	<ol style="list-style-type: none"> 1. Set the SUT power source to AC+DC. 2. Verify that Intel® AMT on the SUT responds to version query via the LAN network interface, if available. 3. Verify that the SUT is in S3/MeOn (CM3). 4. Verify that Intel® AMT on the SUT does not respond to version query via the WLAN network interface.
Pass Criteria:	<p>The test passes if:</p> <ul style="list-style-type: none"> • the SUT remains in S3. • the Intel® CSME moves to MeOn (CM3). • when in S3: <ul style="list-style-type: none"> — Intel® AMT on the SUT does respond to version queries via the LAN network interface, if available. — Intel® AMT on the SUT does not respond to version queries the WLAN network interface.

12.11 ME_PM_8: S0/CM0 to S4/CM-Off or S5/CM-Off

ID:	ME_PM_8.1		
Title:	S0/CM0 to S4/CM-Off via Host OS hibernate (DC-only/PP1/LP3)		
Requirement:	Mandatory	Exemptions	<input checked="" type="checkbox"/> Non-Mobile (AC-only) systems
Method:	Automated by Intel® PETS		
Objective:	This test checks the SUT power flow from S0/CM0 to S4/CM-Off via Host OS hibernate with the parameters outlined below.		
Configuration:	<p>Intel® AMT should be provisioned via manual mode.</p> <p>If Deep S4, Deep S5, and/or G3 are supported on the SUT, please confirm the following:</p> <ul style="list-style-type: none">the SUT and/or BIOS are properly configured to permit Deep S4/S5 or G3 entry.the correct Deep Sx policy is applied to the SUT profile in Intel® PETS. <p>This test assumes that either LAN-only, WLAN-only, or both LAN and WLAN network interfaces are available on the SUT.</p>		
Parameters:	System Power Source		DC-only
	Power States	Initial	S0/MeOn (CM0, CM0-PG)
		Final	S4, S5, Deep S4, Deep S5, G3/MeOff (CM-Off)
		Trigger	Host OS hibernate
	Intel® AMT	Power Package	PP1 (Intel® ME on in S0)
		WLAN Link Policy	LP3 (Enabled in S0, Sx/AC) where available



ID:	ME_PM_8.1
Setup:	<ol style="list-style-type: none"> 1. Set the SUT power source to AC+DC. 2. Bring the SUT to the base state of S0/MeOn (CM0,CM0-PG), and confirm that the Host OS is available. 3. Verify that a DC battery is connected to the SUT, and that it is charged. 4. Set the SUT power source to DC-only. 5. Set the active power package on the SUT to Power Package 1 (Intel® ME on in S0). 6. Set the Intel® AMT WLAN link policy on the SUT to Link Policy 3 (Enabled in S0, Sx/AC), if the WLAN network interface is available. 7. Ensure that the Host OS network device drivers are configured to not wake the SUT. This includes enabling ARP and/or NS Offload features where available to help prevent unexpected host wake events. 8. Verify that Intel® AMT on the SUT responds to version queries via all available network interfaces.
Procedure:	<ol style="list-style-type: none"> 1. Hibernate the SUT via the Host OS. 2. Verify that the SUT is in S4, S5, Deep S4, Deep S5, G3/MeOff (CM-Off).
Pass Criteria:	The test passes if the SUT moves to S4, S5, Deep S4, Deep S5, or G3, and the Intel® CSME moves to MeOff (CM-Off).

ID:	ME_PM_8.2		
Title:	S0/CM0 to S4/CM-Off via Host OS hibernate (AC+DC, AC-only/PP1/LP3)		
Requirement:	Mandatory	Exemptions	None
Method:	Automated by Intel® PETS		
Objective:	This test checks the SUT power flow from S0/CM0 to S4/CM-Off via Host OS hibernate with the parameters outlined below.		
Configuration:	<p>Intel® AMT should be provisioned via manual mode.</p> <p>If Deep S4, Deep S5, and/or G3 are supported on the SUT, please confirm the following:</p> <ul style="list-style-type: none">the SUT and/or BIOS are properly configured to permit Deep S4/S5 or G3 entry.the correct Deep Sx policy is applied to the SUT profile in Intel® PETS. <p>This test assumes that either LAN-only, WLAN-only, or both LAN and WLAN network interfaces are available on the SUT.</p>		
Parameters:	System Power Source		AC+DC or AC-only
	Power States	Initial	S0/MeOn (CM0, CM0-PG)
		Final	S4, S5, Deep S4, Deep S5, G3/MeOff (CM-Off)
		Trigger	Host OS hibernate
	Intel® AMT	Power Package	PP1 (Intel® ME on in S0)
		WLAN Link Policy	LP3 (Enabled in S0, Sx/AC) where available
Setup:	<ol style="list-style-type: none">Set the SUT power source to AC+DC where supported; otherwise AC-only.Bring the SUT to the base state of S0/MeOn (CM0,CM0-PG), and confirm that the Host OS is available.Set the active power package on the SUT to Power Package 1 (Intel® ME on in S0).Set the Intel® AMT WLAN link policy on the SUT to Link Policy 3 (Enabled in S0, Sx/AC), if the WLAN network interface is available.Ensure that the Host OS network device drivers are configured to not wake the SUT. This includes enabling ARP and/or NS Offload features where available to help prevent unexpected host wake events.Verify that Intel® AMT on the SUT responds to version queries via all available network interfaces.		
Procedure:	<ol style="list-style-type: none">Hibernate the SUT via the Host OS.Verify that the SUT is in S4, S5, Deep S4, Deep S5, G3/MeOff (CM-Off).		
Pass Criteria:	The test passes if the SUT moves to S4, S5, Deep S4, Deep S5, or G3, and the Intel® CSME moves to MeOff (CM-Off).		

ID:	ME_PM_8.3
Title:	S0/CM0 to S5/CM-Off via Host OS shutdown (DC-only/PP1/LP3)
Requirement:	Mandatory Exemptions <input checked="" type="checkbox"/> Non-Mobile (AC-only) systems



ID:	ME_PM_8.3		
Method:	Automated by Intel® PETS		
Objective:	This test checks the SUT power flow from S0/CM0 to S5/CM-Off via Host OS shutdown with the parameters outlined below.		
Configuration:	<p>Intel® AMT should be provisioned via manual mode.</p> <p>If Deep S5 and/or G3 are supported on the SUT, please confirm the following:</p> <ul style="list-style-type: none">the SUT and/or BIOS are properly configured to permit Deep S5 or G3 entry.the correct Deep Sx policy is applied to the SUT profile in Intel® PETS. <p>This test assumes that either LAN-only, WLAN-only, or both LAN and WLAN network interfaces are available on the SUT.</p>		
Parameters:	System Power Source		DC-only
	Power States	Initial	S0/MeOn (CM0, CM0-PG)
		Final	S5, Deep S5, G3/MeOff (CM-Off)
		Trigger	Host OS shutdown
	Intel® AMT	Power Package	PP1 (Intel® ME on in S0)
WLAN Link Policy		LP3 (Enabled in S0, Sx/AC) where available	
Setup:	<ol style="list-style-type: none">Set the SUT power source to AC+DC.Bring the SUT to the base state of S0/MeOn (CM0,CM0-PG), and confirm that the Host OS is available.Verify that a DC battery is connected to the SUT, and that it is charged.Set the SUT power source to DC-only.Set the active power package on the SUT to Power Package 1 (Intel® ME on in S0).Set the Intel® AMT WLAN link policy on the SUT to Link Policy 3 (Enabled in S0, Sx/AC), if the WLAN network interface is available.Ensure that the Host OS network device drivers are configured to not wake the SUT. This includes enabling ARP and/or NS Offload features where available to help prevent unexpected host wake events.Verify that Intel® AMT on the SUT responds to version queries via all available network interfaces.		
Procedure:	<ol style="list-style-type: none">Shutdown the SUT via the Host OS.Verify that the SUT is in S5, Deep S5, G3/MeOff (CM-Off).		
Pass Criteria:	The test passes if the SUT moves to S5 (or Deep S5 or G3), and the Intel® CSME moves to MeOff (CM-Off).		

ID:	ME_PM_8.4		
Title:	S0/CM0 to S5/CM-Off via Host OS shutdown (AC+DC, AC-only/PP1/LP3)		
Requirement:	Mandatory	Exemptions	None
Method:	Automated by Intel® PETS		
Objective:	This test checks the SUT power flow from S0/CM0 to S5/CM-Off via Host OS shutdown with the parameters outlined below.		
Configuration:	Intel® AMT should be provisioned via manual mode. If Deep S5 and/or G3 are supported on the SUT, please confirm the following: <ul style="list-style-type: none">the SUT and/or BIOS are properly configured to permit Deep S5 or G3 entry.the correct Deep Sx policy is applied to the SUT profile in Intel® PETS. This test assumes that either LAN-only, WLAN-only, or both LAN and WLAN network interfaces are available on the SUT.		
Parameters:	System Power Source		AC+DC or AC-only
	Power States	Initial	S0/MeOn (CM0, CM0-PG)
		Final	S5, Deep S5, G3/MeOff (CM-Off)
		Trigger	Host OS shutdown
	Intel® AMT	Power Package	PP1 (Intel® ME on in S0)
		WLAN Link Policy	LP3 (Enabled in S0, Sx/AC) where available



ID:	ME_PM_8.4
Setup:	<ol style="list-style-type: none"> 1. Set the SUT power source to AC+DC where supported; otherwise AC-only. 2. Bring the SUT to the base state of S0/MeOn (CM0,CM0-PG), and confirm that the Host OS is available. 3. Set the active power package on the SUT to Power Package 1 (Intel® ME on in S0). 4. Set the Intel® AMT WLAN link policy on the SUT to Link Policy 3 (Enabled in S0, Sx/AC), if the WLAN network interface is available. 5. Ensure that the Host OS network device drivers are configured to not wake the SUT. This includes enabling ARP and/or NS Offload features where available to help prevent unexpected host wake events. 6. Verify that Intel® AMT on the SUT responds to version queries via all available network interfaces.
Procedure:	<ol style="list-style-type: none"> 1. Shutdown the SUT via the Host OS. 2. Verify that the SUT is in S5, Deep S5, G3/MeOff (CM-Off).
Pass Criteria:	The test passes if the SUT moves to S5 (or Deep S5 or G3), and the Intel® CSME moves to MeOff (CM-Off).

ID:	ME_PM_8.5		
Title:	S0/CM0 to S4/CM3-PG with AC Wake via Host OS hibernate (DC-only/PP2/LP3)		
Requirement:	Mandatory	Exemptions	<input checked="" type="checkbox"/> Non-Mobile (AC-only) systems
Method:	Automated by Intel® PETS		
Objective:	This test checks the SUT power flow from S0/CM0 to S4/CM3-PG with AC Wake via Host OS hibernate with the parameters outlined below.		
Configuration:	<p>Intel® AMT should be provisioned via manual mode.</p> <p>If Deep S4, Deep S5, and/or G3 are supported on the SUT, please confirm the following:</p> <ul style="list-style-type: none">the SUT and/or BIOS are properly configured to permit Deep S4/S5 or G3 entry.the correct Deep Sx policy is applied to the SUT profile in Intel® PETS. <p>This test assumes that either LAN-only, WLAN-only, or both LAN and WLAN network interfaces are available on the SUT.</p>		
Parameters:	System Power Source		DC-only
	Power States	Initial	S0/MeOn (CM0, CM0-PG)
		Final	S4,S5,Deep S4,Deep S5,G3/CM3-PG with AC wake
		Trigger	Host OS hibernate
	Intel® AMT	Power Package	PP2 (Intel® ME on in S0, wake in Sx/AC)
		WLAN Link Policy	LP3 (Enabled in S0, Sx/AC) where available
Setup:	<ol style="list-style-type: none">Set the SUT power source to AC+DC.Bring the SUT to the base state of S0/MeOn (CM0,CM0-PG), and confirm that the Host OS is available.Verify that a DC battery is connected to the SUT, and that it is charged.Set the SUT power source to DC-only.Set the active power package on the SUT to Power Package 2 (Intel® ME on in S0, wake in Sx/AC).Set the Intel® AMT WLAN link policy on the SUT to Link Policy 3 (Enabled in S0, Sx/AC), if the WLAN network interface is available.Ensure that the Host OS network device drivers are configured to not wake the SUT. This includes enabling ARP and/or NS Offload features where available to help prevent unexpected host wake events.Verify that Intel® AMT on the SUT responds to version queries via all available network interfaces.		
Procedure:	<ol style="list-style-type: none">Hibernate the SUT via the Host OS.Verify that the SUT is in S4 , S5, Deep S4, Deep S5, G3/CM3-PG.with AC Wake		
Pass Criteria:	The test passes if the SUT moves to S4, S5, Deep S4, Deep S5, or G3, and the Intel® CSME moves to CM3-PG with Ac Wake.		

ID:	ME_PM_8.6
Title:	S0/CM0 to S5/CM3-PG with AC Wake via Host OS shutdown (DC-only/PP2/LP3)
Requirement:	Mandatory Exemptions <input checked="" type="checkbox"/> Non-Mobile (AC-only) systems



ID:	ME_PM_8.6		
Method:	Automated by Intel® PETS		
Objective:	This test checks the SUT power flow from S0/CM0 to S5/CM3-PG with Ac Wake via Host OS shutdown with the parameters outlined below.		
Configuration:	<p>Intel® AMT should be provisioned via manual mode.</p> <p>If Deep S4, Deep S5, and/or G3 are supported on the SUT, please confirm the following:</p> <ul style="list-style-type: none"> the SUT and/or BIOS are properly configured to permit Deep S4/S5 or G3 entry. the correct Deep Sx policy is applied to the SUT profile in Intel® PETS. <p>This test assumes that either LAN-only, WLAN-only, or both LAN and WLAN network interfaces are available on the SUT.</p>		
Parameters:	System Power Source		DC-only
	Power States	Initial	S0/MeOn (CM0, CM0-PG)
		Final	S5, Deep S5, G3/CM3-PG with Ac Wake
		Trigger	Host OS shutdown
	Intel® AMT	Power Package	PP2 (Intel® ME on in S0, wake in Sx/AC)
		WLAN Link Policy	LP3 (Enabled in S0, Sx/AC) where available
Setup:	<ol style="list-style-type: none"> Set the SUT power source to AC+DC. Bring the SUT to the base state of S0/MeOn (CM0, CM0-PG), and confirm that the Host OS is available. Verify that a DC battery is connected to the SUT, and that it is charged. Set the SUT power source to DC-only. Set the active power package on the SUT to Power Package 2 (Intel® ME on in S0, wake in Sx/AC). Set the Intel® AMT WLAN link policy on the SUT to Link Policy 3 (Enabled in S0, Sx/AC), if the WLAN network interface is available. Ensure that the Host OS network device drivers are configured to not wake the SUT. This includes enabling ARP and/or NS Offload features where available to help prevent unexpected host wake events. Verify that Intel® AMT on the SUT responds to version queries via all available network interfaces. 		
Procedure:	<ol style="list-style-type: none"> Shutdown the SUT via the Host OS. Verify that the SUT is in S5, Deep S5, G3/CM3-PG. with Ac Wake 		
Pass Criteria:	The test passes if the SUT moves to S5 (or Deep S5 or G3), and the Intel® CSME moves to CM3-PG with AC Wake.		

12.12 ME_PM_9: G3 or S4/CM-Off or S5/CM-Off (Suspend Well Off) to S0/CM0

ID:	ME_PM_9.1		
Title:	S4/CM-Off to S0/CM0 via Power Button press (DC-only/PP1/LP3)		
Requirement:	Mandatory	Exemptions	<input checked="" type="checkbox"/> Non-Mobile (AC-only) systems
Method:	Automated by Intel® PETS		
Objective:	This test checks the SUT power flow from S4/CM-Off to S0/CM0 via Power Button press with the parameters outlined below.		
Configuration:	<p>Intel® AMT should be provisioned via manual mode.</p> <p>If Deep S4, Deep S5, and/or G3 are supported on the SUT, please confirm the following:</p> <ul style="list-style-type: none"> the SUT and/or BIOS are properly configured to permit Deep S4/S5 or G3 entry. the correct Deep Sx policy is applied to the SUT profile in Intel® PETS. <p>This test assumes that either LAN-only, WLAN-only, or both LAN and WLAN network interfaces are available on the SUT.</p>		



ID:	ME_PM_9.1		
Parameters:	System Power Source		DC-only
	Power States	Initial	S4, S5, Deep S4, Deep S5, G3/MeOff (CM-Off)
		Final	S0/MeOn (CM0, CM0-PG)
		Trigger	Power Button press
	Intel® AMT	Power Package	PP1 (Intel® ME on in S0)
WLAN Link Policy		LP3 (Enabled in S0, Sx/AC) where available	
Setup:	<div>1. Set the SUT power source to AC+DC.</div> <div>2. Bring the SUT to the base state of S0/MeOn (CM0,CM0-PG), and confirm that the Host OS is available.</div> <div>3. Verify that a DC battery is connected to the SUT, and that it is charged.</div> <div>4. Set the SUT power source to DC-only.</div> <div>5. Set the active power package on the SUT to Power Package 1 (Intel® ME on in S0).</div> <div>6. Set the Intel® AMT WLAN link policy on the SUT to Link Policy 3 (Enabled in S0, Sx/AC), if the WLAN network interface is available.</div> <div>7. Ensure that the Host OS network device drivers are configured to not wake the SUT. This includes enabling ARP and/or NS Offload features where available to help prevent unexpected host wake events.</div> <div>8. Verify that Intel® AMT on the SUT responds to version queries via all available network interfaces.</div> <div>9. Ensure yellow bang is not seen on Drivers in Device Manager</div> <div>10. Hibernate the SUT via the Host OS.</div> <div>11. Verify that the SUT is in S4, S5, Deep S4, Deep S5, G3/MeOff (CM-Off).</div>		
Procedure:	<div>1. Briefly press the Power Button on the SUT.</div> <div>2. Verify that the SUT is in S0/MeOn (CM0,CM0-PG).</div> <div>3. Verify that the Host OS on the SUT is available.</div> <div>4. Verify that Intel® AMT on the SUT responds to version queries via all available network interfaces.</div> <div>5. Verify that windows booted from hibernate i.e. value should be 0x02. `run the following power shell command`: Get-WinEvent -ProviderName Microsoft-Windows-Kernel-boot -MaxEvents 10 Where-Object {\$_.message -like "The boot type*"}`</div> <div>6. Verify that the second nibble of the FWSTS2 register on the SUT have a value of 0x60xxxxxx.</div> <div>7. Ensure yellow bang is not seen on Drivers in Device Manager</div>		
Pass Criteria:	<div>The test passes if:</div> <div><ul style="list-style-type: none">the SUT moves from S4, S5, Deep S4, Deep S5, or G3 to S0.the Intel® CSME moves to MeOn (CM0, CM0-PG).Intel® AMT responds to version queries via all available network interfaces.</div>		

ID:	ME_PM_9.2		
Title:	S4/CM-Off to S0/CM0 via Power Button press (AC+DC, AC-only/PP1/LP3)		
Requirement:	Mandatory	Exemptions	None
Method:	Automated by Intel® PETS		
Objective:	This test checks the SUT power flow from S4/CM-Off to S0/CM0 via Power Button press with the parameters outlined below.		
Configuration:	Intel® AMT should be provisioned via manual mode. If Deep S4, Deep S5, and/or G3 are supported on the SUT, please confirm the following: <ul style="list-style-type: none">the SUT and/or BIOS are properly configured to permit Deep S4/S5 or G3 entry.the correct Deep Sx policy is applied to the SUT profile in Intel® PETS. This test assumes that either LAN-only, WLAN-only, or both LAN and WLAN network interfaces are available on the SUT.		
Parameters:	System Power Source		AC+DC or AC-only
	Power States	Initial	S4, S5, Deep S4, Deep S5, G3/MeOff (CM-Off)
		Final	S0/MeOn (CM0, CM0-PG)
		Trigger	Power Button press
	Intel® AMT	Power Package	PP1 (Intel® ME on in S0)
		WLAN Link Policy	LP3 (Enabled in S0, Sx/AC) where available



ID:	ME_PM_9.2
Setup:	<ol style="list-style-type: none"> 1. Set the SUT power source to AC+DC where supported; otherwise AC-only. 2. Bring the SUT to the base state of S0/MeOn (CM0,CM0-PG), and confirm that the Host OS is available. 3. Set the active power package on the SUT to Power Package 1 (Intel® ME on in S0). 4. Set the Intel® AMT WLAN link policy on the SUT to Link Policy 3 (Enabled in S0, Sx/AC), if the WLAN network interface is available. 5. Ensure that the Host OS network device drivers are configured to not wake the SUT. This includes enabling ARP and/or NS Offload features where available to help prevent unexpected host wake events. 6. Verify that Intel® AMT on the SUT responds to version queries via all available network interfaces. 7. Ensure yellow bang is not seen on Drivers in Device Manager 8. Hibernate the SUT via the Host OS. 9. Verify that the SUT is in S4, S5, Deep S4, Deep S5, G3/MeOff (CM-Off).
Procedure:	<ol style="list-style-type: none"> 1. Briefly press the Power Button on the SUT. 2. Verify that the SUT is in S0/MeOn (CM0,CM0-PG). 3. Verify that the Host OS on the SUT is available. 4. Verify that Intel® AMT on the SUT responds to version queries via all available network interfaces. 5. Verify that windows booted from hibernate i.e. value should be 0x02. "run the following power shell command": Get-WinEvent -ProviderName Microsoft-Windows-Kernel-boot -MaxEvents 10 Where-Object {\$_.message -like "The boot type*"} 6. Verify that the second nibble of the FWSTS2 register on the SUT have a value of 0x60xxxxx. 7. Ensure yellow bang is not seen on Drivers in Device Manager
Pass Criteria:	<p>The test passes if:</p> <ul style="list-style-type: none"> • the SUT moves from S4, S5, Deep S4, Deep S5, or G3 to S0. • the Intel® CSME moves to MeOn (CM0, CM0-PG). • Intel® AMT responds to version queries via all available network interfaces.

ID:	ME_PM_9.3		
Title:	S4/CM3-PG with AC wake to S0/CM0 via Power Button press (DC-only/PP2/LP3)		
Requirement:	Mandatory	Exemptions	<input checked="" type="checkbox"/> Non-Mobile (AC-only) systems
Method:	Automated by Intel® PETS		
Objective:	This test checks the SUT power flow from S4/CM3-PG with AC Wake to S0/CM0 via Power Button press with the parameters outlined below.		
Configuration:	<p>Intel® AMT should be provisioned via manual mode.</p> <p>If Deep S4, Deep S5, and/or G3 are supported on the SUT, please confirm the following:</p> <ul style="list-style-type: none">the SUT and/or BIOS are properly configured to permit Deep S4/S5 or G3 entry.the correct Deep Sx policy is applied to the SUT profile in Intel® PETS. <p>This test assumes that either LAN-only, WLAN-only, or both LAN and WLAN network interfaces are available on the SUT.</p>		
Parameters:	System Power Source		DC-only
	Power States	Initial	S4,S5,Deep S4,Deep S5,G3/CM3-PG with AC Wake
		Final	S0/MeOn (CM0, CM0-PG)
		Trigger	Power Button press
	Intel® AMT	Power Package	PP2 (Intel® ME on in S0, wake in Sx/AC)
WLAN Link Policy		LP3 (Enabled in S0, Sx/AC) where available	



ID:	ME_PM_9.3
Setup:	<ol style="list-style-type: none"> 1. Set the SUT power source to AC+DC. 2. Bring the SUT to the base state of S0/MeOn (CM0,CM0-PG), and confirm that the Host OS is available. 3. Verify that a DC battery is connected to the SUT, and that it is charged. 4. Set the SUT power source to DC-only. 5. Set the active power package on the SUT to Power Package 2 (Intel® ME on in S0, wake in Sx/AC). 6. Set the Intel® AMT WLAN link policy on the SUT to Link Policy 3 (Enabled in S0, Sx/AC), if the WLAN network interface is available. 7. Ensure that the Host OS network device drivers are configured to not wake the SUT. This includes enabling ARP and/or NS Offload features where available to help prevent unexpected host wake events. 8. Verify that Intel® AMT on the SUT responds to version queries via all available network interfaces. 9. Ensure yellow bang is not seen on Drivers in Device Manager 10. Hibernate the SUT via the Host OS. 11. Verify that the SUT is in S4 , S5, Deep S4, Deep S5, G3/CM3-PG.with AC wake.
Procedure:	<ol style="list-style-type: none"> 1. Briefly press the Power Button on the SUT. 2. Verify that the SUT is in S0/MeOn (CM0,CM0-PG). 3. Verify that the Host OS on the SUT is available. 4. Verify that Intel® AMT on the SUT responds to version queries via all available network interfaces. 5. Verify that windows booted from hibernate i.e. value should be 0x02. "run the following power shell command": Get-WinEvent -ProviderName Microsoft-Windows-Kernel-boot -MaxEvents 10 Where-Object {\$_.message -like "The boot type*"} 6. Verify that the second nibble of the FWSTS2 register on the SUT have a value of 0x60xxxxxx. 7. Ensure yellow bang is not seen on Drivers in Device Manager
Pass Criteria:	<p>The test passes if:</p> <ul style="list-style-type: none"> • the SUT moves from S4, S5, Deep S4, Deep S5, or G3 to S0. • the Intel® CSME moves to MeOn (CM0, CM0-PG). • Intel® AMT responds to version queries via all available network interfaces.

ID:	ME_PM_9.4																	
Title:	S5/CM-Off to S0/CM0 via Power Button press (DC-only/PP1/LP3)																	
Requirement:	Mandatory	Exemptions	<input checked="" type="checkbox"/> Non-Mobile (AC-only) systems															
Method:	Automated by Intel® PETS																	
Objective:	This test checks the SUT power flow from S5/CM-Off to S0/CM0 via Power Button press with the parameters outlined below.																	
Configuration:	<p>Intel® AMT should be provisioned via manual mode.</p> <p>If Deep S5 and/or G3 are supported on the SUT, please confirm the following:</p> <ul style="list-style-type: none">the SUT and/or BIOS are properly configured to permit Deep S5 or G3 entry.the correct Deep Sx policy is applied to the SUT profile in Intel® PETS. <p>Confirm that the Host OS is configured to shutdown the SUT upon Power Button press.</p> <p>This test assumes that either LAN-only, WLAN-only, or both LAN and WLAN network interfaces are available on the SUT.</p>																	
Parameters:	<table><tr><td colspan="2">System Power Source</td><td>DC-only</td></tr><tr><td rowspan="3">Power States</td><td>Initial</td><td>S5, Deep S5, G3/MeOff (CM-Off)</td></tr><tr><td>Final</td><td>S0/MeOn (CM0, CM0-PG)</td></tr><tr><td>Trigger</td><td>Power Button press</td></tr><tr><td rowspan="2">Intel® AMT</td><td>Power Package</td><td>PP1 (Intel® ME on in S0)</td></tr><tr><td>WLAN Link Policy</td><td>LP3 (Enabled in S0, Sx/AC) where available</td></tr></table>			System Power Source		DC-only	Power States	Initial	S5, Deep S5, G3/MeOff (CM-Off)	Final	S0/MeOn (CM0, CM0-PG)	Trigger	Power Button press	Intel® AMT	Power Package	PP1 (Intel® ME on in S0)	WLAN Link Policy	LP3 (Enabled in S0, Sx/AC) where available
System Power Source		DC-only																
Power States	Initial	S5, Deep S5, G3/MeOff (CM-Off)																
	Final	S0/MeOn (CM0, CM0-PG)																
	Trigger	Power Button press																
Intel® AMT	Power Package	PP1 (Intel® ME on in S0)																
	WLAN Link Policy	LP3 (Enabled in S0, Sx/AC) where available																



ID:	ME_PM_9.4
Setup:	<ol style="list-style-type: none"> 1. Set the SUT power source to AC+DC. 2. Bring the SUT to the base state of S0/MeOn (CM0,CM0-PG), and confirm that the Host OS is available. 3. Verify that a DC battery is connected to the SUT, and that it is charged. 4. Set the SUT power source to DC-only. 5. Set the active power package on the SUT to Power Package 1 (Intel® ME on in S0). 6. Set the Intel® AMT WLAN link policy on the SUT to Link Policy 3 (Enabled in S0, Sx/AC), if the WLAN network interface is available. 7. Ensure that the Host OS network device drivers are configured to not wake the SUT. This includes enabling ARP and/or NS Offload features where available to help prevent unexpected host wake events. 8. Verify that Intel® AMT on the SUT responds to version queries via all available network interfaces. 9. Ensure yellow bang is not seen on Drivers in Device Manager 10. Shutdown the SUT via the brief Power Button press. 11. Verify that the SUT is in S5, Deep S5, G3/MeOff (CM-Off).
Procedure:	<ol style="list-style-type: none"> 1. Briefly press the Power Button on the SUT. 2. Verify that the SUT is in S0/MeOn (CM0,CM0-PG). 3. Verify that the Host OS on the SUT is available. 4. Verify that Intel® AMT on the SUT responds to version queries via all available network interfaces. 5. Verify that the second nibble of the FWSTS2 register on the SUT have a value of 0x60xxxxxx. 6. Ensure yellow bang is not seen on Drivers in Device Manager
Pass Criteria:	<p>The test passes if:</p> <ul style="list-style-type: none"> • the SUT moves from S5 (or Deep S5 or G3) to S0. • the Intel® CSME moves to MeOn (CM0). • Intel® AMT responds to version queries via all available network interfaces.

ID:	ME_PM_9.5		
Title:	S5/CM-Off to S0/CM0 via Power Button press (AC+DC, AC-only/PP1/LP3)		
Requirement:	Mandatory	Exemptions	None
Method:	Automated by Intel® PETS		
Objective:	This test checks the SUT power flow from S5/CM-Off to S0/CM0 via Power Button press with the parameters outlined below.		
Configuration:	<p>Intel® AMT should be provisioned via manual mode.</p> <p>If Deep S5 and/or G3 are supported on the SUT, please confirm the following:</p> <ul style="list-style-type: none">the SUT and/or BIOS are properly configured to permit Deep S5 or G3 entry.the correct Deep Sx policy is applied to the SUT profile in Intel® PETS. <p>Confirm that the Host OS is configured to shutdown the SUT upon Power Button press.</p> <p>This test assumes that either LAN-only, WLAN-only, or both LAN and WLAN network interfaces are available on the SUT.</p>		
Parameters:	System Power Source		AC+DC or AC-only
	Power States	Initial	S5, Deep S5, G3/MeOff (CM-Off)
		Final	S0/MeOn (CM0, CM0-PG)
		Trigger	Power Button press
	Intel® AMT	Power Package	PP1 (Intel® ME on in S0)
WLAN Link Policy		LP3 (Enabled in S0, Sx/AC) where available	



ID:	ME_PM_9.5
Setup:	<ol style="list-style-type: none"> 1. Set the SUT power source to AC+DC where supported; otherwise AC-only. 2. Bring the SUT to the base state of S0/MeOn (CM0,CM0-PG), and confirm that the Host OS is available. 3. Set the active power package on the SUT to Power Package 1 (Intel® ME on in S0). 4. Set the Intel® AMT WLAN link policy on the SUT to Link Policy 3 (Enabled in S0, Sx/AC), if the WLAN network interface is available. 5. Ensure that the Host OS network device drivers are configured to not wake the SUT. This includes enabling ARP and/or NS Offload features where available to help prevent unexpected host wake events. 6. Verify that Intel® AMT on the SUT responds to version queries via all available network interfaces. 7. Ensure yellow bang is not seen on Drivers in Device Manager 8. Shutdown the SUT via the brief Power Button press. 9. Verify that the SUT is in S5, Deep S5, G3/MeOff (CM-Off).
Procedure:	<ol style="list-style-type: none"> 1. Briefly press the Power Button on the SUT. 2. Verify that the SUT is in S0/MeOn (CM0,CM0-PG). 3. Verify that the Host OS on the SUT is available. 4. Verify that Intel® AMT on the SUT responds to version queries via all available network interfaces. 5. Verify that the second nibble of the FWSTS2 register on the SUT have a value of 0x60xxxxxx. 6. Ensure yellow bang is not seen on Drivers in Device Manager
Pass Criteria:	<p>The test passes if:</p> <ul style="list-style-type: none"> • the SUT moves from S5 (or Deep S5 or G3) to S0. • the Intel® CSME moves to MeOn (CM0, CM0-PG). • Intel® AMT responds to version queries via all available network interfaces.

ID:	ME_PM_9.6	
Title:	S5/CM3-PG with AC wake to S0/CM0 via Power Button press (DC-only/PP2/LP3)	
Requirement:	Mandatory	Exemptions <input checked="" type="checkbox"/> Non-Mobile (AC-only) systems
Method:	Automated by Intel® PETS	
Objective:	This test checks the SUT power flow from S5/CM3-PG with AC Wake to S0/CM0 via Power Button press with the parameters outlined below.	
Configuration:	<p>Intel® AMT should be provisioned via manual mode.</p> <p>If Deep S5 and/or G3 are supported on the SUT, please confirm the following:</p> <ul style="list-style-type: none"> • the SUT and/or BIOS are properly configured to permit Deep S5 or G3 entry. • the correct Deep Sx policy is applied to the SUT profile in Intel® PETS. <p>Confirm that the Host OS is configured to shutdown the SUT upon Power Button press.</p> <p>This test assumes that either LAN-only, WLAN-only, or both LAN and WLAN network interfaces are available on the SUT.</p>	
Parameters:	System Power Source	
	DC-only	
	Power States	Initial S5,Deep S5,G3/CM3-PG with AC Wake
		Final S0/MeOn (CM0, CM0-PG)
		Trigger Power Button press
	Intel® AMT	Power Package PP2 (Intel® ME on in S0, wake in Sx/AC)
		WLAN Link Policy LP3 (Enabled in S0, Sx/AC) where available



ID:	ME_PM_9.6
Setup:	<ol style="list-style-type: none"> 1. Set the SUT power source to AC+DC. 2. Bring the SUT to the base state of S0/MeOn (CM0,CM0-PG), and confirm that the Host OS is available. 3. Verify that a DC battery is connected to the SUT, and that it is charged. 4. Set the SUT power source to DC-only. 5. Set the active power package on the SUT to Power Package 2 (Intel® ME on in S0, wake in Sx/AC). 6. Set the Intel® AMT WLAN link policy on the SUT to Link Policy 3 (Enabled in S0, Sx/AC), if the WLAN network interface is available. 7. Ensure that the Host OS network device drivers are configured to not wake the SUT. This includes enabling ARP and/or NS Offload features where available to help prevent unexpected host wake events. 8. Verify that Intel® AMT on the SUT responds to version queries via all available network interfaces. 9. Ensure yellow bang is not seen on Drivers in Device Manager 10. Shutdown the SUT via the brief Power Button press. 11. Verify that the SUT is in S5, Deep S5, G3/CM3-PG.with AC wake.
Procedure:	<ol style="list-style-type: none"> 1. Briefly press the Power Button on the SUT. 2. Verify that the SUT is in S0/MeOn (CM0,CM0-PG). 3. Verify that the Host OS on the SUT is available. 4. Verify that Intel® AMT on the SUT responds to version queries via all available network interfaces. 5. Verify that the second nibble of the FWSTS2 register on the SUT have a value of 0x60xxxxxx. 6. Ensure yellow bang is not seen on Drivers in Device Manager
Pass Criteria:	<p>The test passes if:</p> <ul style="list-style-type: none"> • the SUT moves from S5 (or Deep S5 or G3) to S0. • the Intel® CSME moves to MeOn (CM0, CM0-PG). • Intel® AMT responds to version queries via all available network interfaces.

ID:	ME_PM_9.7																	
Title:	G3/CM-Off to S0/CM0 via AC-attach (AC+DC, AC-only/PP1/LP3)																	
Requirement:	Optional																	
Method:	Automated by Intel® PETS																	
Objective:	This test checks the SUT power flow from G3/CM-Off to S0/CM0 via AC-attach with the parameters outlined below.																	
Configuration:	<p>Intel® AMT should be provisioned via manual mode.</p> <p>If Deep S5 and/or G3 are supported on the SUT, please confirm the following:</p> <ul style="list-style-type: none">the SUT and/or BIOS are properly configured to permit Deep S5 or G3 entry.the correct Deep Sx policy is applied to the SUT profile in Intel® PETS. <p>Confirm that the BIOS is configured to boot SUT upon AC-attach after G3.</p> <p>Confirm that the Host OS is configured to shutdown the SUT upon Power Button press.</p> <p>This test assumes that either LAN-only, WLAN-only, or both LAN and WLAN network interfaces are available on the SUT.</p>																	
Parameters:	<table><tr><td colspan="2">System Power Source</td><td>AC+DC or AC-only</td></tr><tr><td rowspan="3">Power States</td><td>Initial</td><td>G3/MeOff (CM-Off)</td></tr><tr><td>Final</td><td>S0/MeOn (CM0, CM0-PG)</td></tr><tr><td>Trigger</td><td>AC-attach</td></tr><tr><td rowspan="2">Intel® AMT</td><td>Power Package</td><td>PP1 (Intel® ME on in S0)</td></tr><tr><td>WLAN Link Policy</td><td>LP3 (Enabled in S0, Sx/AC) where available</td></tr></table>			System Power Source		AC+DC or AC-only	Power States	Initial	G3/MeOff (CM-Off)	Final	S0/MeOn (CM0, CM0-PG)	Trigger	AC-attach	Intel® AMT	Power Package	PP1 (Intel® ME on in S0)	WLAN Link Policy	LP3 (Enabled in S0, Sx/AC) where available
System Power Source		AC+DC or AC-only																
Power States	Initial	G3/MeOff (CM-Off)																
	Final	S0/MeOn (CM0, CM0-PG)																
	Trigger	AC-attach																
Intel® AMT	Power Package	PP1 (Intel® ME on in S0)																
	WLAN Link Policy	LP3 (Enabled in S0, Sx/AC) where available																



ID:	ME_PM_9.7
Setup:	<ol style="list-style-type: none"> 1. Set the SUT power source to AC+DC where supported; otherwise AC-only. 2. Bring the SUT to the base state of S0/MeOn (CM0,CM0-PG), and confirm that the Host OS is available. 3. Set the active power package on the SUT to Power Package 1 (Intel® ME on in S0). 4. Set the Intel® AMT WLAN link policy on the SUT to Link Policy 3 (Enabled in S0, Sx/AC), if the WLAN network interface is available. 5. Ensure that the Host OS network device drivers are configured to not wake the SUT. This includes enabling ARP and/or NS Offload features where available to help prevent unexpected host wake events. 6. Verify that Intel® AMT on the SUT responds to version queries via all available network interfaces. 7. Ensure yellow bang is not seen on Drivers in Device Manager 8. Shutdown the SUT via the brief Power Button press. 9. Verify that the SUT is in S5, Deep S5, G3/MeOff (CM-Off). 10. Remove power from the SUT via AC-detach, and if necessary also via DC-detach. Wait for 10 seconds before continuing to allow full power drain from the SUT. 11. Verify that the SUT is in G3/MeOff (CM-Off). 12. Verify that Intel® AMT on the SUT does not respond to version queries via any of the available network interfaces.
Procedure:	<ol style="list-style-type: none"> 1. Set the SUT power source to AC+DC where supported; otherwise AC-only. For systems with DC-power support, consult the system design as it may be preferred to connect DC-power before AC-power. 2. Verify that the SUT is in S0/MeOn (CM0,CM0-PG). 3. Verify that the Host OS on the SUT is available. 4. Verify that Intel® AMT on the SUT responds to version queries via all available network interfaces. 5. Verify that the second nibble of the FWSTS2 register on the SUT have a value of 0x60xxxxxx. 6. Ensure yellow bang is not seen on Drivers in Device Manager
Pass Criteria:	<p>The test passes if:</p> <ul style="list-style-type: none"> • the SUT moves from G3 to S0. • the Intel® CSME moves to MeOn (CM0, CM0-PG). • Intel® AMT responds to version queries via all available network interfaces.

ID:	ME_PM_9.8		
Title:	G3/CM-Off to S0/CM0 via AC-attach (AC+DC, AC-only/PP2/LP3)		
Requirement:	Optional		
Method:	Automated by Intel® PETS		
Objective:	This test checks the SUT power flow from G3/CM-Off to S0/CM0 via AC-attach with the parameters outlined below.		
Configuration:	<p>Intel® AMT should be provisioned via manual mode.</p> <p>Confirm that the BIOS is configured to boot SUT upon AC-attach after G3.</p> <p>This test assumes that either LAN-only, WLAN-only, or both LAN and WLAN network interfaces are available on the SUT.</p>		
Parameters:	System Power Source		AC+DC or AC-only
	Power States	Initial	G3/MeOff (CM-Off)
		Final	S0/MeOn (CM0, CM0-PG)
		Trigger	AC-attach
	Intel® AMT	Power Package	PP2 (Intel® ME on in S0, wake in Sx/AC)
		WLAN Link Policy	LP3 (Enabled in S0, Sx/AC) where available



ID:	ME_PM_9.8
Setup:	<ol style="list-style-type: none"> 1. Set the SUT power source to AC+DC where supported; otherwise AC-only. 2. Bring the SUT to the base state of S0/MeOn (CM0,CM0-PG), and confirm that the Host OS is available. 3. Set the active power package on the SUT to Power Package 2 (Intel® ME on in S0, wake in Sx/AC). 4. Set the Intel® AMT WLAN link policy on the SUT to Link Policy 3 (Enabled in S0, Sx/AC), if the WLAN network interface is available. 5. Ensure that the Host OS network device drivers are configured to not wake the SUT. This includes enabling ARP and/or NS Offload features where available to help prevent unexpected host wake events. 6. Verify that Intel® AMT on the SUT responds to version queries via all available network interfaces. 7. Ensure yellow bang is not seen on Drivers in Device Manager 8. Shutdown the SUT via the Host OS. 9. Verify that the SUT is in S5/MeOn (CM3). 10. Verify that Intel® AMT on the SUT responds to version queries via all available network interfaces. 11. Remove power from the SUT via AC-detach, and if necessary also via DC-detach. Wait for 10 seconds before continuing to allow full power drain from the SUT. 12. Verify that Intel® AMT on the SUT does not respond to version queries via any of the available network interfaces. 13. Verify that the SUT is in G3/MeOff (CM-Off).
Procedure:	<ol style="list-style-type: none"> 1. Set the SUT power source to AC+DC where supported; otherwise AC-only. For systems with DC-power support, consult the system design as it may be preferred to connect DC-power before AC-power. 2. Verify that the SUT is in S0/MeOn (CM0,CM0-PG). 3. Verify that the Host OS on the SUT is available. 4. Verify that Intel® AMT on the SUT responds to version queries via all available network interfaces. 5. Verify that the second nibble of the FWSTS2 register on the SUT have a value of 0x60xxxxxx. 6. Ensure yellow bang is not seen on Drivers in Device Manager
Pass Criteria:	<p>The test passes if:</p> <ul style="list-style-type: none"> • the SUT moves from G3 to S0. • the Intel® CSME moves to MeOn (CM0, CM0-PG). • Intel® AMT responds to version queries via all available network interfaces.

12.13 ME_PM_10: S4/CM-Off or S5/CM-Off (Suspend Well On) to S0/CM0

ID:	ME_PM_10.1
Title:	S4/CM-Off to S0/CM0 via magic packet (AC+DC, AC-only/PP1/LP3)
Requirement:	Mandatory Exemptions <input checked="" type="checkbox"/> Systems without WoL and/or WoWLAN support
Method:	Automated by Intel® PETS
Objective:	This test checks the SUT power flow from S4/CM-Off to S0/CM0 via magic packet with the parameters outlined below.
Configuration:	<p>Intel® AMT should be provisioned via manual mode.</p> <p>If Deep S4, Deep S5, and/or G3 are supported on the SUT, please confirm the following:</p> <ul style="list-style-type: none"> • the SUT and/or BIOS are properly configured to permit Deep S4/S5 or G3 entry. • the correct Deep Sx policy is applied to the SUT profile in Intel® PETS. <p>This test assumes that either LAN-only, WLAN-only, or both LAN and WLAN network interfaces are available on the SUT. Where both network interfaces are available, LAN is the initial active network interface in the test, and WLAN is the secondary network interface.</p>



ID:	ME_PM_10.1		
Parameters:	System Power Source		AC+DC or AC-only
	Power States	Initial	S4, S5, Deep S4, Deep S5, G3/MeOff (CM-Off)
		Final	S0/MeOn (CM0, CM0-PG)
		Trigger	Magic Packet receipt
	Intel® AMT	Power Package	PP1 (Intel® ME on in S0)
WLAN Link Policy		LP3 (Enabled in S0, Sx/AC) where available	
Setup:	<div>1. Set the SUT power source to AC+DC where supported; otherwise AC-only.</div> <div>2. Bring the SUT to the base state of S0/MeOn (CM0,CM0-PG), and confirm that the Host OS is available.</div> <div>3. Set the active power package on the SUT to Power Package 1 (Intel® ME on in S0).</div> <div>4. Set the Intel® AMT WLAN link policy on the SUT to Link Policy 3 (Enabled in S0, Sx/AC), if the WLAN network interface is available.</div> <div>5. Ensure that, where available, only the Host OS Wake on LAN and/or Wake on Wireless LAN driver setting(s) are enabled on the SUT. All other network wake sources must be disabled. This includes enabling ARP and/or NS Offload features where available to help prevent unexpected host wake events.</div> <div>6. Verify that Intel® AMT on the SUT responds to version queries via all available network interfaces.</div> <div>7. Ensure yellow bang is not seen on Drivers in Device Manager</div>		
Procedure:	<div>1. Hibernate the SUT via the Host OS.</div> <div>2. Verify that the SUT is in S4, S5, Deep S4, Deep S5, G3/MeOff (CM-Off).</div> <div>3. Send three magic packets, at 2 second intervals, by means of the active network interface.</div> <div>4. Verify that the SUT is in S0/MeOn (CM0,CM0-PG).</div> <div>5. Verify that the Host OS on the SUT is available.</div> <div>6. Verify that Intel® AMT on the SUT responds to version queries via all available network interfaces.</div> <div>7. Verify that windows booted from hibernate i.e. value should be 0x02. "run the following power shell command": Get-WinEvent -ProviderName Microsoft-Windows-Kernel-boot -MaxEvents 10 Where-Object {\$_.message -like "The boot type*"}</div> <div>8. Verify that the second nibble of the FWSTS2 register on the SUT have a value of 0x60xxxxxx.</div> <div>9. Ensure yellow bang is not seen on Drivers in Device Manager</div> <div>If both LAN and WLAN network interfaces are available, repeat this test procedure with the WLAN interface set as the active network interface.</div>		
Pass Criteria:	<div>The test passes if:</div> <div><div>• the SUT moves from S4, S5, Deep S4, Deep S5, or G3 to S0.</div><div>• the Intel® CSME moves to MeOn (CM0, CM0-PG).</div><div>• Intel® AMT responds to version queries via all available network interfaces.</div></div>		

ID:	ME_PM_10.3		
Title:	S4/CM3-PG to S0/CM0 via magic packet (AC+DC, AC-only/PP2/LP3)		
Requirement:	Mandatory	Exemptions	<input checked="" type="checkbox"/> Systems without WoL and/or WoWLAN support
			<input checked="" type="checkbox"/> Systems with a WLAN-only network interface
Method:	Automated by Intel® PETS		
Objective:	This test checks the SUT power flow from S4/CM3-PG to S0/CM0 via magic packet with the parameters outlined below.		
Configuration:	Intel® AMT should be provisioned via manual mode.		
	This test assumes that either LAN-only, or both LAN and WLAN network interfaces are available on the SUT.		



ID:	ME_PM_10.3	
Parameters:	System Power Source AC+DC or AC-only	
	Power States	Initial S4,S5/MeOff (CM3-PG)
		Final S0/MeOn (CM0)
		Trigger Magic Packet receipt
	Intel® AMT	Power Package PP2 (Intel® ME on in S0, wake in Sx/AC)
		WLAN Link Policy LP3 (Enabled in S0, Sx/AC) where available
Setup:	<ol style="list-style-type: none"> Set the SUT power source to AC+DC where supported; otherwise AC-only. Bring the SUT to the base state of S0/MeOn (CM0), and confirm that the Host OS is available. Set the active power package on the SUT to Power Package 2 (Intel® ME on in S0, wake in Sx/AC). Set the Intel® AMT WLAN link policy on the SUT to Link Policy 3 (Enabled in S0, Sx/AC), if the WLAN network interface is available. Ensure the Intel® AMT idle timeout on the SUT is set to 1 minute. Ensure that only the Host OS Wake on LAN driver setting is enabled on the SUT; all other network wake sources must be disabled. This includes enabling ARP and/or NS Offload features where available to help prevent unexpected host wake events, and disabling the Host OS Wake on Wireless LAN driver settings, if available. Verify that Intel® AMT on the SUT responds to version queries via all available network interfaces. Ensure yellow bang is not seen on Drivers in Device Manager Hibernate the SUT via the Host OS. Verify that the SUT is in S4, S5/MeOn (CM3). Verify that Intel® AMT on the SUT responds to version queries via all available network interfaces. Wait for 3 minutes to allow the Intel® ME on the SUT to move to CM3-PG after Intel® AMT idle timeout. Verify that the SUT is in S4, S5/CM3-PG. 	
Procedure:	<ol style="list-style-type: none"> Send three magic packets, at 2 second intervals, by means of the LAN network interface. Verify that the SUT is in S0/MeOn (CM0). Verify that the Host OS on the SUT is available. Verify that Intel® AMT on the SUT responds to version queries via all available network interfaces. Verify that windows booted from hibernate i.e. value should be 0x02. "run the following power shell command": Get-WinEvent -ProviderName Microsoft-Windows-Kernel-boot -MaxEvents 10 Where-Object {\$_.message -like "The boot type*"} Verify that the second nibble of the FWSTS2 register on the SUT have a value of 0x60xxxxxx. Ensure yellow bang is not seen on Drivers in Device Manager 	
Pass Criteria:	The test passes if: <ul style="list-style-type: none"> the SUT moves from S4 to S0. the Intel® CSME moves to MeOn (CM0). Intel® AMT responds to version queries via all available network interfaces. 	

ID:	ME_PM_10.4	
Title:	S4/CM3-PG to S0/CM0 via Power Button press (AC+DC, AC-only/PP2/LP3)	
Requirement:	Mandatory	Exemptions None
Method:	Automated by Intel® PETS	
Objective:	This test checks the SUT power flow from S4/CM3-PG to S0/CM0 via Power Button press with the parameters outlined below.	
Configuration:	Intel® AMT should be provisioned via manual mode. This test assumes that either LAN-only, WLAN-only, or both LAN and WLAN network interfaces are available on the SUT.	



ID:	ME_PM_10.4	
Parameters:	System Power Source AC+DC or AC-only	
	Power States	Initial S4,S5/MeOff (CM3-PG)
		Final S0/MeOn (CM0, CM0-PG)
		Trigger Power Button press
	Intel® AMT	Power Package PP2 (Intel® ME on in S0, wake in Sx/AC)
		WLAN Link Policy LP3 (Enabled in S0, Sx/AC) where available
Setup:	<ol style="list-style-type: none"> 1. Set the SUT power source to AC+DC where supported; otherwise AC-only. 2. Bring the SUT to the base state of S0/MeOn (CM0,CM0-PG), and confirm that the Host OS is available. 3. Set the active power package on the SUT to Power Package 2 (Intel® ME on in S0, wake in Sx/AC). 4. Set the Intel® AMT WLAN link policy on the SUT to Link Policy 3 (Enabled in S0, Sx/AC), if the WLAN network interface is available. 5. Ensure that the Host OS network device drivers are configured to not wake the SUT. This includes enabling ARP and/or NS Offload features where available to help prevent unexpected host wake events. 6. Ensure the Intel® AMT idle timeout on the SUT is set to 1 minute. 7. Verify that Intel® AMT on the SUT responds to version queries via all available network interfaces. 8. Ensure yellow bang is not seen on Drivers in Device Manager 9. Hibernate the SUT via the Host OS. 10. Verify that the SUT is in S4, S5/MeOn (CM3). 11. Verify that Intel® AMT on the SUT responds to version queries via all available network interfaces. 12. Wait for 3 minutes to allow the Intel® ME on the SUT to move to CM3-PG after Intel® AMT idle timeout. 13. Verify that the SUT is in S4, S5/CM3-PG. 	
Procedure:	<ol style="list-style-type: none"> 1. Briefly press the Power Button on the SUT. 2. Verify that the SUT is in S0/MeOn (CM0,CM0-PG). 3. Verify that the Host OS on the SUT is available. 4. Verify that Intel® AMT on the SUT responds to version queries via all available network interfaces. 5. Verify that windows booted from hibernate i.e. value should be 0x02. "run the following power shell command": Get-WinEvent -ProviderName Microsoft-Windows-Kernel-boot -MaxEvents 10 Where-Object {\$_.message -like "The boot type*"} 6. Verify that the second nibble of the FWSTS2 register on the SUT have a value of 0x60xxxxxx. 7. Ensure yellow bang is not seen on Drivers in Device Manager 	
Pass Criteria:	<p>The test passes if:</p> <ul style="list-style-type: none"> • the SUT moves from S4 to S0. • the Intel® CSME moves to MeOn (CM0, CM0-PG). • Intel® AMT responds to version queries via all available network interfaces. 	

ID:	ME_PM_10.5	
Title:	S5/CM-Off to S0/CM0 via magic packet (AC+DC, AC-only/PP1/LP3)	
Requirement:	Mandatory	Exemptions <input checked="" type="checkbox"/> Systems without WoL and/or WoWLAN support
Method:	Automated by Intel® PETS	
Objective:	This test checks the SUT power flow from S5/CM-Off to S0/CM0 via magic packet with the parameters outlined below.	
Configuration:	<p>Intel® AMT should be provisioned via manual mode.</p> <p>If Deep S4, Deep S5, and/or G3 are supported on the SUT, please confirm the following:</p> <ul style="list-style-type: none"> • the SUT and/or BIOS are properly configured to permit Deep S4/S5 or G3 entry. • the correct Deep Sx policy is applied to the SUT profile in Intel® PETS. <p>This test assumes that either LAN-only, WLAN-only, or both LAN and WLAN network interfaces are available on the SUT. Where both network interfaces are available, LAN is the initial active network interface in the test, and WLAN is the secondary network interface.</p>	



ID:	ME_PM_10.5	
Parameters:	System Power Source AC+DC or AC-only	
	Power States	Initial S5, Deep S5, G3/MeOff (CM-Off)
		Final S0/MeOn (CM0, CM0-PG)
		Trigger Magic Packet receipt
	Intel® AMT	Power Package PP1 (Intel® ME on in S0)
		WLAN Link Policy LP3 (Enabled in S0, Sx/AC) where available
Setup:	<ol style="list-style-type: none"> 1. Set the SUT power source to AC+DC where supported; otherwise AC-only. 2. Bring the SUT to the base state of S0/MeOn (CM0,CM0-PG), and confirm that the Host OS is available. 3. Set the active power package on the SUT to Power Package 1 (Intel® ME on in S0). 4. Set the Intel® AMT WLAN link policy on the SUT to Link Policy 3 (Enabled in S0, Sx/AC), if the WLAN network interface is available. 5. Ensure that, where available, only the Host OS Wake on LAN and/or Wake on Wireless LAN driver setting(s) are enabled on the SUT. All other network wake sources must be disabled. This includes enabling ARP and/or NS Offload features where available to help prevent unexpected host wake events. 6. Verify that Intel® AMT on the SUT responds to version queries via all available network interfaces. 7. Ensure yellow bang is not seen on Drivers in Device Manager 	
Procedure:	<ol style="list-style-type: none"> 1. Shutdown the SUT via the Host OS. 2. Verify that the SUT is in S5, Deep S5, G3/MeOff (CM-Off). 3. Send three magic packets, at 2 second intervals, by means of the active network interface. 4. Verify that the SUT is in S0/MeOn (CM0,CM0-PG). 5. Verify that the Host OS on the SUT is available. 6. Verify that Intel® AMT on the SUT responds to version queries via all available network interfaces. 7. Verify that the second nibble of the FWSTS2 register on the SUT have a value of 0x60xxxxxx. 8. Ensure yellow bang is not seen on Drivers in Device Manager <p>If both LAN and WLAN network interfaces are available, repeat this test procedure with the WLAN interface set as the active network interface.</p>	
Pass Criteria:	The test passes if: <ul style="list-style-type: none"> • the SUT moves from S5 (or Deep S5 or G3) to S0. • the Intel® CSME moves to MeOn (CM0, CM0-PG). • Intel® AMT responds to version queries via all available network interfaces. 	

ID:	ME_PM_10.6	
Title:	S5/CM-Off to S0/CM0 via Power Button press (AC+DC, AC-only/PP1/LP3)	
Requirement:	Mandatory	Exemptions None
Method:	Automated by Intel® PETS	
Objective:	This test checks the SUT power flow from S5/CM-Off to S0/CM0 via Power Button press with the parameters outlined below.	
Configuration:	Intel® AMT should be provisioned via manual mode. If Deep S5 and/or G3 are supported on the SUT, please confirm the following: <ul style="list-style-type: none"> • the SUT and/or BIOS are properly configured to permit Deep S5 or G3 entry. • the correct Deep Sx policy is applied to the SUT profile in Intel® PETS. This test assumes that either LAN-only, WLAN-only, or both LAN and WLAN network interfaces are available on the SUT.	
Parameters:	System Power Source AC+DC or AC-only	
	Power States	Initial S5, Deep S5, G3/MeOff (CM-Off)
		Final S0/MeOn (CM0, CM0-PG)
		Trigger Power Button press
	Intel® AMT	Power Package PP1 (Intel® ME on in S0)
		WLAN Link Policy LP3 (Enabled in S0, Sx/AC) where available



ID:	ME_PM_10.6
Setup:	<ol style="list-style-type: none"> 1. Set the SUT power source to AC+DC where supported; otherwise AC-only. 2. Bring the SUT to the base state of S0/MeOn (CM0,CM0-PG), and confirm that the Host OS is available. 3. Set the active power package on the SUT to Power Package 1 (Intel® ME on in S0). 4. Set the Intel® AMT WLAN link policy on the SUT to Link Policy 3 (Enabled in S0, Sx/AC), if the WLAN network interface is available. 5. Ensure that the Host OS network device drivers are configured to not wake the SUT. This includes enabling ARP and/or NS Offload features where available to help prevent unexpected host wake events. 6. Verify that Intel® AMT on the SUT responds to version queries via all available network interfaces. 7. Ensure yellow bang is not seen on Drivers in Device Manager 8. Shutdown the SUT via the Host OS. 9. Verify that the SUT is in S5, Deep S5, G3/MeOff (CM-Off).
Procedure:	<ol style="list-style-type: none"> 1. Briefly press the Power Button on the SUT. 2. Verify that the SUT is in S0/MeOn (CM0,CM0-PG). 3. Verify that the Host OS on the SUT is available. 4. Verify that Intel® AMT on the SUT responds to version queries via all available network interfaces. 5. Verify that the second nibble of the FWSTS2 register on the SUT have a value of 0x60xxxxxx. 6. Ensure yellow bang is not seen on Drivers in Device Manager
Pass Criteria:	<p>The test passes if:</p> <ul style="list-style-type: none"> • the SUT moves from S5 (or Deep S5 or G3) to S0. • the Intel® CSME moves to MeOn (CM0, CM0-PG). • Intel® AMT responds to version queries via all available network interfaces.

ID:	ME_PM_10.7		
Title:	S5/CM3-PG to S0/CM0 via magic packet (AC+DC, AC-only/PP2/LP3)		
Requirement:	Mandatory	Exemptions	<input checked="" type="checkbox"/> Systems without WoL and/or WoWLAN support <input checked="" type="checkbox"/> Systems with a WLAN-only network interface
Method:	Automated by Intel® PETS		
Objective:	This test checks the SUT power flow from S5/CM3-PG to S0/CM0 via magic packet with the parameters outlined below.		
Configuration:	Intel® AMT should be provisioned via manual mode. This test assumes that either LAN-only, or both LAN and WLAN network interfaces are available on the SUT.		
Parameters:	System Power Source		AC+DC or AC-only
	Power States	Initial	S5/MeOff (CM3-PG)
		Final	S0/MeOn (CM0)
		Trigger	Magic Packet receipt
	Intel® AMT	Power Package	PP2 (Intel® ME on in S0, wake in Sx/AC)
		WLAN Link Policy	LP3 (Enabled in S0, Sx/AC) where available



ID:	ME_PM_10.7
Setup:	<ol style="list-style-type: none"> 1. Set the SUT power source to AC+DC where supported; otherwise AC-only. 2. Bring the SUT to the base state of S0/MeOn (CM0), and confirm that the Host OS is available. 3. Set the active power package on the SUT to Power Package 2 (Intel® ME on in S0, wake in Sx/AC). 4. Set the Intel® AMT WLAN link policy on the SUT to Link Policy 3 (Enabled in S0, Sx/AC), if the WLAN network interface is available. 5. Ensure that only the Host OS Wake on LAN driver setting is enabled on the SUT; all other network wake sources must be disabled. This includes enabling ARP and/or NS Offload features where available to help prevent unexpected host wake events, and disabling the Host OS Wake on Wireless LAN driver settings, if available. 6. Ensure the Intel® AMT idle timeout on the SUT is set to 1 minute. 7. Verify that Intel® AMT on the SUT responds to version queries via all available network interfaces. 8. Ensure yellow bang is not seen on Drivers in Device Manager 9. Shutdown the SUT via the Host OS. 10. Verify that the SUT is in S5/MeOn (CM3). 11. Verify that Intel® AMT on the SUT responds to version queries via all available network interfaces. 12. Wait for 3 minutes to allow the Intel® ME on the SUT to move to CM3-PG after Intel® AMT idle timeout. 13. Verify that the SUT is in S5/CM3-PG.
Procedure:	<ol style="list-style-type: none"> 1. Send three magic packets, at 2 second intervals, by means of the LAN network interface. 2. Verify that the SUT is in S0/MeOn (CM0). 3. Verify that the Host OS on the SUT is available. 4. Verify that Intel® AMT on the SUT responds to version queries via all available network interfaces. 5. Verify that the second nibble of the FWSTS2 register on the SUT have a value of 0x60xxxxxx. 6. Ensure yellow bang is not seen on Drivers in Device Manager
Pass Criteria:	<p>The test passes if:</p> <ul style="list-style-type: none"> • the SUT moves from S5 to S0. • the Intel® CSME moves to MeOn (CM0). • Intel® AMT responds to version queries via all available network interfaces.

ID:	ME_PM_10.8		
Title:	S5/CM3-PG to S0/CM0 via Power Button press (AC+DC, AC-only/PP2/LP3)		
Requirement:	Mandatory	Exemptions	None
Method:	Automated by Intel® PETS		
Objective:	This test checks the SUT power flow from S5/CM3-PG to S0/CM0 via Power Button press with the parameters outlined below.		
Configuration:	Intel® AMT should be provisioned via manual mode. This test assumes that either LAN-only, WLAN-only, or both LAN and WLAN network interfaces are available on the SUT.		
Parameters:	System Power Source		AC+DC or AC-only
	Power States	Initial	S5/MeOff (CM3-PG)
		Final	S0/MeOn (CM0, CM0-PG)
		Trigger	Power Button press
	Intel® AMT	Power Package	PP2 (Intel® ME on in S0, wake in Sx/AC)
		WLAN Link Policy	LP3 (Enabled in S0, Sx/AC) where available



ID:	ME_PM_10.8
Setup:	<ol style="list-style-type: none"> 1. Set the SUT power source to AC+DC where supported; otherwise AC-only. 2. Bring the SUT to the base state of S0/MeOn (CM0,CM0-PG), and confirm that the Host OS is available. 3. Set the active power package on the SUT to Power Package 2 (Intel® ME on in S0, wake in Sx/AC). 4. Set the Intel® AMT WLAN link policy on the SUT to Link Policy 3 (Enabled in S0, Sx/AC), if the WLAN network interface is available. 5. Ensure that the Host OS network device drivers are configured to not wake the SUT. This includes enabling ARP and/or NS Offload features where available to help prevent unexpected host wake events. 6. Ensure the Intel® AMT idle timeout on the SUT is set to 1 minute. 7. Verify that Intel® AMT on the SUT responds to version queries via all available network interfaces. 8. Ensure yellow bang is not seen on Drivers in Device Manager 9. Shutdown the SUT via the Host OS. 10. Verify that the SUT is in S5/MeOn (CM3). 11. Verify that Intel® AMT on the SUT responds to version queries via all available network interfaces. 12. Wait for 3 minutes to allow the Intel® ME on the SUT to move to CM3-PG after Intel® AMT idle timeout. 13. Verify that the SUT is in S5/CM3-PG.
Procedure:	<ol style="list-style-type: none"> 1. Briefly press the Power Button on the SUT. 2. Verify that the SUT is in S0/MeOn (CM0,CM0-PG). 3. Verify that the Host OS on the SUT is available. 4. Verify that Intel® AMT on the SUT responds to version queries via all available network interfaces. 5. Verify that the second nibble of the FWSTS2 register on the SUT have a value of 0x60xxxxxx. 6. Ensure yellow bang is not seen on Drivers in Device Manager
Pass Criteria:	<p>The test passes if:</p> <ul style="list-style-type: none"> • the SUT moves from S5 to S0. • the Intel® CSME moves to MeOn (CM0, CM0-PG). • Intel® AMT responds to version queries via all available network interfaces.

ID:	ME_PM_10.9																	
Title:	S4/CM-Off to S0/CM0 via magic packet (DC-only/PP1/LP3)																	
Requirement:	Mandatory	Exemptions	<div><input checked="" type="checkbox"/> Non-Mobile (AC-only) systems</div> <div><input checked="" type="checkbox"/> Systems without WoL and/or WoWLAN support</div>															
Method:	Automated by Intel® PETS																	
Objective:	This test checks the SUT power flow from S4/CM-Off to S0/CM0 via magic packet with the parameters outlined below.																	
Configuration:	<p>Intel® AMT should be provisioned via manual mode.</p> <p>If Deep S4, Deep S5, and/or G3 are supported on the SUT, please confirm the following:</p> <ul style="list-style-type: none">the SUT and/or BIOS are properly configured to permit Deep S4/S5 or G3 entry.the correct Deep Sx policy is applied to the SUT profile in Intel® PETS. <p>This test assumes that either LAN-only, WLAN-only, or both LAN and WLAN network interfaces are available on the SUT. Where both network interfaces are available, LAN is the initial active network interface in the test, and WLAN is the secondary network interface.</p>																	
Parameters:	<table><tr><td colspan="2">System Power Source</td><td>DC-only</td></tr><tr><td rowspan="3">Power States</td><td>Initial</td><td>S4, S5, Deep S4, Deep S5, G3/MeOff (CM-Off)</td></tr><tr><td>Final</td><td>S0/MeOn (CM0, CM0-PG)</td></tr><tr><td>Trigger</td><td>Magic Packet receipt</td></tr><tr><td rowspan="2">Intel® AMT</td><td>Power Package</td><td>PP1 (Intel® ME on in S0)</td></tr><tr><td>WLAN Link Policy</td><td>LP3 (Enabled in S0, Sx/AC) where available</td></tr></table>			System Power Source		DC-only	Power States	Initial	S4, S5, Deep S4, Deep S5, G3/MeOff (CM-Off)	Final	S0/MeOn (CM0, CM0-PG)	Trigger	Magic Packet receipt	Intel® AMT	Power Package	PP1 (Intel® ME on in S0)	WLAN Link Policy	LP3 (Enabled in S0, Sx/AC) where available
System Power Source		DC-only																
Power States	Initial	S4, S5, Deep S4, Deep S5, G3/MeOff (CM-Off)																
	Final	S0/MeOn (CM0, CM0-PG)																
	Trigger	Magic Packet receipt																
Intel® AMT	Power Package	PP1 (Intel® ME on in S0)																
	WLAN Link Policy	LP3 (Enabled in S0, Sx/AC) where available																



ID:	ME_PM_10.9
Setup:	<ol style="list-style-type: none"> Set the SUT power source to AC+DC. Bring the SUT to the base state of S0/MeOn (CM0,CM0-PG), and confirm that the Host OS is available. Verify that a DC battery is connected to the SUT, and that it is charged. Set the SUT power source to DC-only. Set the active power package on the SUT to Power Package 1 (Intel® ME on in S0). Set the Intel® AMT WLAN link policy on the SUT to Link Policy 3 (Enabled in S0, Sx/AC), if the WLAN network interface is available. Ensure that, where available, only the Host OS Wake on LAN and/or Wake on Wireless LAN driver setting(s) are enabled on the SUT. All other network wake sources must be disabled. This includes enabling ARP and/or NS Offload features where available to help prevent unexpected host wake events. Verify that Intel® AMT on the SUT responds to version queries via all available network interfaces. Ensure yellow bang is not seen on Drivers in Device Manager
Procedure:	<ol style="list-style-type: none"> Hibernate the SUT via the Host OS. Verify that the SUT is in S4, S5, Deep S4, Deep S5, G3/MeOff (CM-Off). Send three magic packets, at 2 second intervals, by means of the active network interface. Verify that the SUT is in S0/MeOn (CM0,CM0-PG). Verify that the Host OS on the SUT is available. Verify that Intel® AMT on the SUT responds to version queries via all available network interfaces. Verify that windows booted from hibernate i.e. value should be 0x02. "run the following power shell command": Get-WinEvent -ProviderName Microsoft-Windows-Kernel-boot -MaxEvents 10 Where-Object {\$_.message -like "The boot type*"}. Verify that the second nibble of the FWSTS2 register on the SUT have a value of 0x60xxxxxx. Ensure yellow bang is not seen on Drivers in Device Manager <p>If both LAN and WLAN network interfaces are available, repeat this test procedure with the WLAN interface set as the active network interface.</p>
Pass Criteria:	<p>The test passes if:</p> <ul style="list-style-type: none"> the SUT moves from S4, S5, Deep S4, Deep S5, or G3 to S0. the Intel® CSME moves to MeOn (CM0, CM0-PG). Intel® AMT responds to version queries via all available network interfaces.

ID:	ME_PM_10.10																	
Title:	S4/CM3-PG with AC Wake to S0/CM0 via magic packet (DC-only/PP2/LP3)																	
Requirement:	Mandatory	Exemptions	<div><input checked="" type="checkbox"/> Non-Mobile (AC-only) systems</div> <div><input checked="" type="checkbox"/> Systems without WoL and/or WoWLAN support</div>															
Method:	Automated by Intel® PETS																	
Objective:	This test checks the SUT power flow from S4/CM3-PG with AC Wake to S0/CM0 via magic packet with the parameters outlined below.																	
Configuration:	<p>Intel® AMT should be provisioned via manual mode.</p> <p>If Deep S4, Deep S5, and/or G3 are supported on the SUT, please confirm the following:</p> <ul style="list-style-type: none">the SUT and/or BIOS are properly configured to permit Deep S4/S5 or G3 entry.the correct Deep Sx policy is applied to the SUT profile in Intel® PETS. <p>This test assumes that either LAN-only, WLAN-only, or both LAN and WLAN network interfaces are available on the SUT. Where both network interfaces are available, LAN is the initial active network interface in the test, and WLAN is the secondary network interface.</p>																	
Parameters:	<table><tr><td colspan="2">System Power Source</td><td>DC-only</td></tr><tr><td rowspan="3">Power States</td><td>Initial</td><td>S4,S5,Deep S4,Deep S5,G3/CM3-PG with Ac Wake</td></tr><tr><td>Final</td><td>S0/MeOn (CM0, CM0-PG)</td></tr><tr><td>Trigger</td><td>Magic Packet receipt</td></tr><tr><td rowspan="2">Intel® AMT</td><td>Power Package</td><td>PP2 (Intel® ME on in S0, wake in Sx/AC)</td></tr><tr><td>WLAN Link Policy</td><td>LP3 (Enabled in S0, Sx/AC) where available</td></tr></table>			System Power Source		DC-only	Power States	Initial	S4,S5,Deep S4,Deep S5,G3/CM3-PG with Ac Wake	Final	S0/MeOn (CM0, CM0-PG)	Trigger	Magic Packet receipt	Intel® AMT	Power Package	PP2 (Intel® ME on in S0, wake in Sx/AC)	WLAN Link Policy	LP3 (Enabled in S0, Sx/AC) where available
System Power Source		DC-only																
Power States	Initial	S4,S5,Deep S4,Deep S5,G3/CM3-PG with Ac Wake																
	Final	S0/MeOn (CM0, CM0-PG)																
	Trigger	Magic Packet receipt																
Intel® AMT	Power Package	PP2 (Intel® ME on in S0, wake in Sx/AC)																
	WLAN Link Policy	LP3 (Enabled in S0, Sx/AC) where available																



ID:	ME_PM_10.10
Setup:	<ol style="list-style-type: none"> 1. Set the SUT power source to AC+DC. 2. Bring the SUT to the base state of S0/MeOn (CM0,CM0-PG), and confirm that the Host OS is available. 3. Verify that a DC battery is connected to the SUT, and that it is charged. 4. Set the SUT power source to DC-only. 5. Set the active power package on the SUT to Power Package 2 (Intel® ME on in S0, wake in Sx/AC). 6. Set the Intel® AMT WLAN link policy on the SUT to Link Policy 3 (Enabled in S0, Sx/AC), if the WLAN network interface is available. 7. Ensure that, where available, only the Host OS Wake on LAN and/or Wake on Wireless LAN driver setting(s) are enabled on the SUT. All other network wake sources must be disabled. This includes enabling ARP and/or NS Offload features where available to help prevent unexpected host wake events. 8. Verify that Intel® AMT on the SUT responds to version queries via all available network interfaces. 9. Ensure yellow bang is not seen on Drivers in Device Manager
Procedure:	<ol style="list-style-type: none"> 1. Hibernate the SUT via the Host OS. 2. Verify that the SUT is in S3, Deep S3/CM3-PG with AC Wakewith AC Wake. 3. Send three magic packets, at 2 second intervals, by means of the active network interface. 4. Verify that the SUT is in S0/MeOn (CM0,CM0-PG). 5. Verify that the Host OS on the SUT is available. 6. Verify that Intel® AMT on the SUT responds to version queries via all available network interfaces. 7. Verify that windows booted from hibernate i.e. value should be 0x02. "run the following power shell command": Get-WinEvent -ProviderName Microsoft-Windows-Kernel-boot -MaxEvents 10 Where-Object {\$_.message -like "The boot type*"} 8. Verify that the second nibble of the FWSTS2 register on the SUT have a value of 0x60xxxxxx. 9. Ensure yellow bang is not seen on Drivers in Device Manager <p>If both LAN and WLAN network interfaces are available, repeat this test procedure with the WLAN interface set as the active network interface.</p>
Pass Criteria:	<p>The test passes if:</p> <ul style="list-style-type: none"> • the SUT moves from S4, S5, Deep S4, Deep S5, or G3 to S0. • the Intel® CSME moves to MeOn (CM0, CM0-PG). • Intel® AMT responds to version queries via all available network interfaces.

ID:	ME_PM_10.11																	
Title:	S5/CM-Off to S0/CM0 via magic packet (DC-only/PP1/LP3)																	
Requirement:	Mandatory	Exemptions	<div><input checked="" type="checkbox"/> Non-Mobile (AC-only) systems</div> <div><input checked="" type="checkbox"/> Systems without WoL and/or WoWLAN support</div>															
Method:	Automated by Intel® PETS																	
Objective:	This test checks the SUT power flow from S5/CM-Off to S0/CM0 via magic packet with the parameters outlined below.																	
Configuration:	<p>Intel® AMT should be provisioned via manual mode.</p> <p>If Deep S5 and/or G3 are supported on the SUT, please confirm the following:</p> <ul style="list-style-type: none">the SUT and/or BIOS are properly configured to permit Deep S5 or G3 entry.the correct Deep Sx policy is applied to the SUT profile in Intel® PETS. <p>This test assumes that either LAN-only, WLAN-only, or both LAN and WLAN network interfaces are available on the SUT. Where both network interfaces are available, LAN is the initial active network interface in the test, and WLAN is the secondary network interface.</p>																	
Parameters:	<table><tr><td colspan="2">System Power Source</td><td>DC-only</td></tr><tr><td rowspan="3">Power States</td><td>Initial</td><td>S5, Deep S5, G3/MeOff (CM-Off)</td></tr><tr><td>Final</td><td>S0/MeOn (CM0, CM0-PG)</td></tr><tr><td>Trigger</td><td>Magic Packet receipt</td></tr><tr><td rowspan="2">Intel® AMT</td><td>Power Package</td><td>PP1 (Intel® ME on in S0)</td></tr><tr><td>WLAN Link Policy</td><td>LP3 (Enabled in S0, Sx/AC) where available</td></tr></table>			System Power Source		DC-only	Power States	Initial	S5, Deep S5, G3/MeOff (CM-Off)	Final	S0/MeOn (CM0, CM0-PG)	Trigger	Magic Packet receipt	Intel® AMT	Power Package	PP1 (Intel® ME on in S0)	WLAN Link Policy	LP3 (Enabled in S0, Sx/AC) where available
System Power Source		DC-only																
Power States	Initial	S5, Deep S5, G3/MeOff (CM-Off)																
	Final	S0/MeOn (CM0, CM0-PG)																
	Trigger	Magic Packet receipt																
Intel® AMT	Power Package	PP1 (Intel® ME on in S0)																
	WLAN Link Policy	LP3 (Enabled in S0, Sx/AC) where available																



ID:	ME_PM_10.11
Setup:	<ol style="list-style-type: none"> 1. Set the SUT power source to AC+DC. 2. Bring the SUT to the base state of S0/MeOn (CM0,CM0-PG), and confirm that the Host OS is available. 3. Verify that a DC battery is connected to the SUT, and that it is charged. 4. Set the SUT power source to DC-only. 5. Set the active power package on the SUT to Power Package 1 (Intel® ME on in S0). 6. Set the Intel® AMT WLAN link policy on the SUT to Link Policy 3 (Enabled in S0, Sx/AC), if the WLAN network interface is available. 7. Ensure that, where available, only the Host OS Wake on LAN and/or Wake on Wireless LAN driver setting(s) are enabled on the SUT. All other network wake sources must be disabled. This includes enabling ARP and/or NS Offload features where available to help prevent unexpected host wake events. 8. Verify that Intel® AMT on the SUT responds to version queries via all available network interfaces. 9. Ensure yellow bang is not seen on Drivers in Device Manager
Procedure:	<ol style="list-style-type: none"> 1. Shutdown the SUT via the Host OS. 2. Verify that the SUT is in S5, Deep S5, G3/MeOff (CM-Off). 3. Send three magic packets, at 2 second intervals, by means of the active network interface. 4. Verify that the SUT is in S0/MeOn (CM0,CM0-PG). 5. Verify that the Host OS on the SUT is available. 6. Verify that Intel® AMT on the SUT responds to version queries via all available network interfaces. 7. Verify that the second nibble of the FWSTS2 register on the SUT have a value of 0x60xxxxxx. 8. Ensure yellow bang is not seen on Drivers in Device Manager <p>If both LAN and WLAN network interfaces are available, repeat this test procedure with the WLAN interface set as the active network interface.</p>
Pass Criteria:	<p>The test passes if:</p> <ul style="list-style-type: none"> • the SUT moves from S5 (or Deep S5 or G3) to S0. • the Intel® CSME moves to MeOn (CM0, CM0-PG). • Intel® AMT responds to version queries via all available network interfaces.

ID:	ME_PM_10.12																	
Title:	S5/CM3-PG with AC Wake to S0/CM0 via magic packet (DC-only/PP2/LP3)																	
Requirement:	Mandatory	Exemptions	<div><input checked="" type="checkbox"/> Non-Mobile (AC-only) systems</div> <div><input checked="" type="checkbox"/> Systems without WoL and/or WoWLAN support</div>															
Method:	Automated by Intel® PETS																	
Objective:	This test checks the SUT power flow from S5/CM3-PG with AC Wake to S0/CM0 via magic packet with the parameters outlined below.																	
Configuration:	<p>Intel® AMT should be provisioned via manual mode.</p> <p>If Deep S5 and/or G3 are supported on the SUT, please confirm the following:</p> <ul style="list-style-type: none">the SUT and/or BIOS are properly configured to permit Deep S5 or G3 entry.the correct Deep Sx policy is applied to the SUT profile in Intel® PETS. <p>This test assumes that either LAN-only, WLAN-only, or both LAN and WLAN network interfaces are available on the SUT. Where both network interfaces are available, LAN is the initial active network interface in the test, and WLAN is the secondary network interface.</p>																	
Parameters:	<table><tr><td colspan="2">System Power Source</td><td>DC-only</td></tr><tr><td rowspan="3">Power States</td><td>Initial</td><td>S5,Deep S5,G3/CM3-PG with AC Wake</td></tr><tr><td>Final</td><td>S0/MeOn (CM0, CM0-PG)</td></tr><tr><td>Trigger</td><td>Magic Packet receipt</td></tr><tr><td rowspan="2">Intel® AMT</td><td>Power Package</td><td>PP2 (Intel® ME on in S0, wake in Sx/AC)</td></tr><tr><td>WLAN Link Policy</td><td>LP3 (Enabled in S0, Sx/AC) where available</td></tr></table>			System Power Source		DC-only	Power States	Initial	S5,Deep S5,G3/CM3-PG with AC Wake	Final	S0/MeOn (CM0, CM0-PG)	Trigger	Magic Packet receipt	Intel® AMT	Power Package	PP2 (Intel® ME on in S0, wake in Sx/AC)	WLAN Link Policy	LP3 (Enabled in S0, Sx/AC) where available
System Power Source		DC-only																
Power States	Initial	S5,Deep S5,G3/CM3-PG with AC Wake																
	Final	S0/MeOn (CM0, CM0-PG)																
	Trigger	Magic Packet receipt																
Intel® AMT	Power Package	PP2 (Intel® ME on in S0, wake in Sx/AC)																
	WLAN Link Policy	LP3 (Enabled in S0, Sx/AC) where available																



ID:	ME_PM_10.12
Setup:	<ol style="list-style-type: none"> 1. Set the SUT power source to AC+DC. 2. Bring the SUT to the base state of S0/MeOn (CM0,CM0-PG), and confirm that the Host OS is available. 3. Verify that a DC battery is connected to the SUT, and that it is charged. 4. Set the SUT power source to DC-only. 5. Set the active power package on the SUT to Power Package 2 (Intel® ME on in S0, wake in Sx/AC). 6. Set the Intel® AMT WLAN link policy on the SUT to Link Policy 3 (Enabled in S0, Sx/AC), if the WLAN network interface is available. 7. Ensure that, where available, only the Host OS Wake on LAN and/or Wake on Wireless LAN driver setting(s) are enabled on the SUT. All other network wake sources must be disabled. This includes enabling ARP and/or NS Offload features where available to help prevent unexpected host wake events. 8. Verify that Intel® AMT on the SUT responds to version queries via all available network interfaces. 9. Ensure yellow bang is not seen on Drivers in Device Manager
Procedure:	<ol style="list-style-type: none"> 1. Shutdown the SUT via the Host OS. 2. Verify that the SUT is in S5, Deep S5, G3/CM3-PG.with AC Wake 3. Send three magic packets, at 2 second intervals, by means of the active network interface. 4. Verify that the SUT is in S0/MeOn (CM0,CM0-PG). 5. Verify that the Host OS on the SUT is available. 6. Verify that Intel® AMT on the SUT responds to version queries via all available network interfaces. 7. Verify that the second nibble of the FWSTS2 register on the SUT have a value of 0x60xxxxxx. 8. Ensure yellow bang is not seen on Drivers in Device Manager <p>If both LAN and WLAN network interfaces are available, repeat this test procedure with the WLAN interface set as the active network interface.</p>
Pass Criteria:	<p>The test passes if:</p> <ul style="list-style-type: none"> • the SUT moves from S5 (or Deep S5 or G3) to S0. • the Intel® CSME moves to MeOn (CM0, CM0-PG). • Intel® AMT responds to version queries via all available network interfaces.

12.14 ME_PM_11: S0/CM0 to S4, S5/CM3

ID:	ME_PM_11.1		
Title:	S0/CM0 to S4/CM3 via Host OS hibernate (AC+DC, AC-only/PP2/LP3)		
Requirement:	Mandatory	Exemptions	None
Method:	Automated by Intel® PETS		
Objective:	This test checks the SUT power flow from S0/CM0 to S4/CM3 via Host OS hibernate with the parameters outlined below.		
Configuration:	<p>Intel® AMT should be provisioned via manual mode.</p> <p>This test assumes that either LAN-only, WLAN-only, or both LAN and WLAN network interfaces are available on the SUT.</p>		
Parameters:	System Power Source		AC+DC or AC-only
	Power States	Initial	S0/MeOn (CM0, CM0-PG)
		Final	S4,S5/MeOn (CM3)
		Trigger	Host OS hibernate
	Intel® AMT	Power Package	PP2 (Intel® ME on in S0, wake in Sx/AC)
		WLAN Link Policy	LP3 (Enabled in S0, Sx/AC) where available



ID:	ME_PM_11.1
Setup:	<ol style="list-style-type: none"> 1. Set the SUT power source to AC+DC where supported; otherwise AC-only. 2. Bring the SUT to the base state of S0/MeOn (CM0,CM0-PG), and confirm that the Host OS is available. 3. Set the active power package on the SUT to Power Package 2 (Intel® ME on in S0, wake in Sx/AC). 4. Set the Intel® AMT WLAN link policy on the SUT to Link Policy 3 (Enabled in S0, Sx/AC), if the WLAN network interface is available. 5. Ensure that the Host OS network device drivers are configured to not wake the SUT. This includes enabling ARP and/or NS Offload features where available to help prevent unexpected host wake events. 6. Verify that Intel® AMT on the SUT responds to version queries via all available network interfaces.
Procedure:	<ol style="list-style-type: none"> 1. Hibernate the SUT via the Host OS. 2. Verify that the SUT is in S4, S5/MeOn (CM3). 3. Verify that Intel® AMT on the SUT responds to version queries via all available network interfaces.
Pass Criteria:	<p>The test passes if:</p> <ul style="list-style-type: none"> • the SUT moves to S4. • the Intel® CSME moves to MeOn (CM3). • Intel® AMT responds to version queries via all available network interfaces.

ID:	ME_PM_11.2		
Title:	S0/CM0 to S5/CM3 via Host OS shutdown (AC+DC, AC-only/PP2/LP3)		
Requirement:	Mandatory	Exemptions	None
Method:	Automated by Intel® PETS		
Objective:	This test checks the SUT power flow from S0/CM0 to S5/CM3 via Host OS shutdown with the parameters outlined below.		
Configuration:	Intel® AMT should be provisioned via manual mode. This test assumes that either LAN-only, WLAN-only, or both LAN and WLAN network interfaces are available on the SUT.		
Parameters:	System Power Source		AC+DC or AC-only
	Power States	Initial	S0/MeOn (CM0, CM0-PG)
		Final	S5/MeOn (CM3)
		Trigger	Host OS shutdown
	Intel® AMT	Power Package	PP2 (Intel® ME on in S0, wake in Sx/AC)
		WLAN Link Policy	LP3 (Enabled in S0, Sx/AC) where available
Setup:	<div>1. Set the SUT power source to AC+DC where supported; otherwise AC-only.</div> <div>2. Bring the SUT to the base state of S0/MeOn (CM0,CM0-PG), and confirm that the Host OS is available.</div> <div>3. Set the active power package on the SUT to Power Package 2 (Intel® ME on in S0, wake in Sx/AC).</div> <div>4. Set the Intel® AMT WLAN link policy on the SUT to Link Policy 3 (Enabled in S0, Sx/AC), if the WLAN network interface is available.</div> <div>5. Ensure that the Host OS network device drivers are configured to not wake the SUT. This includes enabling ARP and/or NS Offload features where available to help prevent unexpected host wake events.</div> <div>6. Verify that Intel® AMT on the SUT responds to version queries via all available network interfaces.</div>		
Procedure:	<div>1. Shutdown the SUT via the Host OS.</div> <div>2. Verify that the SUT is in S5/MeOn (CM3).</div> <div>3. Verify that Intel® AMT on the SUT responds to version queries via all available network interfaces.</div>		
Pass Criteria:	The test passes if: <ul style="list-style-type: none">the SUT moves to S5.the Intel® CSME is in MeOn (CM3).Intel® AMT responds to version queries via all available network interfaces.		



ID:	ME_PM_11.21																
Title:	S0/CM0 to S4/CM3 via Host OS hibernate (AC+DC, AC-only/PP2/LP2)																
Requirement:	Mandatory	Exemptions <input checked="" type="checkbox"/> Systems with a LAN-only network interface															
Method:	Automated by Intel® PETS																
Objective:	This test checks the SUT power flow from S0/CM0 to S4/CM3 via Host OS hibernate with the parameters outlined below.																
Configuration:	Intel® AMT should be provisioned via manual mode. This test assumes that either WLAN-only, or both LAN and WLAN network interfaces are available on the SUT.																
Parameters:	<table border="1"> <tr> <td colspan="2">System Power Source</td><td>AC+DC or AC-only</td></tr> <tr> <td rowspan="3">Power States</td><td>Initial</td><td>S0/MeOn (CM0, CM0-PG)</td></tr> <tr> <td>Final</td><td>S4,S5/MeOn (CM3)</td></tr> <tr> <td>Trigger</td><td>Host OS hibernate</td></tr> <tr> <td rowspan="2">Intel® AMT</td><td>Power Package</td><td>PP2 (Intel® ME on in S0, wake in Sx/AC)</td></tr> <tr> <td>WLAN Link Policy</td><td>LP2 (Enabled in S0)</td></tr> </table>		System Power Source		AC+DC or AC-only	Power States	Initial	S0/MeOn (CM0, CM0-PG)	Final	S4,S5/MeOn (CM3)	Trigger	Host OS hibernate	Intel® AMT	Power Package	PP2 (Intel® ME on in S0, wake in Sx/AC)	WLAN Link Policy	LP2 (Enabled in S0)
System Power Source		AC+DC or AC-only															
Power States	Initial	S0/MeOn (CM0, CM0-PG)															
	Final	S4,S5/MeOn (CM3)															
	Trigger	Host OS hibernate															
Intel® AMT	Power Package	PP2 (Intel® ME on in S0, wake in Sx/AC)															
	WLAN Link Policy	LP2 (Enabled in S0)															
Setup:	<ol style="list-style-type: none"> Set the SUT power source to AC+DC where supported; otherwise AC-only. Bring the SUT to the base state of S0/MeOn (CM0,CM0-PG), and confirm that the Host OS is available. Set the active power package on the SUT to Power Package 2 (Intel® ME on in S0, wake in Sx/AC). Set the Intel® AMT WLAN link policy on the SUT to Link Policy 2 (Enabled in S0). Ensure that the Host OS network device drivers are configured to not wake the SUT. This includes enabling ARP and/or NS Offload features where available to help prevent unexpected host wake events. Verify that Intel® AMT on the SUT responds to version queries via all available network interfaces. 																
Procedure:	<ol style="list-style-type: none"> Hibernate the SUT via the Host OS. Verify that the SUT is in S4, S5/MeOn (CM3). Verify that Intel® AMT on the SUT responds to version query via the LAN network interface, if available. Verify that Intel® AMT on the SUT does not respond to version query via the WLAN network interface. 																
Pass Criteria:	<p>The test passes if:</p> <ul style="list-style-type: none"> the SUT moves to S4. the Intel® CSME is in MeOn (CM3). when in S4: <ul style="list-style-type: none"> Intel® AMT on the SUT does respond to version queries via the LAN network interface, if available. Intel® AMT on the SUT does not respond to version queries the WLAN network interface. 																

ID:	ME_PM_11.22	
Title:	S0/CM0 to S5/CM3 via Host OS shutdown (AC+DC, AC-only/PP2/LP2)	
Requirement:	Mandatory	Exemptions <input checked="" type="checkbox"/> Systems with a LAN-only network interface
Method:	Automated by Intel® PETS	
Objective:	This test checks the SUT power flow from S0/CM0 to S5/CM3 via Host OS shutdown with the parameters outlined below.	
Configuration:	Intel® AMT should be provisioned via manual mode. This test assumes that either WLAN-only, or both LAN and WLAN network interfaces are available on the SUT.	



ID:	ME_PM_11.22		
Parameters:	System Power Source		AC+DC or AC-only
	Power States	Initial	S0/MeOn (CM0, CM0-PG)
		Final	S5/MeOn (CM3)
		Trigger	Host OS shutdown
	Intel® AMT	Power Package	PP2 (Intel® ME on in S0, wake in Sx/AC)
		WLAN Link Policy	LP2 (Enabled in S0)
Setup:	<ol style="list-style-type: none"> Set the SUT power source to AC+DC where supported; otherwise AC-only. Bring the SUT to the base state of S0/MeOn (CM0,CM0-PG), and confirm that the Host OS is available. Set the active power package on the SUT to Power Package 2 (Intel® ME on in S0, wake in Sx/AC). Set the Intel® AMT WLAN link policy on the SUT to Link Policy 2 (Enabled in S0). Ensure that the Host OS network device drivers are configured to not wake the SUT. This includes enabling ARP and/or NS Offload features where available to help prevent unexpected host wake events. Verify that Intel® AMT on the SUT responds to version queries via all available network interfaces. 		
Procedure:	<ol style="list-style-type: none"> Shutdown the SUT via the Host OS. Verify that the SUT is in S5/MeOn (CM3). Verify that Intel® AMT on the SUT responds to version query via the LAN network interface, if available. Verify that Intel® AMT on the SUT does not respond to version query via the WLAN network interface. 		
Pass Criteria:	<p>The test passes if:</p> <ul style="list-style-type: none"> the SUT moves to S5. the Intel® CSME is in MeOn (CM3). when in S5: <ul style="list-style-type: none"> Intel® AMT on the SUT does respond to version queries via the LAN network interface, if available. Intel® AMT on the SUT does not respond to version queries the WLAN network interface. 		

12.15 ME_PM_12: S4–S5/CM3 to S0/CM0

ID:	ME_PM_12.1		
Title:	S4/CM3 to S0/CM0 via magic packet (AC+DC, AC-only/PP2/LP3)		
Requirement:	Mandatory	Exemptions	<input checked="" type="checkbox"/> Systems without WoL and/or WoWLAN support <input checked="" type="checkbox"/> Systems with a WLAN-only network interface
Method:	Automated by Intel® PETS		
Objective:	This test checks the SUT power flow from S4/CM3 to S0/CM0 via magic packet with the parameters outlined below.		
Configuration:	<p>Intel® AMT should be provisioned via manual mode.</p> <p>This test assumes that either LAN-only, or both LAN and WLAN network interfaces are available on the SUT.</p>		
Parameters:	System Power Source		AC+DC or AC-only
	Power States	Initial	S4,S5/MeOn (CM3)
		Final	S0/MeOn (CM0)
		Trigger	Magic Packet receipt
	Intel® AMT	Power Package	PP2 (Intel® ME on in S0, wake in Sx/AC)
		WLAN Link Policy	LP3 (Enabled in S0, Sx/AC) where available



ID:	ME_PM_12.1
Setup:	<ol style="list-style-type: none"> 1. Set the SUT power source to AC+DC where supported; otherwise AC-only. 2. Bring the SUT to the base state of S0/MeOn (CM0), and confirm that the Host OS is available. 3. Set the active power package on the SUT to Power Package 2 (Intel® ME on in S0, wake in Sx/AC). 4. Set the Intel® AMT WLAN link policy on the SUT to Link Policy 3 (Enabled in S0, Sx/AC), if the WLAN network interface is available. 5. Ensure that only the Host OS Wake on LAN driver setting is enabled on the SUT; all other network wake sources must be disabled. This includes enabling ARP and/or NS Offload features where available to help prevent unexpected host wake events, and disabling the Host OS Wake on Wireless LAN driver settings, if available. 6. Verify that Intel® AMT on the SUT responds to version queries via all available network interfaces. 7. Ensure yellow bang is not seen on Drivers in Device Manager 8. Hibernate the SUT via the Host OS. 9. Verify that the SUT is in S4, S5/MeOn (CM3). 10. Verify that Intel® AMT on the SUT responds to version queries via all available network interfaces.
Procedure:	<ol style="list-style-type: none"> 1. Send three magic packets, at 2 second intervals, by means of the LAN network interface. 2. Verify that the SUT is in S0/MeOn (CM0). 3. Verify that the Host OS on the SUT is available. 4. Verify that Intel® AMT on the SUT responds to version queries via all available network interfaces. 5. Verify that windows booted from hibernate i.e. value should be 0x02. "run the following power shell command": Get-WinEvent -ProviderName Microsoft-Windows-Kernel-boot -MaxEvents 10 Where-Object {\$_.message -like "The boot type*"} 6. Verify that the second nibble of the FWSTS2 register on the SUT have a value of 0x68xxxxxx. 7. Ensure yellow bang is not seen on Drivers in Device Manager
Pass Criteria:	<p>The test passes if:</p> <ul style="list-style-type: none"> • the SUT moves from S4 to S0. • the Intel® CSME is in MeOn (CM0). • Intel® AMT responds to version queries via all available network interfaces.

ID:	ME_PM_12.2	
Title:	S4/CM3 to S0/CM0 via Power Button press (AC+DC, AC-only/PP2/LP3)	
Requirement:	Mandatory	Exemptions None
Method:	Automated by Intel® PETS	
Objective:	This test checks the SUT power flow from S4/CM3 to S0/CM0 via Power Button press with the parameters outlined below.	
Configuration:	<p>Intel® AMT should be provisioned via manual mode.</p> <p>This test assumes that either LAN-only, WLAN-only, or both LAN and WLAN network interfaces are available on the SUT. This test assumes that either LAN-only, or both LAN and WLAN network interfaces are available on the SUT.</p>	
Parameters:	System Power Source	
	Power States	Initial S4,S5/MeOn (CM3)
		Final S0/MeOn (CM0, CM0-PG)
		Trigger Power Button press
	Intel® AMT	Power Package PP2 (Intel® ME on in S0, wake in Sx/AC)
		WLAN Link Policy LP3 (Enabled in S0, Sx/AC) where available



ID:	ME_PM_12.2
Setup:	<ol style="list-style-type: none"> 1. Set the SUT power source to AC+DC where supported; otherwise AC-only. 2. Bring the SUT to the base state of S0/MeOn (CM0,CM0-PG), and confirm that the Host OS is available. 3. Set the active power package on the SUT to Power Package 2 (Intel® ME on in S0, wake in Sx/AC). 4. Set the Intel® AMT WLAN link policy on the SUT to Link Policy 3 (Enabled in S0, Sx/AC), if the WLAN network interface is available. 5. Ensure that the Host OS network device drivers are configured to not wake the SUT. This includes enabling ARP and/or NS Offload features where available to help prevent unexpected host wake events. 6. Verify that Intel® AMT on the SUT responds to version queries via all available network interfaces. 7. Ensure yellow bang is not seen on Drivers in Device Manager 8. Hibernate the SUT via the Host OS. 9. Verify that the SUT is in S4, S5/MeOn (CM3). 10. Verify that Intel® AMT on the SUT responds to version queries via all available network interfaces.
Procedure:	<ol style="list-style-type: none"> 1. Briefly press the Power Button on the SUT. 2. Verify that the SUT is in S0/MeOn (CM0,CM0-PG). 3. Verify that the Host OS on the SUT is available. 4. Verify that Intel® AMT on the SUT responds to version queries via all available network interfaces. 5. Verify that windows booted from hibernate i.e. value should be 0x02. "run the following power shell command": Get-WinEvent -ProviderName Microsoft-Windows-Kernel-boot -MaxEvents 10 Where-Object {\$_.message -like "The boot type*"} 6. Verify that the second nibble of the FWSTS2 register on the SUT have a value of 0x68xxxxxx. 7. Ensure yellow bang is not seen on Drivers in Device Manager
Pass Criteria:	<p>The test passes if:</p> <ul style="list-style-type: none"> • the SUT moves from S4 to S0. • the Intel® CSME is in MeOn (CM0, CM0-PG). • Intel® AMT responds to version queries via all available network interfaces.

ID:	ME_PM_12.4		
Title:	S5/CM3 to S0/CM0 via magic packet (AC+DC, AC-only/PP2/LP3)		
Requirement:	Mandatory	Exemptions	<input checked="" type="checkbox"/> Systems without WoL and/or WoWLAN support
			<input checked="" type="checkbox"/> Systems with a WLAN-only network interface
Method:	Automated by Intel® PETS		
Objective:	This test checks the SUT power flow from S5/CM3 to S0/CM0 via magic packet with the parameters outlined below.		
Configuration:	Intel® AMT should be provisioned via manual mode. This test assumes that either LAN-only, or both LAN and WLAN network interfaces are available on the SUT.		
Parameters:	System Power Source		AC+DC or AC-only
	Power States	Initial	S5/MeOn (CM3)
		Final	S0/MeOn (CM0)
		Trigger	Magic Packet receipt
	Intel® AMT	Power Package	PP2 (Intel® ME on in S0, wake in Sx/AC)
		WLAN Link Policy	LP3 (Enabled in S0, Sx/AC) where available



ID:	ME_PM_12.4
Setup:	<ol style="list-style-type: none"> 1. Set the SUT power source to AC+DC where supported; otherwise AC-only. 2. Bring the SUT to the base state of S0/MeOn (CM0), and confirm that the Host OS is available. 3. Set the active power package on the SUT to Power Package 2 (Intel® ME on in S0, wake in Sx/AC). 4. Set the Intel® AMT WLAN link policy on the SUT to Link Policy 3 (Enabled in S0, Sx/AC), if the WLAN network interface is available. 5. Ensure that only the Host OS Wake on LAN driver setting is enabled on the SUT; all other network wake sources must be disabled. This includes enabling ARP and/or NS Offload features where available to help prevent unexpected host wake events, and disabling the Host OS Wake on Wireless LAN driver settings, if available. 6. Verify that Intel® AMT on the SUT responds to version queries via all available network interfaces. 7. Ensure yellow bang is not seen on Drivers in Device Manager 8. Shutdown the SUT via the Host OS. 9. Verify that the SUT is in S5/MeOn (CM3). 10. Verify that Intel® AMT on the SUT responds to version queries via all available network interfaces.
Procedure:	<ol style="list-style-type: none"> 1. Send three magic packets, at 2 second intervals, by means of the LAN network interface. 2. Verify that the SUT is in S0/MeOn (CM0). 3. Verify that the Host OS on the SUT is available. 4. Verify that Intel® AMT on the SUT responds to version queries via all available network interfaces. 5. Verify that the second nibble of the FWSTS2 register on the SUT have a value of 0x68xxxxxx. 6. Ensure yellow bang is not seen on Drivers in Device Manager
Pass Criteria:	<p>The test passes if:</p> <ul style="list-style-type: none"> • the SUT moves from S5 to S0. • the Intel® CSME is in MeOn (CM0). • Intel® AMT responds to version queries via all available network interfaces.

ID:	ME_PM_12.5	
Title:	S5/CM3 to S0/CM0 via Power Button press (AC+DC, AC-only/PP2/LP3)	
Requirement:	Mandatory	Exemptions None
Method:	Automated by Intel® PETS	
Objective:	This test checks the SUT power flow from S5/CM3 to S0/CM0 via Power Button press with the parameters outlined below.	
Configuration:	<p>Intel® AMT should be provisioned via manual mode.</p> <p>Confirm that the Host OS is configured to shutdown the SUT upon Power Button press.</p> <p>This test assumes that either LAN-only, WLAN-only, or both LAN and WLAN network interfaces are available on the SUT.</p>	
Parameters:	System Power Source	
	AC+DC or AC-only	
	Power States	Initial S5/MeOn (CM3)
		Final S0/MeOn (CM0, CM0-PG)
		Trigger Power Button press
Intel® AMT	Power Package	PP2 (Intel® ME on in S0, wake in Sx/AC)
	WLAN Link Policy	LP3 (Enabled in S0, Sx/AC) where available



ID:	ME_PM_12.5
Setup:	<ol style="list-style-type: none"> 1. Set the SUT power source to AC+DC where supported; otherwise AC-only. 2. Bring the SUT to the base state of S0/MeOn (CM0,CM0-PG), and confirm that the Host OS is available. 3. Set the active power package on the SUT to Power Package 2 (Intel® ME on in S0, wake in Sx/AC). 4. Set the Intel® AMT WLAN link policy on the SUT to Link Policy 3 (Enabled in S0, Sx/AC), if the WLAN network interface is available. 5. Ensure that the Host OS network device drivers are configured to not wake the SUT. This includes enabling ARP and/or NS Offload features where available to help prevent unexpected host wake events. 6. Verify that Intel® AMT on the SUT responds to version queries via all available network interfaces. 7. Ensure yellow bang is not seen on Drivers in Device Manager 8. Shutdown the SUT via the brief Power Button press. 9. Verify that the SUT is in S5/MeOn (CM3). 10. Verify that Intel® AMT on the SUT responds to version queries via all available network interfaces.
Procedure:	<ol style="list-style-type: none"> 1. Briefly press the Power Button on the SUT. 2. Verify that the SUT is in S0/MeOn (CM0,CM0-PG). 3. Verify that the Host OS on the SUT is available. 4. Verify that Intel® AMT on the SUT responds to version queries via all available network interfaces. 5. Verify that the second nibble of the FWSTS2 register on the SUT have a value of 0x68xxxxxx. 6. Ensure yellow bang is not seen on Drivers in Device Manager
Pass Criteria:	The test passes if: <ul style="list-style-type: none"> • the SUT moves from S5 to S0. • the Intel® CSME is in MeOn (CM0, CM0-PG). • Intel® AMT responds to version queries via all available network interfaces.

ID:	ME_PM_12.21		
Title:	S4/CM3 to S0/CM0 via magic packet (AC+DC, AC-only/PP2/LP2)		
Requirement:	Mandatory	Exemptions	<div><input checked="" type="checkbox"/> Systems without WoL and/or WoWLAN support</div> <div><input checked="" type="checkbox"/> Systems with a WLAN-only network interface</div>
Method:	Automated by Intel® PETS		
Objective:	This test checks the SUT power flow from S4/CM3 to S0/CM0 via magic packet with the parameters outlined below.		
Configuration:	Intel® AMT should be provisioned via manual mode. This test assumes that either LAN-only, or both LAN and WLAN network interfaces are available on the SUT.		
Parameters:	System Power Source		AC+DC or AC-only
	Power States	Initial	S4,S5/MeOn (CM3)
		Final	S0/MeOn (CM0)
		Trigger	Magic Packet receipt
	Intel® AMT	Power Package	PP2 (Intel® ME on in S0, wake in Sx/AC)
		WLAN Link Policy	LP2 (Enabled in S0) where available



ID:	ME_PM_12.21
Setup:	<ol style="list-style-type: none"> 1. Set the SUT power source to AC+DC where supported; otherwise AC-only. 2. Bring the SUT to the base state of S0/MeOn (CM0), and confirm that the Host OS is available. 3. Set the active power package on the SUT to Power Package 2 (Intel® ME on in S0, wake in Sx/AC). 4. Set the Intel® AMT WLAN link policy on the SUT to Link Policy 2 (Enabled in S0), if the WLAN network interface is available. 5. Ensure that only the Host OS Wake on LAN driver setting is enabled on the SUT; all other network wake sources must be disabled. This includes enabling ARP and/or NS Offload features where available to help prevent unexpected host wake events, and disabling the Host OS Wake on Wireless LAN driver settings, if available. 6. Verify that Intel® AMT on the SUT responds to version queries via all available network interfaces. 7. Ensure yellow bang is not seen on Drivers in Device Manager 8. Hibernate the SUT via the Host OS. 9. Verify that the SUT is in S4, S5/MeOn (CM3). 10. Verify that Intel® AMT on the SUT responds to version query via the LAN network interface. 11. Verify that Intel® AMT on the SUT does not respond to version query via the WLAN network interface, if available.
Procedure:	<ol style="list-style-type: none"> 1. Send three magic packets, at 2 second intervals, by means of the LAN network interface. 2. Verify that the SUT is in S0/MeOn (CM0). 3. Verify that the Host OS on the SUT is available. 4. Verify that Intel® AMT on the SUT responds to version queries via all available network interfaces. 5. Verify that windows booted from hibernate i.e. value should be 0x02. "run the following power shell command": Get-WinEvent -ProviderName Microsoft-Windows-Kernel-boot -MaxEvents 10 Where-Object {\$_.message -like "The boot type*"} 6. Verify that the second nibble of the FWSTS2 register on the SUT have a value of 0x68xxxxxx. 7. Ensure yellow bang is not seen on Drivers in Device Manager
Pass Criteria:	<p>The test passes if:</p> <ul style="list-style-type: none"> • the SUT moves from S4 to S0. • the Intel® CSME is in MeOn (CM0). • Intel® AMT responds to version queries via all available network interfaces.

ID:	ME_PM_12.22	
Title:	S4/CM3 to S0/CM0 via Power Button press (AC+DC, AC-only/PP2/LP2)	
Requirement:	Mandatory	Exemptions <input checked="" type="checkbox"/> Systems with a LAN-only network interface
Method:	Automated by Intel® PETS	
Objective:	This test checks the SUT power flow from S4/CM3 to S0/CM0 via Power Button press with the parameters outlined below.	
Configuration:	Intel® AMT should be provisioned via manual mode. This test assumes that either WLAN-only, or both LAN and WLAN network interfaces are available on the SUT.	
Parameters:	System Power Source	
	Power States	Initial S4,S5/MeOn (CM3)
		Final S0/MeOn (CM0, CM0-PG)
		Trigger Power Button press
	Intel® AMT	Power Package PP2 (Intel® ME on in S0, wake in Sx/AC)
		WLAN Link Policy LP2 (Enabled in S0)



ID:	ME_PM_12.22
Setup:	<ol style="list-style-type: none"> 1. Set the SUT power source to AC+DC where supported; otherwise AC-only. 2. Bring the SUT to the base state of S0/MeOn (CM0,CM0-PG), and confirm that the Host OS is available. 3. Set the active power package on the SUT to Power Package 2 (Intel® ME on in S0, wake in Sx/AC). 4. Set the Intel® AMT WLAN link policy on the SUT to Link Policy 2 (Enabled in S0). 5. Ensure that the Host OS network device drivers are configured to not wake the SUT. This includes enabling ARP and/or NS Offload features where available to help prevent unexpected host wake events. 6. Verify that Intel® AMT on the SUT responds to version queries via all available network interfaces. 7. Ensure yellow bang is not seen on Drivers in Device Manager 8. Hibernate the SUT via the Host OS. 9. Verify that the SUT is in S4, S5/MeOn (CM3). 10. Verify that Intel® AMT on the SUT responds to version query via the LAN network interface, if available. 11. Verify that Intel® AMT on the SUT does not respond to version query via the WLAN network interface.
Procedure:	<ol style="list-style-type: none"> 1. Briefly press the Power Button on the SUT. 2. Verify that the SUT is in S0/MeOn (CM0,CM0-PG). 3. Verify that the Host OS on the SUT is available. 4. Verify that Intel® AMT on the SUT responds to version queries via all available network interfaces. 5. Verify that windows booted from hibernate i.e. value should be 0x02. "run the following power shell command": Get-WinEvent -ProviderName Microsoft-Windows-Kernel-boot -MaxEvents 10 Where-Object {\$_.message -like "The boot type*"} 6. Verify that the second nibble of the FWSTS2 register on the SUT have a value of 0x68xxxxxx. 7. Ensure yellow bang is not seen on Drivers in Device Manager
Pass Criteria:	<p>The test passes if:</p> <ul style="list-style-type: none"> • the SUT moves from S4 to S0. • the Intel® CSME is in MeOn (CM0-PG). • Intel® AMT responds to version queries via all available network interfaces.

ID:	ME_PM_12.24		
Title:	S5/CM3 to S0/CM0 via magic packet (AC+DC, AC-only/PP2/LP2)		
Requirement:	Mandatory	Exemptions	<div><input checked="" type="checkbox"/> Systems without WoL and/or WoWLAN support</div> <div><input checked="" type="checkbox"/> Systems with a WLAN-only network interface</div>
Method:	Automated by Intel® PETS		
Objective:	This test checks the SUT power flow from S5/CM3 to S0/CM0 via magic packet with the parameters outlined below.		
Configuration:	Intel® AMT should be provisioned via manual mode. This test assumes that either LAN-only, or both LAN and WLAN network interfaces are available on the SUT.		
Parameters:	System Power Source		AC+DC or AC-only
	Power States	Initial	S5/MeOn (CM3)
		Final	S0/MeOn (CM0)
		Trigger	Magic Packet receipt
	Intel® AMT	Power Package	PP2 (Intel® ME on in S0, wake in Sx/AC)
		WLAN Link Policy	LP2 (Enabled in S0) where available



ID:	ME_PM_12.24
Setup:	<ol style="list-style-type: none"> 1. Set the SUT power source to AC+DC where supported; otherwise AC-only. 2. Bring the SUT to the base state of S0/MeOn (CM0), and confirm that the Host OS is available. 3. Set the active power package on the SUT to Power Package 2 (Intel® ME on in S0, wake in Sx/AC). 4. Set the Intel® AMT WLAN link policy on the SUT to Link Policy 2 (Enabled in S0), if the WLAN network interface is available. 5. Ensure that only the Host OS Wake on LAN driver setting is enabled on the SUT; all other network wake sources must be disabled. This includes enabling ARP and/or NS Offload features where available to help prevent unexpected host wake events, and disabling the Host OS Wake on Wireless LAN driver settings, if available. 6. Verify that Intel® AMT on the SUT responds to version queries via all available network interfaces. 7. Ensure yellow bang is not seen on Drivers in Device Manager 8. Shutdown the SUT via the Host OS. 9. Verify that the SUT is in S5/MeOn (CM3). 10. Verify that Intel® AMT on the SUT responds to version query via the LAN network interface. 11. Verify that Intel® AMT on the SUT does not respond to version query via the WLAN network interface, if available.
Procedure:	<ol style="list-style-type: none"> 1. Send three magic packets, at 2 second intervals, by means of the LAN network interface. 2. Verify that the SUT is in S0/MeOn (CM0). 3. Verify that the Host OS on the SUT is available. 4. Verify that Intel® AMT on the SUT responds to version queries via all available network interfaces. 5. Verify that the second nibble of the FWSTS2 register on the SUT have a value of 0x68xxxxxx. 6. Ensure yellow bang is not seen on Drivers in Device Manager
Pass Criteria:	<p>The test passes if:</p> <ul style="list-style-type: none"> • the SUT moves from S5 to S0. • the Intel® CSME is in MeOn (CM0). • Intel® AMT responds to version queries via all available network interfaces.

ID:	ME_PM_12.25	
Title:	S5/CM3 to S0/CM0 via Power Button press (AC+DC, AC-only/PP2/LP2)	
Requirement:	Mandatory	Exemptions <input checked="" type="checkbox"/> Systems with a LAN-only network interface
Method:	Automated by Intel® PETS	
Objective:	This test checks the SUT power flow from S5/CM3 to S0/CM0 via Power Button press with the parameters outlined below.	
Configuration:	<p>Intel® AMT should be provisioned via manual mode.</p> <p>Confirm that the Host OS is configured to shutdown the SUT upon Power Button press.</p> <p>This test assumes that either WLAN-only, or both LAN and WLAN network interfaces are available on the SUT.</p>	
Parameters:	System Power Source AC+DC or AC-only	
	Power States	Initial S5/MeOn (CM3)
		Final S0/MeOn (CM0, CM0-PG)
		Trigger Power Button press
	Intel® AMT	Power Package PP2 (Intel® ME on in S0, wake in Sx/AC)
		WLAN Link Policy LP2 (Enabled in S0)



ID:	ME_PM_12.25
Setup:	<ol style="list-style-type: none"> 1. Set the SUT power source to AC+DC where supported; otherwise AC-only. 2. Bring the SUT to the base state of S0/MeOn (CM0,CM0-PG), and confirm that the Host OS is available. 3. Set the active power package on the SUT to Power Package 2 (Intel® ME on in S0, wake in Sx/AC). 4. Set the Intel® AMT WLAN link policy on the SUT to Link Policy 2 (Enabled in S0). 5. Ensure that the Host OS network device drivers are configured to not wake the SUT. This includes enabling ARP and/or NS Offload features where available to help prevent unexpected host wake events. 6. Verify that Intel® AMT on the SUT responds to version queries via all available network interfaces. 7. Ensure yellow bang is not seen on Drivers in Device Manager 8. Briefly press the Power Button on the SUT. 9. Verify that the SUT is in S5/MeOn (CM3). 10. Verify that Intel® AMT on the SUT responds to version query via the LAN network interface, if available. 11. Verify that Intel® AMT on the SUT does not respond to version query via the WLAN network interface.
Procedure:	<ol style="list-style-type: none"> 1. Briefly press the Power Button on the SUT. 2. Verify that the SUT is in S0/MeOn (CM0,CM0-PG). 3. Verify that the Host OS on the SUT is available. 4. Verify that Intel® AMT on the SUT responds to version queries via all available network interfaces. 5. Verify that the second nibble of the FWSTS2 register on the SUT have a value of 0x68xxxxxx. 6. Ensure yellow bang is not seen on Drivers in Device Manager
Pass Criteria:	<p>The test passes if:</p> <ul style="list-style-type: none"> • the SUT moves from S5 to S0. • the Intel® CSME is in MeOn (CM0, CM0-PG). • Intel® AMT responds to version queries via all available network interfaces.

12.16 ME_PM_13: S4-S5/CM3 to S4-S5/CM-Off (Without Intel® CSME Wake)

ID:	ME_PM_13.1		
Title:	S4/CM3 to S4/CM3-PG with Ac Wake via AC-detach (AC+DC/PP2/LP3)		
Requirement:	Mandatory	Exemptions	<input checked="" type="checkbox"/> Non-Mobile (AC-only) systems
Method:	Automated by Intel® PETS		
Objective:	This test checks the SUT power flow from S4/CM3 to S4/CM3-PG with AC Wake via AC-detach with the parameters outlined below.		
Configuration:	<p>Intel® AMT should be provisioned via manual mode.</p> <p>If Deep S4, Deep S5, and/or G3 are supported on the SUT, please confirm the following:</p> <ul style="list-style-type: none">the SUT and/or BIOS are properly configured to permit Deep S4/S5 or G3 entry.the correct Deep Sx policy is applied to the SUT profile in Intel® PETS. <p>This test assumes that either LAN-only, WLAN-only, or both LAN and WLAN network interfaces are available on the SUT.</p>		
Parameters:	System Power Source		AC+DC
	Power States	Initial	S4,S5/MeOn (CM3)
		Final	S4,S5,Deep S4,Deep S5,G3/CM3-PG with AC Wake
		Trigger	AC-detach
	Intel® AMT	Power Package	PP2 (Intel® ME on in S0, wake in Sx/AC)
		WLAN Link Policy	LP3 (Enabled in S0, Sx/AC) where available



ID:	ME_PM_13.1
Setup:	<ol style="list-style-type: none"> 1. Set the SUT power source to AC+DC. 2. Bring the SUT to the base state of S0/MeOn (CM0,CM0-PG), and confirm that the Host OS is available. 3. Verify that a DC battery is connected to the SUT, and that it is charged. 4. Set the active power package on the SUT to Power Package 2 (Intel® ME on in S0, wake in Sx/AC). 5. Set the Intel® AMT WLAN link policy on the SUT to Link Policy 3 (Enabled in S0, Sx/AC), if the WLAN network interface is available. 6. Ensure that the Host OS network device drivers are configured to not wake the SUT. This includes enabling ARP and/or NS Offload features where available to help prevent unexpected host wake events. 7. Verify that Intel® AMT on the SUT responds to version queries via all available network interfaces. 8. Hibernate the SUT via the Host OS. 9. Verify that the SUT is in S4, S5/MeOn (CM3). 10. Verify that Intel® AMT on the SUT responds to version queries via all available network interfaces.
Procedure:	<ol style="list-style-type: none"> 1. Set the SUT power source to DC-only. 2. Verify that the SUT is in S4, S5, Deep S4, Deep S5, G3/CM3-PG.with AC Wake
Pass Criteria:	The test passes if the SUT remains in S4 or S5 (or moves to Deep S4, Deep S5, or G3), and the Intel® CSME moves to CM3-PG with AC Wake.

ID:	ME_PM_13.2		
Title:	S4/CM3 to S4/CM-Off via Intel® AMT Power Package change (AC+DC, AC-only/PP2/LP3)		
Requirement:	Mandatory	Exemptions	None
Method:	Automated by Intel® PETS		
Objective:	This test checks the SUT power flow from S4/CM3 to S4/CM-Off via Intel® AMT Power Package change with the parameters outlined below.		
Configuration:	Intel® AMT should be provisioned via manual mode. If Deep S4, Deep S5, and/or G3 are supported on the SUT, please confirm the following: <ul style="list-style-type: none">the SUT and/or BIOS are properly configured to permit Deep S4/S5 or G3 entry.the correct Deep Sx policy is applied to the SUT profile in Intel® PETS. This test assumes that either LAN-only, WLAN-only, or both LAN and WLAN network interfaces are available on the SUT.		
Parameters:	System Power Source		AC+DC or AC-only
	Power States	Initial	S4,S5/MeOn (CM3)
		Final	S4, S5, Deep S4, Deep S5, G3/MeOff (CM-Off)
		Trigger	Set Intel® AMT PP1 (Intel® ME on in S0)
	Intel® AMT	Power Package	PP2 (Intel® ME on in S0, wake in Sx/AC)
		WLAN Link Policy	LP3 (Enabled in S0, Sx/AC) where available
Setup:	<ol style="list-style-type: none">Set the SUT power source to AC+DC where supported; otherwise AC-only.Bring the SUT to the base state of S0/MeOn (CM0,CM0-PG), and confirm that the Host OS is available.Set the active power package on the SUT to Power Package 2 (Intel® ME on in S0, wake in Sx/AC).Set the Intel® AMT WLAN link policy on the SUT to Link Policy 3 (Enabled in S0, Sx/AC), if the WLAN network interface is available.Ensure that the Host OS network device drivers are configured to not wake the SUT. This includes enabling ARP and/or NS Offload features where available to help prevent unexpected host wake events.Verify that Intel® AMT on the SUT responds to version queries via all available network interfaces.Hibernate the SUT via the Host OS.Verify that the SUT is in S4, S5/MeOn (CM3).Verify that Intel® AMT on the SUT responds to version queries via all available network interfaces.		
Procedure:	<ol style="list-style-type: none">Set the active power package on the SUT to Power Package 1 (Intel® ME on in S0).Verify that the SUT is in S4, S5, Deep S4, Deep S5, G3/MeOff (CM-Off).		



ID:	ME_PM_13.2
Pass Criteria:	The test passes if the SUT remains in S4 or S5 (or moves to Deep S4, Deep S5, or G3), and the Intel® CSME moves to MeOff (CM-Off).

ID:	ME_PM_13.3		
Title:	S5/CM3 to S5/CM3-PG with AC Wake via AC-detach (AC+DC/PP2/LP3)		
Requirement:	Mandatory	Exemptions	<input checked="" type="checkbox"/> Non-Mobile (AC-only) systems
Method:	Automated by Intel® PETS		
Objective:	This test checks the SUT power flow from S5/CM3 to S5/CM3-PG with AC Wake via AC-detach with the parameters outlined below.		
Configuration:	<p>Intel® AMT should be provisioned via manual mode.</p> <p>If Deep S5 and/or G3 are supported on the SUT, please confirm the following:</p> <ul style="list-style-type: none"> the SUT and/or BIOS are properly configured to permit Deep S5 or G3 entry. the correct Deep Sx policy is applied to the SUT profile in Intel® PETS. <p>This test assumes that either LAN-only, WLAN-only, or both LAN and WLAN network interfaces are available on the SUT.</p>		
Parameters:	System Power Source		AC+DC
	Power States	Initial	S5/MeOn (CM3)
		Final	S5,Deep S5,G3/CM3-PG with Ac Wake
		Trigger	AC-detach
	Intel® AMT	Power Package	PP2 (Intel® ME on in S0, wake in Sx/AC)
		WLAN Link Policy	LP3 (Enabled in S0, Sx/AC) where available
Setup:	<ol style="list-style-type: none"> Set the SUT power source to AC+DC. Bring the SUT to the base state of S0/MeOn (CM0,CM0-PG), and confirm that the Host OS is available. Verify that a DC battery is connected to the SUT, and that it is charged. Set the active power package on the SUT to Power Package 2 (Intel® ME on in S0, wake in Sx/AC). Set the Intel® AMT WLAN link policy on the SUT to Link Policy 3 (Enabled in S0, Sx/AC), if the WLAN network interface is available. Ensure that the Host OS network device drivers are configured to not wake the SUT. This includes enabling ARP and/or NS Offload features where available to help prevent unexpected host wake events. Verify that Intel® AMT on the SUT responds to version queries via all available network interfaces. Shutdown the SUT via the Host OS. Verify that the SUT is in S5/MeOn (CM3). Verify that Intel® AMT on the SUT responds to version queries via all available network interfaces. 		
Procedure:	<ol style="list-style-type: none"> Set the SUT power source to DC-only. Verify that the SUT is in S5, Deep S5, G3/CM3-PG.with AC Wake 		
Pass Criteria:	The test passes if the SUT remains in S5 (or moves to Deep S5 or G3), and the Intel® CSME moves to CM3-PG with AC Wake.		

ID:	ME_PM_13.4		
Title:	S5/CM3 to S5/CM-Off via Intel® AMT Power Package change (AC+DC, AC-only/PP2/LP3)		
Requirement:	Mandatory	Exemptions	None
Method:	Automated by Intel® PETS		
Objective:	This test checks the SUT power flow from S5/CM3 to S5/CM-Off via Intel® AMT Power Package change with the parameters outlined below.		



ID:	ME_PM_13.4																
Configuration:	<p>Intel® AMT should be provisioned via manual mode.</p> <p>If Deep S5 and/or G3 are supported on the SUT, please confirm the following:</p> <ul style="list-style-type: none"> the SUT and/or BIOS are properly configured to permit Deep S5 or G3 entry. the correct Deep Sx policy is applied to the SUT profile in Intel® PETS. <p>This test assumes that either LAN-only, WLAN-only, or both LAN and WLAN network interfaces are available on the SUT.</p>																
Parameters:	<table> <tr> <td colspan="2">System Power Source</td><td>AC+DC or AC-only</td></tr> <tr> <td rowspan="3">Power States</td><td>Initial</td><td>S5/MeOn (CM3)</td></tr> <tr> <td>Final</td><td>S5, Deep S5, G3/MeOff (CM-Off)</td></tr> <tr> <td>Trigger</td><td>Set Intel® AMT PP1 (Intel® ME on in S0)</td></tr> <tr> <td rowspan="2">Intel® AMT</td><td>Power Package</td><td>PP2 (Intel® ME on in S0, wake in Sx/AC)</td></tr> <tr> <td>WLAN Link Policy</td><td>LP3 (Enabled in S0, Sx/AC) where available</td></tr> </table>	System Power Source		AC+DC or AC-only	Power States	Initial	S5/MeOn (CM3)	Final	S5, Deep S5, G3/MeOff (CM-Off)	Trigger	Set Intel® AMT PP1 (Intel® ME on in S0)	Intel® AMT	Power Package	PP2 (Intel® ME on in S0, wake in Sx/AC)	WLAN Link Policy	LP3 (Enabled in S0, Sx/AC) where available	
System Power Source		AC+DC or AC-only															
Power States	Initial	S5/MeOn (CM3)															
	Final	S5, Deep S5, G3/MeOff (CM-Off)															
	Trigger	Set Intel® AMT PP1 (Intel® ME on in S0)															
Intel® AMT	Power Package	PP2 (Intel® ME on in S0, wake in Sx/AC)															
	WLAN Link Policy	LP3 (Enabled in S0, Sx/AC) where available															
Setup:	<ol style="list-style-type: none"> Set the SUT power source to AC+DC. Bring the SUT to the base state of S0/MeOn (CM0,CM0-PG), and confirm that the Host OS is available. Set the active power package on the SUT to Power Package 2 (Intel® ME on in S0, wake in Sx/AC). Set the Intel® AMT WLAN link policy on the SUT to Link Policy 3 (Enabled in S0, Sx/AC), if the WLAN network interface is available. Ensure that the Host OS network device drivers are configured to not wake the SUT. This includes enabling ARP and/or NS Offload features where available to help prevent unexpected host wake events. Verify that Intel® AMT on the SUT responds to version queries via all available network interfaces. Shutdown the SUT via the Host OS. Verify that the SUT is in S5/MeOn (CM3). Verify that Intel® AMT on the SUT responds to version queries via all available network interfaces. 																
Procedure:	<ol style="list-style-type: none"> Set the active power package on the SUT to Power Package 1 (Intel® ME on in S0). Verify that the SUT is in S5, Deep S5, G3/MeOff (CM-Off). 																
Pass Criteria:	The test passes if the SUT remains in S5 (or moves to Deep S5 or G3), and the Intel® CSME moves to MeOff (CM-Off).																

ID:	ME_PM_13.21																
Title:	S4/CM3 to S4/CM3-PG with AC wake via AC-detach (AC+DC/PP2/LP2)																
Requirement:	Mandatory	Exemptions <ul style="list-style-type: none"> <input checked="" type="checkbox"/> Non-Mobile (AC-only) systems <input checked="" type="checkbox"/> Systems with a LAN-only network interface 															
Method:	Automated by Intel® PETS																
Objective:	This test checks the SUT power flow from S4/CM3 to S4/CM-Off via AC-detach with the parameters outlined below.																
Configuration:	<p>Intel® AMT should be provisioned via manual mode.</p> <p>If Deep S4, Deep S5, and/or G3 are supported on the SUT, please confirm the following:</p> <ul style="list-style-type: none"> the SUT and/or BIOS are properly configured to permit Deep S4/S5 or G3 entry. the correct Deep Sx policy is applied to the SUT profile in Intel® PETS. <p>This test assumes that either WLAN-only, or both LAN and WLAN network interfaces are available on the SUT.</p>																
Parameters:	<table> <tr> <td colspan="2">System Power Source</td><td>AC+DC</td></tr> <tr> <td rowspan="3">Power States</td><td>Initial</td><td>S4,S5/MeOn (CM3)</td></tr> <tr> <td>Final</td><td>S4,S5,Deep S4,Deep S5,G3/CM3-PG with AC Wake</td></tr> <tr> <td>Trigger</td><td>AC-detach</td></tr> <tr> <td rowspan="2">Intel® AMT</td><td>Power Package</td><td>PP2 (Intel® ME on in S0, wake in Sx/AC)</td></tr> <tr> <td>WLAN Link Policy</td><td>LP2 (Enabled in S0)</td></tr> </table>	System Power Source		AC+DC	Power States	Initial	S4,S5/MeOn (CM3)	Final	S4,S5,Deep S4,Deep S5,G3/CM3-PG with AC Wake	Trigger	AC-detach	Intel® AMT	Power Package	PP2 (Intel® ME on in S0, wake in Sx/AC)	WLAN Link Policy	LP2 (Enabled in S0)	
System Power Source		AC+DC															
Power States	Initial	S4,S5/MeOn (CM3)															
	Final	S4,S5,Deep S4,Deep S5,G3/CM3-PG with AC Wake															
	Trigger	AC-detach															
Intel® AMT	Power Package	PP2 (Intel® ME on in S0, wake in Sx/AC)															
	WLAN Link Policy	LP2 (Enabled in S0)															



ID:	ME_PM_13.21
Setup:	<ol style="list-style-type: none"> 1. Set the SUT power source to AC+DC. 2. Bring the SUT to the base state of S0/MeOn (CM0,CM0-PG), and confirm that the Host OS is available. 3. Verify that a DC battery is connected to the SUT, and that it is charged. 4. Set the active power package on the SUT to Power Package 2 (Intel® ME on in S0, wake in Sx/AC). 5. Set the Intel® AMT WLAN link policy on the SUT to Link Policy 2 (Enabled in S0). 6. Ensure that the Host OS network device drivers are configured to not wake the SUT. This includes enabling ARP and/or NS Offload features where available to help prevent unexpected host wake events. 7. Verify that Intel® AMT on the SUT responds to version queries via all available network interfaces. 8. Hibernate the SUT via the Host OS. 9. Verify that the SUT is in S4, S5/MeOn (CM3). 10. Verify that Intel® AMT on the SUT responds to version query via the LAN network interface, if available. 11. Verify that Intel® AMT on the SUT does not respond to version query via the WLAN network interface.
Procedure:	<ol style="list-style-type: none"> 1. Set the SUT power source to DC-only. 2. Verify that the SUT is in S4, S5, Deep S4, Deep S5, G3/CM3-PG.with AC Wake
Pass Criteria:	The test passes if the SUT remains in S4 or S5 (or moves to Deep S4, Deep S5, or G3), and the Intel® CSME moves to CM3-PG with AC Wake.

ID:	ME_PM_13.22		
Title:	S4/CM3 to S4/CM-Off via Intel® AMT Power Package change (AC+DC, AC-only/PP2/LP2)		
Requirement:	Mandatory	Exemptions	<input checked="" type="checkbox"/> Systems with a single network interface (not LAN+WLAN)
Method:	Automated by Intel® PETS		
Objective:	This test checks the SUT power flow from S4/CM3 to S4/CM-Off via Intel® AMT Power Package change with the parameters outlined below.		
Configuration:	Intel® AMT should be provisioned via manual mode. If Deep S4, Deep S5, and/or G3 are supported on the SUT, please confirm the following: <ul style="list-style-type: none">the SUT and/or BIOS are properly configured to permit Deep S4/S5 or G3 entry.the correct Deep Sx policy is applied to the SUT profile in Intel® PETS. This test assumes that both LAN and WLAN network interfaces are available on the SUT.		
Parameters:	System Power Source		AC+DC or AC-only
	Power States	Initial	S4,S5/MeOn (CM3)
		Final	S4, S5, Deep S4, Deep S5, G3/MeOff (CM-Off)
		Trigger	Set Intel® AMT PP1 (Intel® ME on in S0)
	Intel® AMT	Power Package	PP2 (Intel® ME on in S0, wake in Sx/AC)
WLAN Link Policy		LP2 (Enabled in S0)	
Setup:	<ol style="list-style-type: none">Set the SUT power source to AC+DC where supported; otherwise AC-only.Bring the SUT to the base state of S0/MeOn (CM0), and confirm that the Host OS is available.Set the active power package on the SUT to Power Package 2 (Intel® ME on in S0, wake in Sx/AC).Set the Intel® AMT WLAN link policy on the SUT to Link Policy 2 (Enabled in S0).Ensure that the Host OS network device drivers are configured to not wake the SUT. This includes enabling ARP and/or NS Offload features where available to help prevent unexpected host wake events.Verify that Intel® AMT on the SUT responds to version queries via all available network interfaces.Hibernate the SUT via the Host OS.Verify that the SUT is in S4, S5/MeOn (CM3).Verify that Intel® AMT on the SUT responds to version query via the LAN network interface.Verify that Intel® AMT on the SUT does not respond to version query via the WLAN network interface.		
Procedure:	<ol style="list-style-type: none">Set the active power package on the SUT to Power Package 1 (Intel® ME on in S0).Verify that the SUT is in S4, S5, Deep S4, Deep S5, G3/MeOff (CM-Off).		



ID:	ME_PM_13.22
Pass Criteria:	The test passes if the SUT remains in S4 or S5 (or moves to Deep S4, Deep S5, or G3), and the Intel® CSME moves to MeOff (CM-Off).

ID:	ME_PM_13.23		
Title:	S5/CM3 to S5/CM3-PG with AC Wake via AC-detach (AC+DC/PP2/LP2)		
Requirement:	Mandatory	Exemptions	<input checked="" type="checkbox"/> Non-Mobile (AC-only) systems <input checked="" type="checkbox"/> Systems with a LAN-only network interface
Method:	Automated by Intel® PETS		
Objective:	This test checks the SUT power flow from S5/CM3 to S5/CM-Off via AC-detach with the parameters outlined below.		
Configuration:	Intel® AMT should be provisioned via manual mode. If Deep S5 and/or G3 are supported on the SUT, please confirm the following: <ul style="list-style-type: none">the SUT and/or BIOS are properly configured to permit Deep S5 or G3 entry.the correct Deep Sx policy is applied to the SUT profile in Intel® PETS. This test assumes that either WLAN-only, or both LAN and WLAN network interfaces are available on the SUT.		
Parameters:	System Power Source		AC+DC
	Power States	Initial	S5/MeOn (CM3)
		Final	S5,Deep S5,G3/CM3-PG with AC Wake
		Trigger	AC-detach
	Intel® AMT	Power Package	PP2 (Intel® ME on in S0, wake in Sx/AC)
		WLAN Link Policy	LP2 (Enabled in S0)
Setup:	<ol style="list-style-type: none">Set the SUT power source to AC+DC.Bring the SUT to the base state of S0/MeOn (CM0,CM0-PG), and confirm that the Host OS is available.Verify that a DC battery is connected to the SUT, and that it is charged.Set the active power package on the SUT to Power Package 2 (Intel® ME on in S0, wake in Sx/AC).Set the Intel® AMT WLAN link policy on the SUT to Link Policy 2 (Enabled in S0).Ensure that the Host OS network device drivers are configured to not wake the SUT. This includes enabling ARP and/or NS Offload features where available to help prevent unexpected host wake events.Verify that Intel® AMT on the SUT responds to version queries via all available network interfaces.Shutdown the SUT via the Host OS.Verify that the SUT is in S5/MeOn (CM3).Verify that Intel® AMT on the SUT responds to version query via the LAN network interface, if available.Verify that Intel® AMT on the SUT does not respond to version query via the WLAN network interface.		
Procedure:	<ol style="list-style-type: none">Set the SUT power source to DC-only.Verify that the SUT is in S5, Deep S5, G3/CM3-PG.with AC Wake		
Pass Criteria:	The test passes if the SUT remains in S5 (or moves to Deep S5 or G3), and the Intel® CSME moves to CM3-PG with AC Wake		

ID:	ME_PM_13.24		
Title:	S5/CM3 to S5/CM-Off via Intel® AMT Power Package change (AC+DC, AC-only/PP2/LP2)		
Requirement:	Mandatory	Exemptions	<input checked="" type="checkbox"/> Systems with a single network interface (not LAN+WLAN)
Method:	Automated by Intel® PETS		
Objective:	This test checks the SUT power flow from S5/CM3 to S5/CM-Off via Intel® AMT Power Package change with the parameters outlined below.		



ID:	ME_PM_13.24																	
Configuration:	<p>Intel® AMT should be provisioned via manual mode.</p> <p>If Deep S5 and/or G3 are supported on the SUT, please confirm the following:</p> <ul style="list-style-type: none">the SUT and/or BIOS are properly configured to permit Deep S5 or G3 entry.the correct Deep Sx policy is applied to the SUT profile in Intel® PETS. <p>This test assumes that both LAN and WLAN network interfaces are available on the SUT.</p>																	
Parameters:	<table><tr><td colspan="2">System Power Source</td><td>AC+DC or AC-only</td></tr><tr><td rowspan="3">Power States</td><td>Initial</td><td>S5/MeOn (CM3)</td></tr><tr><td>Final</td><td>S5, Deep S5, G3/MeOff (CM-Off)</td></tr><tr><td>Trigger</td><td>Set Intel® AMT PP1 (Intel® ME on in S0)</td></tr><tr><td rowspan="2">Intel® AMT</td><td>Power Package</td><td>PP2 (Intel® ME on in S0, wake in Sx/AC)</td></tr><tr><td>WLAN Link Policy</td><td>LP2 (Enabled in S0)</td></tr></table>			System Power Source		AC+DC or AC-only	Power States	Initial	S5/MeOn (CM3)	Final	S5, Deep S5, G3/MeOff (CM-Off)	Trigger	Set Intel® AMT PP1 (Intel® ME on in S0)	Intel® AMT	Power Package	PP2 (Intel® ME on in S0, wake in Sx/AC)	WLAN Link Policy	LP2 (Enabled in S0)
System Power Source		AC+DC or AC-only																
Power States	Initial	S5/MeOn (CM3)																
	Final	S5, Deep S5, G3/MeOff (CM-Off)																
	Trigger	Set Intel® AMT PP1 (Intel® ME on in S0)																
Intel® AMT	Power Package	PP2 (Intel® ME on in S0, wake in Sx/AC)																
	WLAN Link Policy	LP2 (Enabled in S0)																
Setup:	<ol style="list-style-type: none">Set the SUT power source to AC+DC.Bring the SUT to the base state of S0/MeOn (CM0), and confirm that the Host OS is available.Set the active power package on the SUT to Power Package 2 (Intel® ME on in S0, wake in Sx/AC).Set the Intel® AMT WLAN link policy on the SUT to Link Policy 2 (Enabled in S0).Ensure that the Host OS network device drivers are configured to not wake the SUT. This includes enabling ARP and/or NS Offload features where available to help prevent unexpected host wake events.Verify that Intel® AMT on the SUT responds to version queries via all available network interfaces.Shutdown the SUT via the Host OS.Verify that the SUT is in S5/MeOn (CM3).Verify that Intel® AMT on the SUT responds to version query via the LAN network interface.Verify that Intel® AMT on the SUT does not respond to version query via the WLAN network interface.																	
Procedure:	<ol style="list-style-type: none">Set the active power package on the SUT to Power Package 1 (Intel® ME on in S0).Verify that the SUT is in S5, Deep S5, G3/MeOff (CM-Off).																	
Pass Criteria:	The test passes if the SUT remains in S5 (or moves to Deep S5 or G3), and the Intel® CSME moves to MeOff (CM-Off).																	

12.17 ME_PM_14: S4-S5/CM3 to S4-S5/CM-Off (with Intel® CSME Wake)

ID:	ME_PM_14.1		
Title:	S4/CM3 to S4/CM3-PG via Intel® AMT idle timeout (AC+DC, AC-only/PP2/LP3)		
Requirement:	Mandatory	Exemptions	None
Method:	Automated by Intel® PETS		
Objective:	This test checks the SUT power flow from S4/CM3 to S4/CM3-PG via Intel® AMT idle timeout with the parameters outlined below.		
Configuration:	Intel® AMT should be provisioned via manual mode. This test assumes that either LAN-only, WLAN-only, or both LAN and WLAN network interfaces are available on the SUT.		
Parameters:	System Power Source		AC+DC or AC-only
	Power States	Initial	S4,S5/MeOn (CM3)
		Final	S4,S5/MeOff (CM3-PG)
		Trigger	Intel® AMT idle timeout
	Intel® AMT	Power Package	PP2 (Intel® ME on in S0, wake in Sx/AC)
		WLAN Link Policy	LP3 (Enabled in S0, Sx/AC) where available



ID:	ME_PM_14.1
Setup:	<ol style="list-style-type: none"> 1. Set the SUT power source to AC+DC where supported; otherwise AC-only. 2. Bring the SUT to the base state of S0/MeOn (CM0,CM0-PG), and confirm that the Host OS is available. 3. Set the active power package on the SUT to Power Package 2 (Intel® ME on in S0, wake in Sx/AC). 4. Set the Intel® AMT WLAN link policy on the SUT to Link Policy 3 (Enabled in S0, Sx/AC), if the WLAN network interface is available. 5. Ensure that the Host OS network device drivers are configured to not wake the SUT. This includes enabling ARP and/or NS Offload features where available to help prevent unexpected host wake events. 6. Ensure the Intel® AMT idle timeout on the SUT is set to 1 minute. 7. Verify that Intel® AMT on the SUT responds to version queries via all available network interfaces. 8. Hibernate the SUT via the Host OS. 9. Verify that the SUT is in S4, S5/MeOn (CM3). 10. Verify that Intel® AMT on the SUT responds to version queries via all available network interfaces.
Procedure:	<ol style="list-style-type: none"> 1. Wait for 3 minutes to allow the Intel® ME on the SUT to move to CM3-PG after Intel® AMT idle timeout. 2. Verify that the Intel® ME on the SUT is in CM3-PG.
Pass Criteria:	The test passes if the SUT remains in S4 or S5, and the Intel® CSME moves to CM3-PG.

ID:	ME_PM_14.2		
Title:	S5/CM3 to S5/CM3-PG via Intel® AMT idle timeout ((AC+DC, AC-only/PP2/LP2)AC-only/PP2/LP3)		
Requirement:	Mandatory	Exemptions	None
Method:	Automated by Intel® PETS		
Objective:	This test checks the SUT power flow from S5/CM3 to S5/CM-Off via Intel® AMT idle timeout with the parameters outlined below.		
Configuration:	Intel® AMT should be provisioned via manual mode. This test assumes that either LAN-only, WLAN-only, or both LAN and WLAN network interfaces are available on the SUT.		
Parameters:	System Power Source		AC+DC or AC-only
	Power States	Initial	S5/MeOn (CM3)
		Final	S5/MeOff (CM3-PG)
		Trigger	Intel® AMT idle timeout
	Intel® AMT	Power Package	PP2 (Intel® ME on in S0, wake in Sx/AC)
		WLAN Link Policy	LP3 (Enabled in S0, Sx/AC) where available
Setup:	<div>1. Set the SUT power source to AC+DC where supported; otherwise AC-only.</div> <div>2. Bring the SUT to the base state of S0/MeOn (CM0,CM0-PG), and confirm that the Host OS is available.</div> <div>3. Set the active power package on the SUT to Power Package 2 (Intel® ME on in S0, wake in Sx/AC).</div> <div>4. Set the Intel® AMT WLAN link policy on the SUT to Link Policy 3 (Enabled in S0, Sx/AC), if the WLAN network interface is available.</div> <div>5. Ensure that the Host OS network device drivers are configured to not wake the SUT. This includes enabling ARP and/or NS Offload features where available to help prevent unexpected host wake events.</div> <div>6. Ensure the Intel® AMT idle timeout on the SUT is set to 1 minute.</div> <div>7. Verify that Intel® AMT on the SUT responds to version queries via all available network interfaces.</div> <div>8. Shutdown the SUT via the Host OS.</div> <div>9. Verify that the SUT is in S5/MeOn (CM3).</div> <div>10. Verify that Intel® AMT on the SUT responds to version queries via all available network interfaces.</div>		
Procedure:	<div>1. Wait for 3 minutes to allow the Intel® ME on the SUT to move to CM3-PG after Intel® AMT idle timeout.</div> <div>2. Verify that the Intel® ME on the SUT is in CM3-PG.</div>		
Pass Criteria:	The test passes if the SUT remains in S5, and the Intel® CSME moves to CM3-PG.		



ID:	ME_PM_14.21		
Title:	S4/CM3 to S4/CM3-PG via Intel® AMT idle timeout (AC+DC, AC-only/PP2/LP2)		
Requirement:	Mandatory	Exemptions	<input checked="" type="checkbox"/> Systems with a single network interface (not LAN+WLAN)
Method:	Automated by Intel® PETS		
Objective:	This test checks the SUT power flow from S4/CM3 to S4/CM-Off via Intel® AMT idle timeout with the parameters outlined below.		
Configuration:	Intel® AMT should be provisioned via manual mode. This test assumes that both LAN and WLAN network interfaces are available on the SUT.		
Parameters:	System Power Source		AC+DC or AC-only
	Power States	Initial	S4,S5/MeOn (CM3)
		Final	S4,S5/MeOff (CM3-PG)
		Trigger	Intel® AMT idle timeout
	Intel® AMT	Power Package	PP2 (Intel® ME on in S0, wake in Sx/AC)
		WLAN Link Policy	LP2 (Enabled in S0)
Setup:	<ol style="list-style-type: none"> Set the SUT power source to AC+DC where supported; otherwise AC-only. Bring the SUT to the base state of S0/MeOn (CM0), and confirm that the Host OS is available. Set the active power package on the SUT to Power Package 2 (Intel® ME on in S0, wake in Sx/AC). Set the Intel® AMT WLAN link policy on the SUT to Link Policy 2 (Enabled in S0). Ensure that the Host OS network device drivers are configured to not wake the SUT. This includes enabling ARP and/or NS Offload features where available to help prevent unexpected host wake events. Ensure the Intel® AMT idle timeout on the SUT is set to 1 minute. Verify that Intel® AMT on the SUT responds to version queries via all available network interfaces. Hibernate the SUT via the Host OS. Verify that the SUT is in S4, S5/MeOn (CM3). Verify that Intel® AMT on the SUT responds to version query via the LAN network interface. Verify that Intel® AMT on the SUT does not respond to version query via the WLAN network interface. 		
Procedure:	<ol style="list-style-type: none"> Wait for 3 minutes to allow the Intel® ME on the SUT to move to CM3-PG after Intel® AMT idle timeout. Verify that the Intel® ME on the SUT is in CM3-PG. 		
Pass Criteria:	The test passes if the SUT remains in S4 or S5, and the Intel® CSME moves to MeOff (CM3-PG).		

ID:	ME_PM_14.22		
Title:	S5/CM3 to S5/CM3-PG via Intel® AMT idle timeout (AC+DC, AC-only/PP2/LP2)		
Requirement:	Mandatory	Exemptions	<input checked="" type="checkbox"/> Systems with a single network interface (not LAN+WLAN)
Method:	Automated by Intel® PETS		
Objective:	This test checks the SUT power flow from S5/CM3 to S5/CM3-PG via Intel® AMT idle timeout with the parameters outlined below.		
Configuration:	Intel® AMT should be provisioned via manual mode. This test assumes that both LAN and WLAN network interfaces are available on the SUT.		
Parameters:	System Power Source		AC+DC or AC-only
	Power States	Initial	S5/MeOn (CM3)
		Final	S5/MeOff (CM3-PG)
		Trigger	Intel® AMT idle timeout
	Intel® AMT	Power Package	PP2 (Intel® ME on in S0, wake in Sx/AC)
		WLAN Link Policy	LP2 (Enabled in S0)



ID:	ME_PM_14.22
Setup:	<ol style="list-style-type: none"> 1. Set the SUT power source to AC+DC where supported; otherwise AC-only. 2. Bring the SUT to the base state of S0/MeOn (CM0), and confirm that the Host OS is available. 3. Set the active power package on the SUT to Power Package 2 (Intel® ME on in S0, wake in Sx/AC). 4. Set the Intel® AMT WLAN link policy on the SUT to Link Policy 2 (Enabled in S0). 5. Ensure that the Host OS network device drivers are configured to not wake the SUT. This includes enabling ARP and/or NS Offload features where available to help prevent unexpected host wake events. 6. Ensure the Intel® AMT idle timeout on the SUT is set to 1 minute. 7. Verify that Intel® AMT on the SUT responds to version queries via all available network interfaces. 8. Shutdown the SUT via the Host OS. 9. Verify that the SUT is in S5/MeOn (CM3). 10. Verify that Intel® AMT on the SUT responds to version query via the LAN network interface. 11. Verify that Intel® AMT on the SUT does not respond to version query via the WLAN network interface.
Procedure:	<ol style="list-style-type: none"> 1. Wait for 3 minutes to allow the Intel® ME on the SUT to move to CM3-PG after Intel® AMT idle timeout. 2. Verify that the Intel® ME on the SUT is in CM3-PG.
Pass Criteria:	The test passes if the SUT remains in S5, and the Intel® CSME moves to MeOff (CM3-PG).

12.18 ME_PM_15: G3 or S4–S5/CM-Off (Suspend Well Off) to S4–S5/CM3

ID:	ME_PM_15.1		
Title:	S4/CM3-PG with Ac Wake to S4/CM3 via AC-attach (DC-only/PP2/LP3)		
Requirement:	Mandatory	Exemptions	<input checked="" type="checkbox"/> Non-Mobile (AC-only) systems
Method:	Automated by Intel® PETS		
Objective:	This test checks the SUT power flow from S4/CM3-PG with Ac Wake to S4/CM3 via AC-attach with the parameters outlined below.		
Configuration:	<p>Intel® AMT should be provisioned via manual mode.</p> <p>If Deep S4, Deep S5, and/or G3 are supported on the SUT, please confirm the following:</p> <ul style="list-style-type: none"> • the SUT and/or BIOS are properly configured to permit Deep S4/S5 or G3 entry. • the correct Deep Sx policy is applied to the SUT profile in Intel® PETS. <p>This test assumes that either LAN-only, WLAN-only, or both LAN and WLAN network interfaces are available on the SUT.</p>		
Parameters:	System Power Source		DC-only
	Power States	Initial	S4,S5,Deep S4,Deep S5,G3/CM3-PGwith AC Wake
		Final	S4,S5/MeOn (CM3)
		Trigger	AC-attach
	Intel® AMT	Power Package	PP2 (Intel® ME on in S0, wake in Sx/AC)
		WLAN Link Policy	LP3 (Enabled in S0, Sx/AC) where available



ID:	ME_PM_15.1
Setup:	<ol style="list-style-type: none"> 1. Set the SUT power source to AC+DC. 2. Bring the SUT to the base state of S0/MeOn (CM0,CM0-PG), and confirm that the Host OS is available. 3. Verify that a DC battery is connected to the SUT, and that it is charged. 4. Set the SUT power source to DC-only. 5. Set the active power package on the SUT to Power Package 2 (Intel® ME on in S0, wake in Sx/AC). 6. Set the Intel® AMT WLAN link policy on the SUT to Link Policy 3 (Enabled in S0, Sx/AC), if the WLAN network interface is available. 7. Ensure that the Host OS network device drivers are configured to not wake the SUT. This includes enabling ARP and/or NS Offload features where available to help prevent unexpected host wake events. 8. Verify that Intel® AMT on the SUT responds to version queries via all available network interfaces. 9. Hibernate the SUT via the Host OS. 10. Verify that the SUT is in S4, S5, Deep S4, Deep S5, G3/CM3-PG.with AC Wake
Procedure:	<ol style="list-style-type: none"> 1. Set the SUT power source to AC+DC. 2. Verify that Intel® AMT on the SUT responds to version queries via all available network interfaces. 3. Verify that the SUT is in S4, S5/MeOn (CM3).
Pass Criteria:	<p>The test passes if:</p> <ul style="list-style-type: none"> • the SUT remains in S4 or S5 (or moves to S4 or S5 from Deep S4, Deep S5, or G3). • the Intel® CSME moves to MeOn (CM3). • Intel® AMT responds to version queries via all available network interfaces.

ID:	ME_PM_15.2																	
Title:	S5/CM3-PG with AC Wake to S5/CM3 via AC-attach (DC-only/PP2/LP3)																	
Requirement:	Mandatory	Exemptions	<input checked="" type="checkbox"/> Non-Mobile (AC-only) systems															
Method:	Automated by Intel® PETS																	
Objective:	This test checks the SUT power flow from S5/CM3-PG with AC Wake to S5/CM3 via AC-attach with the parameters outlined below.																	
Configuration:	<p>Intel® AMT should be provisioned via manual mode.</p> <p>If Deep S5 and/or G3 are supported on the SUT, please confirm the following:</p> <ul style="list-style-type: none">the SUT and/or BIOS are properly configured to permit Deep S5 or G3 entry.the correct Deep Sx policy is applied to the SUT profile in Intel® PETS. <p>This test assumes that either LAN-only, WLAN-only, or both LAN and WLAN network interfaces are available on the SUT.</p>																	
Parameters:	<table><tr><td colspan="2">System Power Source</td><td>DC-only</td></tr><tr><td rowspan="3">Power States</td><td>Initial</td><td>S5,Deep S5,G3/CM3-PGwith Ac Wake</td></tr><tr><td>Final</td><td>S5/MeOn (CM3)</td></tr><tr><td>Trigger</td><td>AC-attach</td></tr><tr><td rowspan="2">Intel® AMT</td><td>Power Package</td><td>PP2 (Intel® ME on in S0, wake in Sx/AC)</td></tr><tr><td>WLAN Link Policy</td><td>LP3 (Enabled in S0, Sx/AC) where available</td></tr></table>			System Power Source		DC-only	Power States	Initial	S5,Deep S5,G3/CM3-PGwith Ac Wake	Final	S5/MeOn (CM3)	Trigger	AC-attach	Intel® AMT	Power Package	PP2 (Intel® ME on in S0, wake in Sx/AC)	WLAN Link Policy	LP3 (Enabled in S0, Sx/AC) where available
System Power Source		DC-only																
Power States	Initial	S5,Deep S5,G3/CM3-PGwith Ac Wake																
	Final	S5/MeOn (CM3)																
	Trigger	AC-attach																
Intel® AMT	Power Package	PP2 (Intel® ME on in S0, wake in Sx/AC)																
	WLAN Link Policy	LP3 (Enabled in S0, Sx/AC) where available																
Setup:	<ol style="list-style-type: none">Set the SUT power source to AC+DC.Bring the SUT to the base state of S0/MeOn (CM0,CM0-PG), and confirm that the Host OS is available.Verify that a DC battery is connected to the SUT, and that it is charged.Set the SUT power source to DC-only.Set the active power package on the SUT to Power Package 2 (Intel® ME on in S0, wake in Sx/AC).Set the Intel® AMT WLAN link policy on the SUT to Link Policy 3 (Enabled in S0, Sx/AC), if the WLAN network interface is available.Ensure that the Host OS network device drivers are configured to not wake the SUT. This includes enabling ARP and/or NS Offload features where available to help prevent unexpected host wake events.Verify that Intel® AMT on the SUT responds to version queries via all available network interfaces.Shutdown the SUT via the Host OS.Verify that the SUT is in S5, Deep S5, G3/CM3-PG.with AC Wake																	



ID:	ME_PM_15.2
Procedure:	<ol style="list-style-type: none"> 1. Set the SUT power source to AC+DC. 2. Verify that Intel® AMT on the SUT responds to version queries via all available network interfaces. 3. Verify that the SUT is in S5/MeOn (CM3).
Pass Criteria:	<p>The test passes if:</p> <ul style="list-style-type: none"> • the SUT remains in S5 (or moves to S5 from Deep S5 or G3). • the Intel® CSME moves to MeOn (CM3). • Intel® AMT responds to version queries via all available network interfaces.

ID:	ME_PM_15.3		
Title:	G3/CM-Off to S5/CM3 via AC-attach (AC+DC, AC-only/PP2/LP3)		
Requirement:	Mandatory	Exemptions	None
Method:	Automated by Intel® PETS		
Objective:	This test checks the SUT power flow from G3/CM-Off to S5/CM3 via AC-attach with the parameters outlined below.		
Configuration:	<p>Intel® AMT should be provisioned via manual mode.</p> <p>Confirm that the BIOS is configured to move the SUT to S5 from G3 upon AC-attach.</p> <p>This test assumes that either LAN-only, WLAN-only, or both LAN and WLAN network interfaces are available on the SUT.</p>		
Parameters:	System Power Source		AC+DC or AC-only
	Power States	Initial	G3/MeOff (CM-Off)
		Final	S5/MeOn (CM3)
		Trigger	AC-attach
	Intel® AMT	Power Package	PP2 (Intel® ME on in S0, wake in Sx/AC)
		WLAN Link Policy	LP3 (Enabled in S0, Sx/AC) where available
Setup:	<ol style="list-style-type: none"> 1. Set the SUT power source to AC+DC where supported; otherwise AC-only. 2. Bring the SUT to the base state of S0/MeOn (CM0,CM0-PG), and confirm that the Host OS is available. 3. Set the active power package on the SUT to Power Package 2 (Intel® ME on in S0, wake in Sx/AC). 4. Set the Intel® AMT WLAN link policy on the SUT to Link Policy 3 (Enabled in S0, Sx/AC), if the WLAN network interface is available. 5. Ensure that the Host OS network device drivers are configured to not wake the SUT. This includes enabling ARP and/or NS Offload features where available to help prevent unexpected host wake events. 6. Verify that Intel® AMT on the SUT responds to version queries via all available network interfaces. 7. Shutdown the SUT via the Host OS. 8. Verify that the SUT is in S5/MeOn (CM3). 9. Verify that Intel® AMT on the SUT responds to version queries via all available network interfaces. 10. Remove power from the SUT via AC-detach, and if necessary also via DC-detach. Wait for 10 seconds before continuing to allow full power drain from the SUT. 11. Verify that the SUT is in G3/MeOff (CM-Off). 12. Verify that Intel® AMT on the SUT does not respond to version queries via any of the available network interfaces. 		
Procedure:	<ol style="list-style-type: none"> 1. Set the SUT power source to AC+DC where supported; otherwise AC-only. For systems with DC-power support, consult the system design as it may be preferred to connect DC-power before AC-power. 2. Verify that Intel® AMT on the SUT responds to version queries via all available network interfaces. 3. Verify that the SUT is in S5/MeOn (CM3). 		
Pass Criteria:	<p>The test passes if:</p> <ul style="list-style-type: none"> • the SUT moves from G3 to S5. • the Intel® CSME moves to MeOn (CM3). • Intel® AMT responds to version queries via all available network interfaces. 		



ID:	ME_PM_15.21																
Title:	S4/CM3-PG with Ac Wake to S4/CM3 via AC-attach (DC-only/PP2/LP2)																
Requirement:	Mandatory Exemptions	<input checked="" type="checkbox"/> Non-Mobile (AC-only) systems <input checked="" type="checkbox"/> Systems with a LAN-only network interface															
Method:	Automated by Intel® PETS																
Objective:	This test checks the SUT power flow from S4/CM3-PG with AC Wake to S4/CM3 via AC-attach with the parameters outlined below.																
Configuration:	Intel® AMT should be provisioned via manual mode. If Deep S4, Deep S5, and/or G3 are supported on the SUT, please confirm the following: <ul style="list-style-type: none"> the SUT and/or BIOS are properly configured to permit Deep S4/S5 or G3 entry. the correct Deep Sx policy is applied to the SUT profile in Intel® PETS. This test assumes that either WLAN-only, or both LAN and WLAN network interfaces are available on the SUT.																
Parameters:	<table border="1"> <tr> <td colspan="2">System Power Source</td><td>DC-only</td></tr> <tr> <td rowspan="3">Power States</td><td>Initial</td><td>S4,S5,Deep S4,Deep S5,G3/CM3-PG with Ac Wake</td></tr> <tr> <td>Final</td><td>S4,S5/MeOn (CM3)</td></tr> <tr> <td>Trigger</td><td>AC-attach</td></tr> <tr> <td rowspan="2">Intel® AMT</td><td>Power Package</td><td>PP2 (Intel® ME on in S0, wake in Sx/AC)</td></tr> <tr> <td>WLAN Link Policy</td><td>LP2 (Enabled in S0)</td></tr> </table>		System Power Source		DC-only	Power States	Initial	S4,S5,Deep S4,Deep S5,G3/CM3-PG with Ac Wake	Final	S4,S5/MeOn (CM3)	Trigger	AC-attach	Intel® AMT	Power Package	PP2 (Intel® ME on in S0, wake in Sx/AC)	WLAN Link Policy	LP2 (Enabled in S0)
System Power Source		DC-only															
Power States	Initial	S4,S5,Deep S4,Deep S5,G3/CM3-PG with Ac Wake															
	Final	S4,S5/MeOn (CM3)															
	Trigger	AC-attach															
Intel® AMT	Power Package	PP2 (Intel® ME on in S0, wake in Sx/AC)															
	WLAN Link Policy	LP2 (Enabled in S0)															
Setup:	1. Set the SUT power source to AC+DC. 2. Bring the SUT to the base state of S0/MeOn (CM0,CM0-PG), and confirm that the Host OS is available. 3. Verify that a DC battery is connected to the SUT, and that it is charged. 4. Set the SUT power source to DC-only . 5. Set the active power package on the SUT to Power Package 2 (Intel® ME on in S0, wake in Sx/AC). 6. Set the Intel® AMT WLAN link policy on the SUT to Link Policy 2 (Enabled in S0). 7. Ensure that the Host OS network device drivers are configured to not wake the SUT. This includes enabling ARP and/or NS Offload features where available to help prevent unexpected host wake events. 8. Verify that Intel® AMT on the SUT responds to version queries via all available network interfaces. 9. Hibernate the SUT via the Host OS. 10. Verify that the SUT is in S4 , S5, Deep S4, Deep S5, G3/CM3-PG.with AC Wake																
Procedure:	1. Set the SUT power source to AC+DC. 2. Verify that Intel® AMT on the SUT responds to version query via the LAN network interface, if available. 3. Verify that Intel® AMT on the SUT does not respond to version query via the WLAN network interface. 4. Verify that the SUT is in S4, S5/MeOn (CM3).																
Pass Criteria:	The test passes if: <ul style="list-style-type: none"> the SUT remains in S4 or S5 (or moves to S4 or S5 from Deep S4, Deep S5, or G3). the Intel® CSME moves to MeOn (CM3). when in S4 or S5: <ul style="list-style-type: none"> Intel® AMT on the SUT does respond to version queries via the LAN network interface, if available. Intel® AMT on the SUT does not respond to version queries the WLAN network interface. 																

ID:	ME_PM_15.22	
Title:	S5/CM3-PG with AC Wake to S5/CM3 via AC-attach (DC-only/PP2/LP2)	
Requirement:	Mandatory Exemptions	<input checked="" type="checkbox"/> Non-Mobile (AC-only) systems <input checked="" type="checkbox"/> Systems with a LAN-only network interface
Method:	Automated by Intel® PETS	
Objective:	This test checks the SUT power flow from S5/CM3-PG with AC Wake to S5/CM3 via AC-attach with the parameters outlined below.	



ID:	ME_PM_15.22																	
Configuration:	<p>Intel® AMT should be provisioned via manual mode.</p> <p>If Deep S5 and/or G3 are supported on the SUT, please confirm the following:</p> <ul style="list-style-type: none">the SUT and/or BIOS are properly configured to permit Deep S5 or G3 entry.the correct Deep Sx policy is applied to the SUT profile in Intel® PETS. <p>This test assumes that either WLAN-only, or both LAN and WLAN network interfaces are available on the SUT.</p>																	
Parameters:	<table><tr><td colspan="2">System Power Source</td><td>DC-only</td></tr><tr><td rowspan="3">Power States</td><td>Initial</td><td>S5,Deep S5,G3/CM3-PGwith AC Wake</td></tr><tr><td>Final</td><td>S5/MeOn (CM3)</td></tr><tr><td>Trigger</td><td>AC-attach</td></tr><tr><td rowspan="2">Intel® AMT</td><td>Power Package</td><td>PP2 (Intel® ME on in S0, wake in Sx/AC)</td></tr><tr><td>WLAN Link Policy</td><td>LP2 (Enabled in S0)</td></tr></table>			System Power Source		DC-only	Power States	Initial	S5,Deep S5,G3/CM3-PGwith AC Wake	Final	S5/MeOn (CM3)	Trigger	AC-attach	Intel® AMT	Power Package	PP2 (Intel® ME on in S0, wake in Sx/AC)	WLAN Link Policy	LP2 (Enabled in S0)
System Power Source		DC-only																
Power States	Initial	S5,Deep S5,G3/CM3-PGwith AC Wake																
	Final	S5/MeOn (CM3)																
	Trigger	AC-attach																
Intel® AMT	Power Package	PP2 (Intel® ME on in S0, wake in Sx/AC)																
	WLAN Link Policy	LP2 (Enabled in S0)																
Setup:	<ol style="list-style-type: none">Set the SUT power source to AC+DC.Bring the SUT to the base state of S0/MeOn (CM0,CM0-PG), and confirm that the Host OS is available.Verify that a DC battery is connected to the SUT, and that it is charged.Set the SUT power source to DC-only.Set the active power package on the SUT to Power Package 2 (Intel® ME on in S0, wake in Sx/AC).Set the Intel® AMT WLAN link policy on the SUT to Link Policy 2 (Enabled in S0).Ensure that the Host OS network device drivers are configured to not wake the SUT. This includes enabling ARP and/or NS Offload features where available to help prevent unexpected host wake events.Verify that Intel® AMT on the SUT responds to version queries via all available network interfaces.Shutdown the SUT via the Host OS.Verify that the SUT is in S5, Deep S5, G3/CM3-PG.with AC Wake																	
Procedure:	<ol style="list-style-type: none">Set the SUT power source to AC+DC.Verify that Intel® AMT on the SUT responds to version query via the LAN network interface, if available.Verify that Intel® AMT on the SUT does not respond to version query via the WLAN network interface.Verify that the SUT is in S5/MeOn (CM3).																	
Pass Criteria:	<p>The test passes if:</p> <ul style="list-style-type: none">the SUT remains in S5 (or moves to S5 from Deep S5 or G3).the Intel® CSME moves to MeOn (CM3).when in S4 or S5:<ul style="list-style-type: none">Intel® AMT on the SUT does respond to version queries via the LAN network interface, if available.Intel® AMT on the SUT does not respond to version queries the WLAN network interface.																	

ID:	ME_PM_15.23
Title:	G3/CM-Off to S5/CM3 via AC-attach (AC+DC, AC-only/PP2/LP2)
Requirement:	Mandatory Exemptions <input checked="" type="checkbox"/> Systems with a LAN-only network interface
Method:	Automated by Intel® PETS
Objective:	This test checks the SUT power flow from G3/CM-Off to S5/CM3 via AC-attach with the parameters outlined below.
Configuration:	<p>Intel® AMT should be provisioned via manual mode.</p> <p>Confirm that the BIOS is configured to move the SUT to S5 from G3 upon AC-attach.</p> <p>This test assumes that either WLAN-only, or both LAN and WLAN network interfaces are available on the SUT.</p>



ID:	ME_PM_15.23	
Parameters:	System Power Source AC+DC or AC-only	
	Power States	Initial G3/MeOff (CM-Off)
		Final S5/MeOn (CM3)
		Trigger AC-attach
	Intel® AMT	Power Package PP2 (Intel® ME on in S0, wake in Sx/AC)
		WLAN Link Policy LP2 (Enabled in S0)
Setup:	<ol style="list-style-type: none"> 1. Set the SUT power source to AC+DC where supported; otherwise AC-only. 2. Bring the SUT to the base state of S0/MeOn (CM0,CM0-PG), and confirm that the Host OS is available. 3. Set the active power package on the SUT to Power Package 2 (Intel® ME on in S0, wake in Sx/AC). 4. Set the Intel® AMT WLAN link policy on the SUT to Link Policy 2 (Enabled in S0). 5. Ensure that the Host OS network device drivers are configured to not wake the SUT. This includes enabling ARP and/or NS Offload features where available to help prevent unexpected host wake events. 6. Verify that Intel® AMT on the SUT responds to version queries via all available network interfaces. 7. Shutdown the SUT via the Host OS. 8. Verify that the SUT is in S5/MeOn (CM3). 9. Verify that Intel® AMT on the SUT responds to version query via the LAN network interface. 10. Verify that Intel® AMT on the SUT does not respond to version query via the WLAN network interface. 11. Remove power from the SUT via AC-detach, and if necessary also via DC-detach. Wait for 10 seconds before continuing to allow full power drain from the SUT. 12. Verify that the SUT is in G3/MeOff (CM-Off). 13. Verify that Intel® AMT on the SUT does not respond to version queries via any of the available network interfaces. 	
Procedure:	<ol style="list-style-type: none"> 1. Set the SUT power source to AC+DC where supported; otherwise AC-only. For systems with DC-power support, consult the system design as it may be preferred to connect DC-power before AC-power. 2. Verify that Intel® AMT on the SUT responds to version query via the LAN network interface. 3. Verify that Intel® AMT on the SUT does not respond to version query via the WLAN network interface. 4. Verify that the SUT is in S5/MeOn (CM3). 	
Pass Criteria:	<p>The test passes if:</p> <ul style="list-style-type: none"> • the SUT moves from G3 to S5. • the Intel® CSME moves to MeOn (CM3). • when in S5: <ul style="list-style-type: none"> – Intel® AMT on the SUT does respond to version queries via the LAN network interface, if available. – Intel® AMT on the SUT does not respond to version queries the WLAN network interface. 	

12.19 ME_PM_16: S4–S5/CM-Off (Suspend Well On) to S4–S5/CM3

ID:	ME_PM_16.1
Title:	S4/CM3-PG to S4/CM3 via Intel® AMT network access (AC+DC, AC-only/PP2/LP3)
Requirement:	Mandatory Exemptions None
Method:	Automated by Intel® PETS
Objective:	This test checks the SUT power flow from S4/CM3-PG to S4/CM3 via Intel® AMT network access with the parameters outlined below.
Configuration:	Intel® AMT should be provisioned via manual mode. This test assumes that either LAN-only, WLAN-only, or both LAN and WLAN network interfaces are available on the SUT. Where both network interfaces are available, LAN is the initial active network interface in the test, and WLAN is the secondary network interface.



ID:	ME_PM_16.1	
Parameters:	System Power Source	AC+DC or AC-only
	Power States	Initial S4,S5/MeOff (CM3-PG)
		Final S4,S5/MeOn (CM3)
		Trigger Intel® AMT network access
	Intel® AMT	Power Package PP2 (Intel® ME on in S0, wake in Sx/AC)
		WLAN Link Policy LP3 (Enabled in S0, Sx/AC) where available
Setup:	<ol style="list-style-type: none"> 1. Set the SUT power source to AC+DC where supported; otherwise AC-only. 2. Bring the SUT to the base state of S0/MeOn (CM0,CM0-PG), and confirm that the Host OS is available. 3. Set the active power package on the SUT to Power Package 2 (Intel® ME on in S0, wake in Sx/AC). 4. Set the Intel® AMT WLAN link policy on the SUT to Link Policy 3 (Enabled in S0, Sx/AC), if the WLAN network interface is available. 5. Ensure the Intel® AMT idle timeout on the SUT is set to 1 minute. 6. Ensure that the Host OS network device drivers are configured to not wake the SUT. This includes enabling ARP and/or NS Offload features where available to help prevent unexpected host wake events. 7. Verify that Intel® AMT on the SUT responds to version queries via all available network interfaces. 8. Hibernate the SUT via the Host OS. 9. Verify that the SUT is in S4, S5/MeOn (CM3). 10. Verify that Intel® AMT on the SUT responds to version queries via all available network interfaces. 	
Procedure:	<ol style="list-style-type: none"> 1. Wait for 3 minutes to allow the Intel® ME on the SUT to move to CM3-PG after Intel® AMT idle timeout. 2. Verify that the Intel® ME on the SUT is in CM3-PG. 3. Verify that Intel® AMT on the SUT responds to version query by means of the active network interface. 4. Verify that the Intel® ME on the SUT is on. <p>If both LAN and WLAN network interfaces are available, repeat this test procedure with the WLAN interface set as the active network interface.</p>	
Pass Criteria:	<p>The test passes if:</p> <ul style="list-style-type: none"> • Intel® AMT responds to version queries via all available network interfaces. • the SUT remains in S4 or S5. • the Intel® CSME moves to MeOn (CM3). 	

ID:	ME_PM_16.2	
Title:	S5/CM3-PG to S5/CM3 via Intel® AMT network access (AC+DC, AC-only/PP2/LP3)	
Requirement:	Mandatory	Exemptions None
Method:	Automated by Intel® PETS	
Objective:	This test checks the SUT power flow from S5/CM3-PG to S5/CM3 via Intel® AMT network access with the parameters outlined below.	
Configuration:	<p>Intel® AMT should be provisioned via manual mode.</p> <p>This test assumes that either LAN-only, WLAN-only, or both LAN and WLAN network interfaces are available on the SUT. Where both network interfaces are available, LAN is the initial active network interface in the test, and WLAN is the secondary network interface.</p>	
Parameters:	System Power Source	AC+DC or AC-only
	Power States	Initial S5/MeOff (CM3-PG)
		Final S5/MeOn (CM3)
		Trigger Intel® AMT network access
	Intel® AMT	Power Package PP2 (Intel® ME on in S0, wake in Sx/AC)
		WLAN Link Policy LP3 (Enabled in S0, Sx/AC) where available



ID:	ME_PM_16.2
Setup:	<ol style="list-style-type: none"> 1. Set the SUT power source to AC+DC where supported; otherwise AC-only. 2. Bring the SUT to the base state of S0/MeOn (CM0,CM0-PG), and confirm that the Host OS is available. 3. Set the active power package on the SUT to Power Package 2 (Intel® ME on in S0, wake in Sx/AC). 4. Set the Intel® AMT WLAN link policy on the SUT to Link Policy 3 (Enabled in S0, Sx/AC), if the WLAN network interface is available. 5. Ensure the Intel® AMT idle timeout on the SUT is set to 1 minute. 6. Ensure that the Host OS network device drivers are configured to not wake the SUT. This includes enabling ARP and/or NS Offload features where available to help prevent unexpected host wake events. 7. Verify that Intel® AMT on the SUT responds to version queries via all available network interfaces. 8. Shutdown the SUT via the Host OS. 9. Verify that the SUT is in S5/MeOn (CM3). 10. Verify that Intel® AMT on the SUT responds to version queries via all available network interfaces.
Procedure:	<ol style="list-style-type: none"> 1. Wait for 3 minutes to allow the Intel® ME on the SUT to move to CM3-PG after Intel® AMT idle timeout. 2. Verify that the Intel® ME on the SUT is in CM3-PG. 3. Verify that Intel® AMT on the SUT responds to version query by means of the active network interface. 4. Verify that the Intel® ME on the SUT is on. <p>If both LAN and WLAN network interfaces are available, repeat this test procedure with the WLAN interface set as the active network interface.</p>
Pass Criteria:	<p>The test passes if:</p> <ul style="list-style-type: none"> • Intel® AMT responds to version queries via all available network interfaces. • the SUT remains in S5. • the Intel® CSME moves to MeOn (CM3).

ID:	ME_PM_16.21		
Title:	S4/CM3-PG to S4/CM3 via Intel® AMT network access (AC+DC, AC-only/PP2/LP2)		
Requirement:	Mandatory	Exemptions	<input checked="" type="checkbox"/> Systems with a single network interface (not LAN+WLAN)
Method:	Automated by Intel® PETS		
Objective:	This test checks the SUT power flow from S4/CM-Off to S4/CM3 via Intel® AMT network access with the parameters outlined below.		
Configuration:	Intel® AMT should be provisioned via manual mode. This test assumes that both LAN and WLAN network interfaces are available on the SUT.		
Parameters:	System Power Source		AC+DC or AC-only
	Power States	Initial	S4,S5/MeOff (CM3-PG)
		Final	S4,S5/MeOn (CM3)
		Trigger	Intel® AMT network access
	Intel® AMT	Power Package	PP2 (Intel® ME on in S0, wake in Sx/AC)
		WLAN Link Policy	LP2 (Enabled in S0)



ID:	ME_PM_16.21
Setup:	<ol style="list-style-type: none"> 1. Set the SUT power source to AC+DC where supported; otherwise AC-only. 2. Bring the SUT to the base state of S0/MeOn (CM0), and confirm that the Host OS is available. 3. Set the active power package on the SUT to Power Package 2 (Intel® ME on in S0, wake in Sx/AC). 4. Set the Intel® AMT WLAN link policy on the SUT to Link Policy 2 (Enabled in S0). 5. Ensure the Intel® AMT idle timeout on the SUT is set to 1 minute. 6. Ensure that the Host OS network device drivers are configured to not wake the SUT. This includes enabling ARP and/or NS Offload features where available to help prevent unexpected host wake events. 7. Verify that Intel® AMT on the SUT responds to version queries via all available network interfaces. 8. Hibernate the SUT via the Host OS. 9. Verify that the SUT is in S4, S5/MeOn (CM3). 10. Verify that Intel® AMT on the SUT responds to version query via the LAN network interface. 11. Verify that Intel® AMT on the SUT does not respond to version query via the WLAN network interface.
Procedure:	<ol style="list-style-type: none"> 1. Wait for 3 minutes to allow the Intel® ME on the SUT to move to CM3-PG after Intel® AMT idle timeout. 2. Verify that the Intel® ME on the SUT is in CM3-PG. 3. Verify that Intel® AMT on the SUT responds to version query via the LAN network interface. 4. Verify that the Intel® ME on the SUT is on. 5. Verify that Intel® AMT on the SUT does not respond to version query via the WLAN network interface.
Pass Criteria:	<p>The test passes if:</p> <ul style="list-style-type: none"> • the SUT remains in S4 or S5. • the Intel® CSME moves to MeOn (CM3). • when in S4 or S5: <ul style="list-style-type: none"> – Intel® AMT on the SUT does respond to version queries via the LAN network interface, if available. – Intel® AMT on the SUT does not respond to version queries the WLAN network interface.

ID:	ME_PM_16.22		
Title:	S5/CM3-PG to S5/CM3 via Intel® AMT network access (AC+DC, AC-only/PP2/LP2)		
Requirement:	Mandatory	Exemptions	<input checked="" type="checkbox"/> Systems with a single network interface (not LAN+WLAN)
Method:	Automated by Intel® PETS		
Objective:	This test checks the SUT power flow from S5/CM-Off to S5/CM3 via Intel® AMT network access with the parameters outlined below.		
Configuration:	Intel® AMT should be provisioned via manual mode. This test assumes that both LAN and WLAN network interfaces are available on the SUT.		
Parameters:	System Power Source		AC+DC or AC-only
	Power States	Initial	S5/MeOff (CM3-PG)
		Final	S5/MeOn (CM3)
		Trigger	Intel® AMT network access
	Intel® AMT	Power Package	PP2 (Intel® ME on in S0, wake in Sx/AC)
		WLAN Link Policy	LP2 (Enabled in S0)



ID:	ME_PM_16.22
Setup:	<ol style="list-style-type: none"> 1. Set the SUT power source to AC+DC where supported; otherwise AC-only. 2. Bring the SUT to the base state of S0/MeOn (CM0), and confirm that the Host OS is available. 3. Set the active power package on the SUT to Power Package 2 (Intel® ME on in S0, wake in Sx/AC). 4. Set the Intel® AMT WLAN link policy on the SUT to Link Policy 2 (Enabled in S0). 5. Ensure the Intel® AMT idle timeout on the SUT is set to 1 minute. 6. Ensure that the Host OS network device drivers are configured to not wake the SUT. This includes enabling ARP and/or NS Offload features where available to help prevent unexpected host wake events. 7. Verify that Intel® AMT on the SUT responds to version queries via all available network interfaces. 8. Shutdown the SUT via the Host OS. 9. Verify that the SUT is in S5/MeOn (CM3). 10. Verify that Intel® AMT on the SUT responds to version query via the LAN network interface. 11. Verify that Intel® AMT on the SUT does not respond to version query via the WLAN network interface.
Procedure:	<ol style="list-style-type: none"> 1. Wait for 3 minutes to allow the Intel® ME on the SUT to move to CM3-PG after Intel® AMT idle timeout. 2. Verify that the Intel® ME on the SUT is in CM3-PG. 3. Verify that Intel® AMT on the SUT responds to version query via the LAN network interface. 4. Verify that the Intel® ME on the SUT is on. 5. Verify that Intel® AMT on the SUT does not respond to version query via the WLAN network interface.
Pass Criteria:	<p>The test passes if:</p> <ul style="list-style-type: none"> • the SUT remains in S5. • the Intel® CSME moves to MeOn (CM3). • when in S5: <ul style="list-style-type: none"> — Intel® AMT on the SUT does respond to version queries via the LAN network interface, if available. — Intel® AMT on the SUT does not respond to version queries via the WLAN network interface.

12.20 ME_PM_17: Cold Reset

ID:	ME_PM_17.6		
Title:	S0/CM0 to S0/CM0 via CF9 Cold Reset (AC+DC, AC-only/PP2/LP3)		
Requirement:	Mandatory	Exemptions	None
Method:	Automated by Intel® PETS		
Objective:	This test checks the SUT power flow from S0/CM0 to S0/CM0 via CF9 Cold Reset with the parameters outlined below.		
Configuration:	Intel® AMT should be provisioned via manual mode. This test assumes that either LAN-only, WLAN-only, or both LAN and WLAN network interfaces are available on the SUT.		
Parameters:	System Power Source		AC+DC or AC-only
	Power States	Initial	S0/MeOn (CM0, CM0-PG)
		Final	S0/MeOn (CM0, CM0-PG)
		Trigger	CF9 Cold Reset
	Intel® AMT	Power Package	PP2 (Intel® ME on in S0, wake in Sx/AC)
		WLAN Link Policy	LP3 (Enabled in S0, Sx/AC) where available



ID:	ME_PM_17.6
Setup:	<ol style="list-style-type: none"> 1. Set the SUT power source to AC+DC where supported; otherwise AC-only. 2. Bring the SUT to the base state of S0/MeOn (CM0,CM0-PG), and confirm that the Host OS is available. 3. Set the active power package on the SUT to Power Package 2 (Intel® ME on in S0, wake in Sx/AC). 4. Set the Intel® AMT WLAN link policy on the SUT to Link Policy 3 (Enabled in S0, Sx/AC), if the WLAN network interface is available. 5. Record the Host OS last boot time on the SUT (to verify reset execution). 6. Verify that Intel® AMT on the SUT responds to version queries via all available network interfaces. 7. Ensure yellow bang is not seen on Drivers in Device Manager
Procedure:	<ol style="list-style-type: none"> 1. Ensure that CF9h Global Reset (CF9GR) is cleared to 0b. 2. Perform a cold reset of the SUT by writing Eh to I/O register CF9h. 3. Verify that the SUT is in S0/MeOn (CM0,CM0-PG). 4. Wait 2 minutes before proceeding if the WLAN network interface is available. Because the Host OS may boot to error recovery screen following unexpected shutdown, the Host OS WLAN driver may not become available immediately. This delay allows enough time for Intel® AMT firmware to take control over the WLAN hardware and respond to manageability requests. 5. Verify that Intel® AMT on the SUT responds to version queries via all available network interfaces. 6. Verify the Host OS last boot time on the SUT does not match the boot time recorded before reset, or that the Host OS is unavailable. 7. Ensure yellow bang is not seen on Drivers in Device Manager
Pass Criteria:	<p>The test passes if:</p> <ul style="list-style-type: none"> • the SUT is reset to S0. • the Intel® CSME is available in MeOn (CM0, CM0-PG). • Intel® AMT responds to version queries via all available network interfaces. • the Host OS last boot time does not match, or the Host OS is unavailable.

12.21 ME_PM_18: Global Reset

Note: In order for Global reset tests to pass, the SUT should be in manufacturing mode.

ID:	ME_PM_18.1		
Title:	S0/CM0 to S0/CM0 via CF9 Global Reset (DC-only/PP1/LP3)		
Requirement:	Mandatory	Exemptions	<div><input checked="" type="checkbox"/> Non-Mobile (AC-only) systems</div> <div><input checked="" type="checkbox"/> Systems not in Intel® ME manufacturing mode</div>
Method:	Automated by Intel® PETS		
Objective:	This test checks the SUT power flow from S0/CM0 to S0/CM0 via CF9 Global Reset with the parameters outlined below.		
Configuration:	Intel® AMT should be provisioned via manual mode. Intel® ME should be configured in manufacturing mode. Confirm that the BIOS has not set the CF9 Lockdown. This test assumes that either LAN-only, WLAN-only, or both LAN and WLAN network interfaces are available on the SUT.		
Parameters:	System Power Source		DC-only
	Power States	Initial	S0/MeOn (CM0, CM0-PG)
		Final	S0/MeOn (CM0, CM0-PG)
		Trigger	CF9 Global Reset
	Intel® AMT	Power Package	PP1 (Intel® ME on in S0)
		WLAN Link Policy	LP3 (Enabled in S0, Sx/AC) where available



ID:	ME_PM_18.1
Setup:	<ol style="list-style-type: none"> 1. Set the SUT power source to AC+DC. 2. Bring the SUT to the base state of S0/MeOn (CM0,CM0-PG), and confirm that the Host OS is available. 3. Verify that a DC battery is connected to the SUT, and that it is charged. 4. Set the SUT power source to DC-only. 5. Set the active power package on the SUT to Power Package 1 (Intel® ME on in S0). 6. Set the Intel® AMT WLAN link policy on the SUT to Link Policy 3 (Enabled in S0, Sx/AC), if the WLAN network interface is available. 7. Record the Host OS last boot time on the SUT (to verify reset execution). 8. Verify that Intel® AMT on the SUT responds to version queries via all available network interfaces. 9. Verify that the Intel® ME is configured in manufacturing mode. 10. Ensure yellow bang is not seen on Drivers in Device Manager 11. Write 1b to CF6GR to enable global Reset.
Procedure:	<ol style="list-style-type: none"> 1. Ensure that CF9h Global Reset (CF9GR) is set to 1b to enable global reset. 2. Perform a global reset of the SUT by writing either 6h or Eh to I/O register CF9h. 3. Verify that the SUT is in S0/MeOn (CM0,CM0-PG). 4. Wait 2 minutes before proceeding if the WLAN network interface is available. Because the Host OS may boot to error recovery screen following unexpected shutdown, the Host OS WLAN driver may not become available immediately. This delay allows enough time for Intel® AMT firmware to take control over the WLAN hardware and respond to manageability requests. 5. Verify that Intel® AMT on the SUT responds to version queries via all available network interfaces. 6. Verify the Host OS last boot time on the SUT does not match the boot time recorded before reset, or that the Host OS is unavailable. 7. Ensure yellow bang is not seen on Drivers in Device Manager
Pass Criteria:	<p>The test passes if:</p> <ul style="list-style-type: none"> • the SUT is reset to S0. • the Intel® CSME is available in MeOn (CM0, CM0-PG). • Intel® AMT responds to version queries via all available network interfaces. • the Host OS last boot time does not match, or the Host OS is unavailable.

ID:	ME_PM_18.2		
Title:	S0/CM0 to S0/CM0 via CF9 Global Reset (AC+DC, AC-only/PP1/LP3)		
Requirement:	Mandatory	Exemptions	<input checked="" type="checkbox"/> Systems not in Intel® ME manufacturing mode
Method:	Automated by Intel® PETS		
Objective:	This test checks the SUT power flow from S0/CM0 to S0/CM0 via CF9 Global Reset with the parameters outlined below.		
Configuration:	Intel® AMT should be provisioned via manual mode. Intel® ME should be configured in manufacturing mode. Confirm that the BIOS has not set the CF9 Lockdown. This test assumes that either LAN-only, WLAN-only, or both LAN and WLAN network interfaces are available on the SUT.		
Parameters:	System Power Source		AC+DC or AC-only
	Power States	Initial	S0/MeOn (CM0, CM0-PG)
		Final	S0/MeOn (CM0, CM0-PG)
		Trigger	CF9 Global Reset
	Intel® AMT	Power Package	PP1 (Intel® ME on in S0)
		WLAN Link Policy	LP3 (Enabled in S0, Sx/AC) where available



ID:	ME_PM_18.2
Setup:	<ol style="list-style-type: none"> 1. Set the SUT power source to AC+DC where supported; otherwise AC-only. 2. Bring the SUT to the base state of S0/MeOn (CM0,CM0-PG), and confirm that the Host OS is available. 3. Set the active power package on the SUT to Power Package 1 (Intel® ME on in S0). 4. Set the Intel® AMT WLAN link policy on the SUT to Link Policy 3 (Enabled in S0, Sx/AC), if the WLAN network interface is available. 5. Record the Host OS last boot time on the SUT (to verify reset execution). 6. Verify that Intel® AMT on the SUT responds to version queries via all available network interfaces. 7. Verify that the Intel® ME is configured in manufacturing mode. 8. Ensure yellow bang is not seen on Drivers in Device Manager 9. Write 1b to CF6GR to enable global Reset.
Procedure:	<ol style="list-style-type: none"> 1. Ensure that CF9h Global Reset (CF9GR) is set to 1b to enable global reset. 2. Perform a global reset of the SUT by writing either 6h or Eh to I/O register CF9h. 3. Verify that the SUT is in S0/MeOn (CM0,CM0-PG). 4. Wait 2 minutes before proceeding if the WLAN network interface is available. Because the Host OS may boot to error recovery screen following unexpected shutdown, the Host OS WLAN driver may not become available immediately. This delay allows enough time for Intel® AMT firmware to take control over the WLAN hardware and respond to manageability requests. 5. Verify that Intel® AMT on the SUT responds to version queries via all available network interfaces. 6. Verify the Host OS last boot time on the SUT does not match the boot time recorded before reset, or that the Host OS is unavailable. 7. Ensure yellow bang is not seen on Drivers in Device Manager
Pass Criteria:	<p>The test passes if:</p> <ul style="list-style-type: none"> • the SUT is reset to S0. • the Intel® CSME is available in MeOn (CM0, CM0-PG). • Intel® AMT responds to version queries via all available network interfaces. • the Host OS last boot time does not match, or the Host OS is unavailable.

ID:	ME_PM_18.3		
Title:	S0/CM0 to S0/CM0 via CF9 Global Reset (DC-only/PP2/LP3)		
Requirement:	Mandatory	Exemptions	<input checked="" type="checkbox"/> Non-Mobile (AC-only) systems
			<input checked="" type="checkbox"/> Systems not in Intel® ME manufacturing mode
Method:	Automated by Intel® PETS		
Objective:	This test checks the SUT power flow from S0/CM0 to S0/CM0 via CF9 Global Reset with the parameters outlined below.		
Configuration:	Intel® AMT should be provisioned via manual mode.		
	Intel® ME should be configured in manufacturing mode.		
	Confirm that the BIOS has not set the CF9 Lockdown.		
	This test assumes that either LAN-only, WLAN-only, or both LAN and WLAN network interfaces are available on the SUT.		
Parameters:	System Power Source		DC-only
	Power States	Initial	S0/MeOn (CM0, CM0-PG)
		Final	S0/MeOn (CM0, CM0-PG)
		Trigger	CF9 Global Reset
	Intel® AMT	Power Package	PP2 (Intel® ME on in S0, wake in Sx/AC)
		WLAN Link Policy	LP3 (Enabled in S0, Sx/AC) where available



ID:	ME_PM_18.3
Setup:	<ol style="list-style-type: none"> 1. Set the SUT power source to AC+DC. 2. Bring the SUT to the base state of S0/MeOn (CM0,CM0-PG), and confirm that the Host OS is available. 3. Verify that a DC battery is connected to the SUT, and that it is charged. 4. Set the SUT power source to DC-only. 5. Set the active power package on the SUT to Power Package 2 (Intel® ME on in S0, wake in Sx/AC). 6. Set the Intel® AMT WLAN link policy on the SUT to Link Policy 3 (Enabled in S0, Sx/AC), if the WLAN network interface is available. 7. Record the Host OS last boot time on the SUT (to verify reset execution). 8. Verify that Intel® AMT on the SUT responds to version queries via all available network interfaces. 9. Verify that the Intel® ME is configured in manufacturing mode. 10. Ensure yellow bang is not seen on Drivers in Device Manager 11. Write 1b to CF6GR to enable global Reset.
Procedure:	<ol style="list-style-type: none"> 1. Ensure that CF9h Global Reset (CF9GR) is set to 1b to enable global reset. 2. Perform a global reset of the SUT by writing either 6h or Eh to I/O register CF9h. 3. Verify that the SUT is in S0/MeOn (CM0,CM0-PG). 4. Wait 2 minutes before proceeding if the WLAN network interface is available. Because the Host OS may boot to error recovery screen following unexpected shutdown, the Host OS WLAN driver may not become available immediately. This delay allows enough time for Intel® AMT firmware to take control over the WLAN hardware and respond to manageability requests. 5. Verify that Intel® AMT on the SUT responds to version queries via all available network interfaces. 6. Verify the Host OS last boot time on the SUT does not match the boot time recorded before reset, or that the Host OS is unavailable. 7. Ensure yellow bang is not seen on Drivers in Device Manager
Pass Criteria:	<p>The test passes if:</p> <ul style="list-style-type: none"> • the SUT is reset to S0. • the Intel® CSME is available in MeOn (CM0, CM0-PG). • Intel® AMT responds to version queries via all available network interfaces. • the Host OS last boot time does not match, or the Host OS is unavailable.

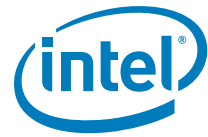
ID:	ME_PM_18.4		
Title:	S0/CM0 to S0/CM0 via CF9 Global Reset (AC+DC, AC-only/PP2/LP3)		
Requirement:	Mandatory	Exemptions	<input checked="" type="checkbox"/> Systems not in Intel® ME manufacturing mode
Method:	Automated by Intel® PETS		
Objective:	This test checks the SUT power flow from S0/CM0 to S0/CM0 via CF9 Global Reset with the parameters outlined below.		
Configuration:	Intel® AMT should be provisioned via manual mode. Intel® ME should be configured in manufacturing mode. Confirm that the BIOS has not set the CF9 Lockdown. This test assumes that either LAN-only, WLAN-only, or both LAN and WLAN network interfaces are available on the SUT.		
Parameters:	System Power Source		AC+DC or AC-only
	Power States	Initial	S0/MeOn (CM0, CM0-PG)
		Final	S0/MeOn (CM0, CM0-PG)
		Trigger	CF9 Global Reset
	Intel® AMT	Power Package	PP2 (Intel® ME on in S0, wake in Sx/AC)
		WLAN Link Policy	LP3 (Enabled in S0, Sx/AC) where available



ID:	ME_PM_18.4
Setup:	<ol style="list-style-type: none"> 1. Set the SUT power source to AC+DC where supported; otherwise AC-only. 2. Bring the SUT to the base state of S0/MeOn (CM0,CM0-PG), and confirm that the Host OS is available. 3. Set the active power package on the SUT to Power Package 2 (Intel® ME on in S0, wake in Sx/AC). 4. Set the Intel® AMT WLAN link policy on the SUT to Link Policy 3 (Enabled in S0, Sx/AC), if the WLAN network interface is available. 5. Record the Host OS last boot time on the SUT (to verify reset execution). 6. Verify that Intel® AMT on the SUT responds to version queries via all available network interfaces. 7. Verify that the Intel® ME is configured in manufacturing mode. 8. Ensure yellow bang is not seen on Drivers in Device Manager 9. Write 1b to CF6GR to enable global Reset.
Procedure:	<ol style="list-style-type: none"> 1. Ensure that CF9h Global Reset (CF9GR) is set to 1b to enable global reset. 2. Perform a global reset of the SUT by writing either 6h or Eh to I/O register CF9h. 3. Verify that the SUT is in S0/MeOn (CM0,CM0-PG). 4. Wait 2 minutes before proceeding if the WLAN network interface is available. Because the Host OS may boot to error recovery screen following unexpected shutdown, the Host OS WLAN driver may not become available immediately. This delay allows enough time for Intel® AMT firmware to take control over the WLAN hardware and respond to manageability requests. 5. Verify that Intel® AMT on the SUT responds to version queries via all available network interfaces. 6. Verify the Host OS last boot time on the SUT does not match the boot time recorded before reset, or that the Host OS is unavailable. 7. Ensure yellow bang is not seen on Drivers in Device Manager
Pass Criteria:	<p>The test passes if:</p> <ul style="list-style-type: none"> • the SUT is reset to S0. • the Intel® CSME is available in MeOn (CM0, CM0-PG). • Intel® AMT responds to version queries via all available network interfaces. • the Host OS last boot time does not match, or the Host OS is unavailable.

12.22 ME_PM_19: Straight-to-S5, Intel® ME Power Policy is S0 Only

ID:	ME_PM_19.1	
Title:	S0/CM0 to S5/CM-Off via Power Button override (DC-only/PP1/LP3)	
Requirement:	Mandatory	Exemptions <input checked="" type="checkbox"/> Non-Mobile (AC-only) systems
Method:	Automated by Intel® PETS	
Objective:	This test checks the SUT power flow from S0/CM0 to S5/CM-Off via Power Button override with the parameters outlined below.	
Configuration:	<p>Intel® AMT should be provisioned via manual mode.</p> <p>If Deep S5 and/or G3 are supported on the SUT, please confirm the following:</p> <ul style="list-style-type: none"> • the SUT and/or BIOS are properly configured to permit Deep S5 or G3 entry. • the correct Deep Sx policy is applied to the SUT profile in Intel® PETS. <p>This test assumes that either LAN-only, WLAN-only, or both LAN and WLAN network interfaces are available on the SUT.</p>	
Parameters:	System Power Source	
	DC-only	
	Power States	Initial S0/MeOn (CM0, CM0-PG)
		Final S5, Deep S5, G3/MeOff (CM-Off)
		Trigger Power Button override
	Intel® AMT	Power Package PP1 (Intel® ME on in S0)
		WLAN Link Policy LP3 (Enabled in S0, Sx/AC) where available



ID:	ME_PM_19.1
Setup:	<ol style="list-style-type: none"> 1. Set the SUT power source to AC+DC. 2. Bring the SUT to the base state of S0/MeOn (CM0,CM0-PG), and confirm that the Host OS is available. 3. Verify that a DC battery is connected to the SUT, and that it is charged. 4. Set the SUT power source to DC-only. 5. Set the active power package on the SUT to Power Package 1 (Intel® ME on in S0). 6. Set the Intel® AMT WLAN link policy on the SUT to Link Policy 3 (Enabled in S0, Sx/AC), if the WLAN network interface is available. 7. Ensure that the Host OS network device drivers are configured to not wake the SUT. This includes enabling ARP and/or NS Offload features where available to help prevent unexpected host wake events. 8. Verify that Intel® AMT on the SUT responds to version queries via all available network interfaces.
Procedure:	<ol style="list-style-type: none"> 1. Shutdown the SUT via a Power Button press for more than 5 seconds. 2. Verify that the SUT is in S5, Deep S5, G3/MeOff (CM-Off).
Pass Criteria:	The test passes if the SUT moves to S5 (or Deep S5 or G3), and the Intel® CSME moves to MeOff (CM-Off).

ID:	ME_PM_19.2		
Title:	S0/CM0 to S5/CM-Off via Power Button override (AC+DC, AC-only/PP1/LP3)		
Requirement:	Mandatory	Exemptions	None
Method:	Automated by Intel® PETS		
Objective:	This test checks the SUT power flow from S0/CM0 to S5/CM-Off via Power Button override with the parameters outlined below.		
Configuration:	<p>Intel® AMT should be provisioned via manual mode.</p> <p>If Deep S5 and/or G3 are supported on the SUT, please confirm the following:</p> <ul style="list-style-type: none"> • the SUT and/or BIOS are properly configured to permit Deep S5 or G3 entry. • the correct Deep Sx policy is applied to the SUT profile in Intel® PETS. <p>This test assumes that either LAN-only, WLAN-only, or both LAN and WLAN network interfaces are available on the SUT.</p>		
Parameters:	System Power Source		AC+DC or AC-only
	Power States	Initial	S0/MeOn (CM0, CM0-PG)
		Final	S5, Deep S5, G3/MeOff (CM-Off)
		Trigger	Power Button override
	Intel® AMT	Power Package	PP1 (Intel® ME on in S0)
		WLAN Link Policy	LP3 (Enabled in S0, Sx/AC) where available
Setup:	<ol style="list-style-type: none"> 1. Set the SUT power source to AC+DC where supported; otherwise AC-only. 2. Bring the SUT to the base state of S0/MeOn (CM0,CM0-PG), and confirm that the Host OS is available. 3. Set the active power package on the SUT to Power Package 1 (Intel® ME on in S0). 4. Set the Intel® AMT WLAN link policy on the SUT to Link Policy 3 (Enabled in S0, Sx/AC), if the WLAN network interface is available. 5. Ensure that the Host OS network device drivers are configured to not wake the SUT. This includes enabling ARP and/or NS Offload features where available to help prevent unexpected host wake events. 6. Verify that Intel® AMT on the SUT responds to version queries via all available network interfaces. 		
Procedure:	<ol style="list-style-type: none"> 1. Shutdown the SUT via a Power Button press for more than 5 seconds. 2. Verify that the SUT is in S5, Deep S5, G3/MeOff (CM-Off). 		
Pass Criteria:	The test passes if the SUT moves to S5 (or Deep S5 or G3), and the Intel® CSME moves to MeOff (CM-Off).		



ID:	ME_PM_19.3																
Title:	S3/CM-Off to S5/CM-Off via Power Button override (DC-only/PP1/LP3)																
Requirement:	Mandatory	Exemptions	<input checked="" type="checkbox"/> Non-Mobile (AC-only) systems <input checked="" type="checkbox"/> Modern Standby and InstantGo* systems														
Method:	Automated by Intel® PETS																
Objective:	This test checks the SUT power flow from S3/CM-Off to S5/CM-Off via Power Button override with the parameters outlined below.																
Configuration:	This test assumes that either LAN-only, WLAN-only, or both LAN and WLAN network interfaces are available on the SUT.																
Parameters:	<table><tr><td rowspan="4">Power States</td><td>System Power Source</td><td>DC-only</td></tr><tr><td>Initial</td><td>S3/MeOff (CM-Off)</td></tr><tr><td>Final</td><td>S5, Deep S5, G3/MeOff (CM-Off)</td></tr><tr><td>Trigger</td><td>Power Button override</td></tr><tr><td rowspan="2">Intel® AMT</td><td>Power Package</td><td>PP1 (Intel® ME on in S0)</td></tr><tr><td>WLAN Link Policy</td><td>LP3 (Enabled in S0, Sx/AC) where available</td></tr></table>			Power States	System Power Source	DC-only	Initial	S3/MeOff (CM-Off)	Final	S5, Deep S5, G3/MeOff (CM-Off)	Trigger	Power Button override	Intel® AMT	Power Package	PP1 (Intel® ME on in S0)	WLAN Link Policy	LP3 (Enabled in S0, Sx/AC) where available
Power States	System Power Source	DC-only															
	Initial	S3/MeOff (CM-Off)															
	Final	S5, Deep S5, G3/MeOff (CM-Off)															
	Trigger	Power Button override															
Intel® AMT	Power Package	PP1 (Intel® ME on in S0)															
	WLAN Link Policy	LP3 (Enabled in S0, Sx/AC) where available															
Setup:	<div>1. Set the SUT power source to AC+DC.</div> <div>2. Bring the SUT to the base state of S0/MeOn (CM0,CM0-PG), and confirm that the Host OS is available.</div> <div>3. Verify that a DC battery is connected to the SUT, and that it is charged.</div> <div>4. Set the SUT power source to DC-only.</div> <div>5. Set the active power package on the SUT to Power Package 1 (Intel® ME on in S0).</div> <div>6. Set the Intel® AMT WLAN link policy on the SUT to Link Policy 3 (Enabled in S0, Sx/AC), if the WLAN network interface is available.</div> <div>7. Ensure that the Host OS network device drivers are configured to not wake the SUT. This includes enabling ARP and/or NS Offload features where available to help prevent unexpected host wake events. Most especially, ensure that the Host OS Wireless Wake on LAN driver setting on the SUT is disabled, if the WLAN network interface is available.</div> <div>8. Ensure that Intel® RMT is disabled, if running on an All-in-One (AIO) SUT with feature support.</div> <div>9. Verify that Intel® AMT on the SUT responds to version queries via all available network interfaces.</div> <div>10. Suspend the SUT via the Host OS.</div> <div>11. Verify that the SUT is in S3/MeOff (CM-Off).</div> <div>12. Verify that the SUT is in S3, Deep S3/MeOff (CM-Off).</div>																
Procedure:	<div>1. Shutdown the SUT via a Power Button press for more than 5 seconds.</div> <div>2. Verify that the SUT is in S5, Deep S5, G3/MeOff (CM-Off).</div>																
Pass Criteria:	The test passes if the SUT moves to S5 (or Deep S5 or G3), and the Intel® CSME is in MeOff (CM-Off). Note: Some systems may briefly move electrically to S0 before final transition to S5 (or Deep S5 or G3).																

ID:	ME_PM_19.4		
Title:	S3/CM-Off to S5/CM-Off via Power Button override (AC+DC, AC-only/PP1/LP3)		
Requirement:	Mandatory	Exemptions	<input checked="" type="checkbox"/> Modern Standby and InstantGo* systems
Method:	Automated by Intel® PETS		
Objective:	This test checks the SUT power flow from S3/CM-Off to S5/CM-Off via Power Button override with the parameters outlined below.		
Configuration:	This test assumes that either LAN-only, WLAN-only, or both LAN and WLAN network interfaces are available on the SUT.		



ID:	ME_PM_19.4		
Parameters:	System Power Source		AC+DC or AC-only
	Power States	Initial	S3/MeOff (CM-Off)
		Final	S5, Deep S5, G3/MeOff (CM-Off)
		Trigger	Power Button override
	Intel® AMT	Power Package	PP1 (Intel® ME on in S0)
		WLAN Link Policy	LP3 (Enabled in S0, Sx/AC) where available
Setup:	<ol style="list-style-type: none"> Set the SUT power source to AC+DC where supported; otherwise AC-only. Bring the SUT to the base state of S0/MeOn (CM0,CM0-PG), and confirm that the Host OS is available. Set the active power package on the SUT to Power Package 1 (Intel® ME on in S0). Set the Intel® AMT WLAN link policy on the SUT to Link Policy 3 (Enabled in S0, Sx/AC), if the WLAN network interface is available. Ensure that the Host OS network device drivers are configured to not wake the SUT. This includes enabling ARP and/or NS Offload features where available to help prevent unexpected host wake events. Most especially, ensure that the Host OS Wireless Wake on LAN driver setting on the SUT is disabled, if the WLAN network interface is available. Ensure that Intel® RMT is disabled, if running on a Desktop or All-in-One (AIO) SUT with feature support. Verify that Intel® AMT on the SUT responds to version queries via all available network interfaces. Suspend the SUT via the Host OS. Verify that the SUT is in S3/MeOff (CM-Off). 		
Procedure:	<ol style="list-style-type: none"> Shutdown the SUT via a Power Button press for more than 5 seconds. Verify that the SUT is in S5, Deep S5, G3/MeOff (CM-Off). 		
Pass Criteria:	<p>The test passes if the SUT moves to S5 (or Deep S5 or G3), and the Intel® CSME is in MeOff (CM-Off).</p> <p>Note: Some systems may briefly move electrically to S0 before final transition to S5 (or Deep S5 or G3).</p>		

ID:	ME_PM_19.5		
Title:	S4/CM-Off to S5/CM-Off via Power Button override (DC-only/PP1/LP3)		
Requirement:	Mandatory	Exemptions	<input checked="" type="checkbox"/> Non-Mobile (AC-only) systems
Method:	Automated by Intel® PETS		
Objective:	This test checks the SUT power flow from S4/CM-Off to S5/CM-Off via Power Button override with the parameters outlined below.		
Configuration:	<p>Intel® AMT should be provisioned via manual mode.</p> <p>If Deep S4, Deep S5, and/or G3 are supported on the SUT, please confirm the following:</p> <ul style="list-style-type: none"> the SUT and/or BIOS are properly configured to permit Deep S4/S5 or G3 entry. the correct Deep Sx policy is applied to the SUT profile in Intel® PETS. <p>This test assumes that either LAN-only, WLAN-only, or both LAN and WLAN network interfaces are available on the SUT.</p>		
Parameters:	System Power Source		DC-only
	Power States	Initial	S4, S5, Deep S4, Deep S5, G3/MeOff (CM-Off)
		Final	S5, Deep S5, G3/MeOff (CM-Off)
		Trigger	Power Button override
	Intel® AMT	Power Package	PP1 (Intel® ME on in S0)
		WLAN Link Policy	LP3 (Enabled in S0, Sx/AC) where available



ID:	ME_PM_19.5
Setup:	<ol style="list-style-type: none"> 1. Set the SUT power source to AC+DC. 2. Bring the SUT to the base state of S0/MeOn (CM0,CM0-PG), and confirm that the Host OS is available. 3. Verify that a DC battery is connected to the SUT, and that it is charged. 4. Set the SUT power source to DC-only. 5. Set the active power package on the SUT to Power Package 1 (Intel® ME on in S0). 6. Set the Intel® AMT WLAN link policy on the SUT to Link Policy 3 (Enabled in S0, Sx/AC), if the WLAN network interface is available. 7. Ensure that the Host OS network device drivers are configured to not wake the SUT. This includes enabling ARP and/or NS Offload features where available to help prevent unexpected host wake events. 8. Verify that Intel® AMT on the SUT responds to version queries via all available network interfaces. 9. Hibernate the SUT via the Host OS. 10. Verify that the SUT is in S4, S5, Deep S4, Deep S5, G3/MeOff (CM-Off).
Procedure:	<ol style="list-style-type: none"> 1. Shutdown the SUT via a Power Button press for more than 5 seconds. 2. Verify that the SUT is in S5, Deep S5, G3/MeOff (CM-Off).
Pass Criteria:	<p>The test passes if the SUT moves to, if not already there, S5 (or Deep S5 or G3), and the Intel® CSME is in MeOff (CM-Off).</p> <p>Note: Some systems may briefly move electrically to S0 before final transition to S5 (or Deep S5 or G3).</p>

ID:	ME_PM_19.6																
Title:	S4/CM-Off to S5/CM-Off via Power Button override (AC+DC, AC-only/PP1/LP3)																
Requirement:	Mandatory	Exemptions None															
Method:	Automated by Intel® PETS																
Objective:	This test checks the SUT power flow from S4/CM-Off to S5/CM-Off via Power Button override with the parameters outlined below.																
Configuration:	<p>Intel® AMT should be provisioned via manual mode.</p> <p>If Deep S4, Deep S5, and/or G3 are supported on the SUT, please confirm the following:</p> <ul style="list-style-type: none"> • the SUT and/or BIOS are properly configured to permit Deep S4/S5 or G3 entry. • the correct Deep Sx policy is applied to the SUT profile in Intel® PETS. <p>This test assumes that either LAN-only, WLAN-only, or both LAN and WLAN network interfaces are available on the SUT.</p>																
Parameters:	<table border="1"> <thead> <tr> <th colspan="2">System Power Source</th><th>AC+DC or AC-only</th></tr> </thead> <tbody> <tr> <td rowspan="3">Power States</td><td>Initial</td><td>S4, S5, Deep S4, Deep S5, G3/MeOff (CM-Off)</td></tr> <tr> <td>Final</td><td>S5, Deep S5, G3/MeOff (CM-Off)</td></tr> <tr> <td>Trigger</td><td>Power Button override</td></tr> <tr> <td rowspan="2">Intel® AMT</td><td>Power Package</td><td>PP1 (Intel® ME on in S0)</td></tr> <tr> <td>WLAN Link Policy</td><td>LP3 (Enabled in S0, Sx/AC) where available</td></tr> </tbody> </table>		System Power Source		AC+DC or AC-only	Power States	Initial	S4, S5, Deep S4, Deep S5, G3/MeOff (CM-Off)	Final	S5, Deep S5, G3/MeOff (CM-Off)	Trigger	Power Button override	Intel® AMT	Power Package	PP1 (Intel® ME on in S0)	WLAN Link Policy	LP3 (Enabled in S0, Sx/AC) where available
System Power Source		AC+DC or AC-only															
Power States	Initial	S4, S5, Deep S4, Deep S5, G3/MeOff (CM-Off)															
	Final	S5, Deep S5, G3/MeOff (CM-Off)															
	Trigger	Power Button override															
Intel® AMT	Power Package	PP1 (Intel® ME on in S0)															
	WLAN Link Policy	LP3 (Enabled in S0, Sx/AC) where available															
Setup:	<ol style="list-style-type: none"> 1. Set the SUT power source to AC+DC where supported; otherwise AC-only. 2. Bring the SUT to the base state of S0/MeOn (CM0,CM0-PG), and confirm that the Host OS is available. 3. Set the active power package on the SUT to Power Package 1 (Intel® ME on in S0). 4. Set the Intel® AMT WLAN link policy on the SUT to Link Policy 3 (Enabled in S0, Sx/AC), if the WLAN network interface is available. 5. Ensure that the Host OS network device drivers are configured to not wake the SUT. This includes enabling ARP and/or NS Offload features where available to help prevent unexpected host wake events. 6. Verify that Intel® AMT on the SUT responds to version queries via all available network interfaces. 7. Hibernate the SUT via the Host OS. 8. Verify that the SUT is in S4, S5, Deep S4, Deep S5, G3/MeOff (CM-Off). 																
Procedure:	<ol style="list-style-type: none"> 1. Shutdown the SUT via a Power Button press for more than 5 seconds. 2. Verify that the SUT is in S5, Deep S5, G3/MeOff (CM-Off). 																
Pass Criteria:	<p>The test passes if the SUT moves to, if not already there, S5 (or Deep S5 or G3), and the Intel® CSME is in MeOff (CM-Off).</p> <p>Note: Some systems may briefly move electrically to S0 before final transition to S5 (or Deep S5 or G3).</p>																



ID:	ME_PM_19.7	
Title:	S5/CM-Off to S5/CM-Off via Power Button override (DC-only/PP1/LP3)	
Requirement:	Mandatory	Exemptions <input checked="" type="checkbox"/> Non-Mobile (AC-only) systems
Method:	Automated by Intel® PETS	
Objective:	This test checks the SUT power flow from S5/CM-Off to S5/CM-Off via Power Button override with the parameters outlined below.	
Configuration:	<p>Intel® AMT should be provisioned via manual mode.</p> <p>If Deep S5 and/or G3 are supported on the SUT, please confirm the following:</p> <ul style="list-style-type: none"> the SUT and/or BIOS are properly configured to permit Deep S5 or G3 entry. the correct Deep Sx policy is applied to the SUT profile in Intel® PETS. <p>This test assumes that either LAN-only, WLAN-only, or both LAN and WLAN network interfaces are available on the SUT.</p>	
Parameters:	System Power Source DC-only	
	Power States	Initial S5, Deep S5, G3/MeOff (CM-Off)
		Final S5, Deep S5, G3/MeOff (CM-Off)
		Trigger Power Button override
	Intel® AMT	Power Package PP1 (Intel® ME on in S0)
		WLAN Link Policy LP3 (Enabled in S0, Sx/AC) where available
Setup:	<ol style="list-style-type: none"> Set the SUT power source to AC+DC. Bring the SUT to the base state of S0/MeOn (CM0,CM0-PG), and confirm that the Host OS is available. Verify that a DC battery is connected to the SUT, and that it is charged. Set the SUT power source to DC-only. Set the active power package on the SUT to Power Package 1 (Intel® ME on in S0). Set the Intel® AMT WLAN link policy on the SUT to Link Policy 3 (Enabled in S0, Sx/AC), if the WLAN network interface is available. Ensure that the Host OS network device drivers are configured to not wake the SUT. This includes enabling ARP and/or NS Offload features where available to help prevent unexpected host wake events. Verify that Intel® AMT on the SUT responds to version queries via all available network interfaces. Shutdown the SUT via the Host OS. Verify that the SUT is in S5, Deep S5, G3/MeOff (CM-Off). 	
Procedure:	<ol style="list-style-type: none"> Shutdown the SUT via a Power Button press for more than 5 seconds. Verify that the SUT is in S5, Deep S5, G3/MeOff (CM-Off). 	
Pass Criteria:	<p>The test passes if the SUT ends the test in S5 (or Deep S5 or G3), and the Intel® CSME is in MeOff (CM-Off).</p> <p>Note: Some systems may briefly move electrically to S0 before final transition to S5 (or Deep S5 or G3).</p>	

ID:	ME_PM_19.8	
Title:	S5/CM-Off to S5/CM-Off via Power Button override (AC+DC, AC-only/PP1/LP3)	
Requirement:	Mandatory	Exemptions None
Method:	Automated by Intel® PETS	
Objective:	This test checks the SUT power flow from S5/CM-Off to S5/CM-Off via Power Button override with the parameters outlined below.	
Configuration:	<p>Intel® AMT should be provisioned via manual mode.</p> <p>If Deep S5 and/or G3 are supported on the SUT, please confirm the following:</p> <ul style="list-style-type: none"> the SUT and/or BIOS are properly configured to permit Deep S5 or G3 entry. the correct Deep Sx policy is applied to the SUT profile in Intel® PETS. <p>This test assumes that either LAN-only, WLAN-only, or both LAN and WLAN network interfaces are available on the SUT.</p>	



ID:	ME_PM_19.8		
Parameters:	System Power Source		AC+DC or AC-only
	Power States	Initial	S5, Deep S5, G3/MeOff (CM-Off)
		Final	S5, Deep S5, G3/MeOff (CM-Off)
		Trigger	Power Button override
	Intel® AMT	Power Package	PP1 (Intel® ME on in S0)
		WLAN Link Policy	LP3 (Enabled in S0, Sx/AC) where available
Setup:	<ol style="list-style-type: none"> 1. Set the SUT power source to AC+DC where supported; otherwise AC-only. 2. Bring the SUT to the base state of S0/MeOn (CM0,CM0-PG), and confirm that the Host OS is available. 3. Set the active power package on the SUT to Power Package 1 (Intel® ME on in S0). 4. Set the Intel® AMT WLAN link policy on the SUT to Link Policy 3 (Enabled in S0, Sx/AC), if the WLAN network interface is available. 5. Ensure that the Host OS network device drivers are configured to not wake the SUT. This includes enabling ARP and/or NS Offload features where available to help prevent unexpected host wake events. 6. Verify that Intel® AMT on the SUT responds to version queries via all available network interfaces. 7. Shutdown the SUT via the Host OS. 8. Verify that the SUT is in S5, Deep S5, G3/MeOff (CM-Off). 		
Procedure:	<ol style="list-style-type: none"> 1. Shutdown the SUT via a Power Button press for more than 5 seconds. 2. Verify that the SUT is in S5, Deep S5, G3/MeOff (CM-Off). 		
Pass Criteria:	<p>The test passes if the SUT ends the test in S5 (or Deep S5 or G3), and the Intel® CSME is in MeOff (CM-Off). Note: Some systems may briefly move electrically to S0 before final transition to S5 (or Deep S5 or G3).</p>		

ID:	ME_PM_19.9		
Title:	S0/CM0 to G3/CM-Off via Power loss (DC-only/PP1/LP3)		
Requirement:	Mandatory	Exemptions	<input checked="" type="checkbox"/> Non-Mobile (AC-only) systems
Method:	Automated by Intel® PETS		
Objective:	This test checks the SUT power flow from S0/CM0 to G3/CM-Off via Power loss with the parameters outlined below.		
Configuration:	<p>Intel® AMT should be provisioned via manual mode.</p> <p>If Deep S5 and/or G3 are supported on the SUT, please confirm the following:</p> <ul style="list-style-type: none"> • the SUT and/or BIOS are properly configured to permit Deep S5 or G3 entry. • the correct Deep Sx policy is applied to the SUT profile in Intel® PETS. <p>This test assumes that either LAN-only, WLAN-only, or both LAN and WLAN network interfaces are available on the SUT.</p>		
Parameters:	System Power Source		DC-only
	Power States	Initial	S0/MeOn (CM0, CM0-PG)
		Final	S5, Deep S5, G3/MeOff (CM-Off)
		Trigger	Power loss
	Intel® AMT	Power Package	PP1 (Intel® ME on in S0)
		WLAN Link Policy	LP3 (Enabled in S0, Sx/AC) where available



ID:	ME_PM_19.9
Setup:	<ol style="list-style-type: none"> 1. Set the SUT power source to AC+DC. 2. Bring the SUT to the base state of S0/MeOn (CM0,CM0-PG), and confirm that the Host OS is available. 3. Verify that a DC battery is connected to the SUT, and that it is charged. 4. Set the SUT power source to DC-only. 5. Set the active power package on the SUT to Power Package 1 (Intel® ME on in S0). 6. Set the Intel® AMT WLAN link policy on the SUT to Link Policy 3 (Enabled in S0, Sx/AC), if the WLAN network interface is available. 7. Ensure that the Host OS network device drivers are configured to not wake the SUT. This includes enabling ARP and/or NS Offload features where available to help prevent unexpected host wake events. 8. Verify that Intel® AMT on the SUT responds to version queries via all available network interfaces.
Procedure:	<ol style="list-style-type: none"> 1. Put the system to S5/ G3 via Unconditional Power Loss. 2. Verify that the SUT is in S5, Deep S5, G3/MeOff (CM-Off).
Pass Criteria:	The test passes if the SUT moves to S5 (or Deep S5 or G3), and the Intel® CSME moves to MeOff (CM-Off).

12.23 ME_PM_20: Straight-to-S5 via Power Button Override

ID:	ME_PM_20.1		
Title:	S0/CM0 to S5/CM3 via Power Button override (AC+DC, AC-only/PP2/LP3)		
Requirement:	Mandatory	Exemptions	None
Method:	Automated by Intel® PETS		
Objective:	This test checks the SUT power flow from S0/CM0 to S5/CM3 via Power Button override with the parameters outlined below.		
Configuration:	Intel® AMT should be provisioned via manual mode. This test assumes that either LAN-only, WLAN-only, or both LAN and WLAN network interfaces are available on the SUT.		
Parameters:	System Power Source		AC+DC or AC-only
	Power States	Initial	S0/MeOn (CM0, CM0-PG)
		Final	S5/MeOn (CM3)
		Trigger	Power Button override
	Intel® AMT	Power Package	PP2 (Intel® ME on in S0, wake in Sx/AC)
		WLAN Link Policy	LP3 (Enabled in S0, Sx/AC) where available
Setup:	<ol style="list-style-type: none"> 1. Set the SUT power source to AC+DC where supported; otherwise AC-only. 2. Bring the SUT to the base state of S0/MeOn (CM0,CM0-PG), and confirm that the Host OS is available. 3. Set the active power package on the SUT to Power Package 2 (Intel® ME on in S0, wake in Sx/AC). 4. Set the Intel® AMT WLAN link policy on the SUT to Link Policy 3 (Enabled in S0, Sx/AC), if the WLAN network interface is available. 5. Ensure that the Host OS network device drivers are configured to not wake the SUT. This includes enabling ARP and/or NS Offload features where available to help prevent unexpected host wake events. 6. Verify that Intel® AMT on the SUT responds to version queries via all available network interfaces. 		
Procedure:	<ol style="list-style-type: none"> 1. Shutdown the SUT via a Power Button press for more than 5 seconds. 2. Verify that the SUT is in S5/MeOn (CM3). 3. Verify that Intel® AMT on the SUT responds to version queries via all available network interfaces. 		
Pass Criteria:	The test passes if: <ul style="list-style-type: none"> • the SUT moves to S5. • the Intel® CSME is in MeOn (CM3). • Intel® AMT responds to version queries via all available network interfaces. Note: Some systems may briefly move electrically to S0 before final transition to S5.		



ID:	ME_PM_20.2		
Title:	S0/CM0 to S5/CM3-PG with AC Wake via Power Button override (DC-only/PP2/LP3)		
Requirement:	Mandatory	Exemptions	<input checked="" type="checkbox"/> Non-Mobile (AC-only) systems
Method:	Automated by Intel® PETS		
Objective:	This test checks the SUT power flow from S0/CM0 to S5/CM3-PG with Ac Wake via Power Button override with the parameters outlined below.		
Configuration:	<p>Intel® AMT should be provisioned via manual mode.</p> <p>If Deep S5 and/or G3 are supported on the SUT, please confirm the following:</p> <ul style="list-style-type: none"> the SUT and/or BIOS are properly configured to permit Deep S5 or G3 entry. the correct Deep Sx policy is applied to the SUT profile in Intel® PETS. <p>This test assumes that either LAN-only, WLAN-only, or both LAN and WLAN network interfaces are available on the SUT.</p>		
Parameters:	System Power Source		DC-only
	Power States	Initial	S0/MeOn (CM0, CM0-PG)
		Final	S5,Deep S5,G3/CM3-PG with AC Wake
		Trigger	Power Button override
	Intel® AMT	Power Package	PP2 (Intel® ME on in S0, wake in Sx/AC)
		WLAN Link Policy	LP3 (Enabled in S0, Sx/AC) where available
Setup:	<ol style="list-style-type: none"> Set the SUT power source to AC+DC. Bring the SUT to the base state of S0/MeOn (CM0,CM0-PG), and confirm that the Host OS is available. Verify that a DC battery is connected to the SUT, and that it is charged. Set the SUT power source to DC-only. Set the active power package on the SUT to Power Package 2 (Intel® ME on in S0, wake in Sx/AC). Set the Intel® AMT WLAN link policy on the SUT to Link Policy 3 (Enabled in S0, Sx/AC), if the WLAN network interface is available. Ensure that the Host OS network device drivers are configured to not wake the SUT. This includes enabling ARP and/or NS Offload features where available to help prevent unexpected host wake events. Verify that Intel® AMT on the SUT responds to version queries via all available network interfaces. 		
Procedure:	<ol style="list-style-type: none"> Shutdown the SUT via a Power Button press for more than 5 seconds. Verify that the SUT is in S5, Deep S5, G3/CM3-PG.with AC Wake 		
Pass Criteria:	The test passes if the SUT moves to S5 (or Deep S5 or G3), and the Intel® CSME moves to CM3-PG with AC Wake.		

ID:	ME_PM_20.3		
Title:	S3/CM3 to S5/CM3 via Power Button override (AC+DC, AC-only/PP2/LP3)		
Requirement:	Mandatory	Exemptions	<input checked="" type="checkbox"/> Modern Standby and InstantGo* systems
Method:	Automated by Intel® PETS		
Objective:	This test checks the SUT power flow from S3/CM3 to S5/CM3 via Power Button override with the parameters outlined below.		
Configuration:	<p>Intel® AMT should be provisioned via manual mode.</p> <p>This test assumes that either LAN-only, WLAN-only, or both LAN and WLAN network interfaces are available on the SUT.</p>		
Parameters:	System Power Source		AC+DC or AC-only
	Power States	Initial	S3/MeOn (CM3)
		Final	S5/MeOn (CM3)
		Trigger	Power Button override
	Intel® AMT	Power Package	PP2 (Intel® ME on in S0, wake in Sx/AC)
		WLAN Link Policy	LP3 (Enabled in S0, Sx/AC) where available



ID:	ME_PM_20.3
Setup:	<ol style="list-style-type: none"> 1. Set the SUT power source to AC+DC where supported; otherwise AC-only. 2. Bring the SUT to the base state of S0/MeOn (CM0,CM0-PG), and confirm that the Host OS is available. 3. Set the active power package on the SUT to Power Package 2 (Intel® ME on in S0, wake in Sx/AC). 4. Set the Intel® AMT WLAN link policy on the SUT to Link Policy 3 (Enabled in S0, Sx/AC), if the WLAN network interface is available. 5. Ensure that the Host OS network device drivers are configured to not wake the SUT. This includes enabling ARP and/or NS Offload features where available to help prevent unexpected host wake events. Most especially, ensure that the Host OS Wireless Wake on LAN driver setting on the SUT is disabled, if the WLAN network interface is available. 6. Ensure that Intel® RMT is disabled, if running on a Desktop or All-in-One (AIO) SUT with feature support. 7. Verify that Intel® AMT on the SUT responds to version queries via all available network interfaces. 8. Suspend the SUT via the Host OS. 9. Verify that the SUT is in S3/MeOn (CM3). 10. Verify that Intel® AMT on the SUT responds to version queries via all available network interfaces.
Procedure:	<ol style="list-style-type: none"> 1. Shutdown the SUT via a Power Button press for more than 5 seconds. 2. Verify that the SUT is in S5/MeOn (CM3). 3. Verify that Intel® AMT on the SUT responds to version queries via all available network interfaces.
Pass Criteria:	<p>The test passes if:</p> <ul style="list-style-type: none"> • the SUT moves to S5. • the Intel® CSME is in MeOn (CM3). • Intel® AMT responds to version queries via all available network interfaces. <p>Note: Some systems may briefly move electrically to S0 before final transition to S5.</p>

ID:	ME_PM_20.4	
Title:	S3/CM3-PG to S5/CM3 via Power Button override (AC+DC, AC-only/PP2/LP3)	
Requirement:	Mandatory	Exemptions <input checked="" type="checkbox"/> Modern Standby and InstantGo* systems
Method:	Automated by Intel® PETS	
Objective:	This test checks the SUT power flow from S3/CM3-PG to S5/CM3 via Power Button override with the parameters outlined below.	
Configuration:	Intel® AMT should be provisioned via manual mode. This test assumes that either LAN-only, WLAN-only, or both LAN and WLAN network interfaces are available on the SUT.	
Parameters:	System Power Source	AC+DC or AC-only
	Power States	Initial S3/CM3-PG
		Final S5/MeOn (CM3)
		Trigger Power Button override
	Intel® AMT	Power Package PP2 (Intel® ME on in S0, wake in Sx/AC) WLAN Link Policy LP3 (Enabled in S0, Sx/AC) where available



ID:	ME_PM_20.4
Setup:	<ol style="list-style-type: none"> 1. Set the SUT power source to AC+DC where supported; otherwise AC-only. 2. Bring the SUT to the base state of S0/MeOn (CM0,CM0-PG), and confirm that the Host OS is available. 3. Set the active power package on the SUT to Power Package 2 (Intel® ME on in S0, wake in Sx/AC). 4. Set the Intel® AMT WLAN link policy on the SUT to Link Policy 3 (Enabled in S0, Sx/AC), if the WLAN network interface is available. 5. Ensure the Intel® AMT idle timeout on the SUT is set to 1 minute. 6. Ensure that the Host OS network device drivers are configured to not wake the SUT. This includes enabling ARP and/or NS Offload features where available to help prevent unexpected host wake events. Most especially, ensure that the Host OS Wireless Wake on LAN driver setting on the SUT is disabled, if the WLAN network interface is available. 7. Ensure that Intel® RMT is disabled, if running on a Desktop or All-in-One (AIO) SUT with feature support. 8. Verify that Intel® AMT on the SUT responds to version queries via all available network interfaces. 9. Suspend the SUT via the Host OS. 10. Verify that the SUT is in S3/MeOn (CM3). 11. Verify that Intel® AMT on the SUT responds to version queries via all available network interfaces. 12. Wait for 3 minutes to allow the Intel® ME on the SUT to move to CM3-PG after Intel® AMT idle timeout. 13. Verify that the Intel® ME on the SUT is in CM3-PG.
Procedure:	<ol style="list-style-type: none"> 1. Shutdown the SUT via a Power Button press for more than 5 seconds. 2. Verify that the SUT is in S5/MeOn (CM3). 3. Verify that Intel® AMT on the SUT responds to version queries via all available network interfaces.
Pass Criteria:	<p>The test passes if:</p> <ul style="list-style-type: none"> • the SUT moves to S5. • the Intel® CSME is in MeOn (CM3). • Intel® AMT responds to version queries via all available network interfaces. <p>Note: Some systems may briefly move electrically to S0 before final transition to S5.</p>

ID:	ME_PM_20.5		
Title:	S4/CM3 to S5/CM3 via Power Button override (AC+DC, AC-only/PP2/LP3)		
Requirement:	Mandatory	Exemptions	None
Method:	Automated by Intel® PETS		
Objective:	This test checks the SUT power flow from S4/CM3 to S5/CM3 via Power Button override with the parameters outlined below.		
Configuration:	<p>Intel® AMT should be provisioned via manual mode.</p> <p>This test assumes that either LAN-only, WLAN-only, or both LAN and WLAN network interfaces are available on the SUT.</p>		
Parameters:	System Power Source		AC+DC or AC-only
	Power States	Initial	S4,S5/MeOn (CM3)
		Final	S5/MeOn (CM3)
		Trigger	Power Button override
	Intel® AMT	Power Package	PP2 (Intel® ME on in S0, wake in Sx/AC)
		WLAN Link Policy	LP3 (Enabled in S0, Sx/AC) where available



ID:	ME_PM_20.5
Setup:	<ol style="list-style-type: none"> 1. Set the SUT power source to AC+DC where supported; otherwise AC-only. 2. Bring the SUT to the base state of S0/MeOn (CM0,CM0-PG), and confirm that the Host OS is available. 3. Set the active power package on the SUT to Power Package 2 (Intel® ME on in S0, wake in Sx/AC). 4. Set the Intel® AMT WLAN link policy on the SUT to Link Policy 3 (Enabled in S0, Sx/AC), if the WLAN network interface is available. 5. Ensure that the Host OS network device drivers are configured to not wake the SUT. This includes enabling ARP and/or NS Offload features where available to help prevent unexpected host wake events. 6. Verify that Intel® AMT on the SUT responds to version queries via all available network interfaces. 7. Hibernate the SUT via the Host OS. 8. Verify that the SUT is in S4, S5/MeOn (CM3). 9. Verify that Intel® AMT on the SUT responds to version queries via all available network interfaces.
Procedure:	<ol style="list-style-type: none"> 1. Shutdown the SUT via a Power Button press for more than 5 seconds. 2. Verify that the SUT is in S5/MeOn (CM3). 3. Verify that Intel® AMT on the SUT responds to version queries via all available network interfaces.
Pass Criteria:	<p>The test passes if:</p> <ul style="list-style-type: none"> • the SUT moves to S5. • the Intel® CSME is in MeOn (CM3). • Intel® AMT responds to version queries via all available network interfaces. <p>Note: Some systems may briefly move electrically to S0 before final transition to S5.</p>

ID:	ME_PM_20.6		
Title:	S4/CM3-PG to S5/CM3 via Power Button override (AC+DC, AC-only/PP2/LP3)		
Requirement:	Mandatory	Exemptions	None
Method:	Automated by Intel® PETS		
Objective:	This test checks the SUT power flow from S4/CM3-PG to S5/CM3 via Power Button override with the parameters outlined below.		
Configuration:	Intel® AMT should be provisioned via manual mode. This test assumes that either LAN-only, WLAN-only, or both LAN and WLAN network interfaces are available on the SUT.		
Parameters:	System Power Source		AC+DC or AC-only
	Power States	Initial	S4,S5/MeOff (CM3-PG)
		Final	S5/MeOn (CM3)
		Trigger	Power Button override
	Intel® AMT	Power Package	PP2 (Intel® ME on in S0, wake in Sx/AC)
		WLAN Link Policy	LP3 (Enabled in S0, Sx/AC) where available



ID:	ME_PM_20.6
Setup:	<ol style="list-style-type: none"> 1. Set the SUT power source to AC+DC where supported; otherwise AC-only. 2. Bring the SUT to the base state of S0/MeOn (CM0,CM0-PG), and confirm that the Host OS is available. 3. Set the active power package on the SUT to Power Package 2 (Intel® ME on in S0, wake in Sx/AC). 4. Set the Intel® AMT WLAN link policy on the SUT to Link Policy 3 (Enabled in S0, Sx/AC), if the WLAN network interface is available. 5. Ensure the Intel® AMT idle timeout on the SUT is set to 1 minute. 6. Ensure that the Host OS network device drivers are configured to not wake the SUT. This includes enabling ARP and/or NS Offload features where available to help prevent unexpected host wake events. 7. Verify that Intel® AMT on the SUT responds to version queries via all available network interfaces. 8. Hibernate the SUT via the Host OS. 9. Verify that the SUT is in S4, S5/MeOn (CM3). 10. Verify that Intel® AMT on the SUT responds to version queries via all available network interfaces. 11. Wait for 3 minutes to allow the Intel® ME on the SUT to move to CM3-PG after Intel® AMT idle timeout. 12. Verify that the Intel® ME on the SUT is in CM3-PG.
Procedure:	<ol style="list-style-type: none"> 1. Shutdown the SUT via a Power Button press for more than 5 seconds. 2. Verify that the SUT is in S5/MeOn (CM3). 3. Verify that Intel® AMT on the SUT responds to version queries via all available network interfaces.
Pass Criteria:	<p>The test passes if:</p> <ul style="list-style-type: none"> • the SUT moves to S5. • the Intel® CSME is in MeOn (CM3). • Intel® AMT responds to version queries via all available network interfaces. <p>Note: Some systems may briefly move electrically to S0 before final transition to S5.</p>

ID:	ME_PM_20.7		
Title:	S5/CM3-PG to S5/CM3 via Power Button override (AC+DC, AC-only/PP2/LP3)		
Requirement:	Mandatory	Exemptions	None
Method:	Automated by Intel® PETS		
Objective:	This test checks the SUT power flow from S5/CM3-PG to S5/CM3 via Power Button override with the parameters outlined below.		
Configuration:	Intel® AMT should be provisioned via manual mode. This test assumes that either LAN-only, WLAN-only, or both LAN and WLAN network interfaces are available on the SUT.		
Parameters:	System Power Source		AC+DC or AC-only
	Power States	Initial	S5/MeOff (CM3-PG)
		Final	S5/MeOn (CM3)
		Trigger	Power Button override
	Intel® AMT	Power Package	PP2 (Intel® ME on in S0, wake in Sx/AC)
		WLAN Link Policy	LP3 (Enabled in S0, Sx/AC) where available



ID:	ME_PM_20.7
Setup:	<ol style="list-style-type: none"> 1. Set the SUT power source to AC+DC where supported; otherwise AC-only. 2. Bring the SUT to the base state of S0/MeOn (CM0,CM0-PG), and confirm that the Host OS is available. 3. Set the active power package on the SUT to Power Package 2 (Intel® ME on in S0, wake in Sx/AC). 4. Set the Intel® AMT WLAN link policy on the SUT to Link Policy 3 (Enabled in S0, Sx/AC), if the WLAN network interface is available. 5. Ensure the Intel® AMT idle timeout on the SUT is set to 1 minute. 6. Ensure that the Host OS network device drivers are configured to not wake the SUT. This includes enabling ARP and/or NS Offload features where available to help prevent unexpected host wake events. 7. Verify that Intel® AMT on the SUT responds to version queries via all available network interfaces. 8. Shutdown the SUT via the Host OS. 9. Verify that the SUT is in S5/MeOn (CM3). 10. Verify that Intel® AMT on the SUT responds to version queries via all available network interfaces. 11. Wait for 3 minutes to allow the Intel® ME on the SUT to move to CM3-PG after Intel® AMT idle timeout. 12. Verify that the Intel® ME on the SUT is in CM3-PG.
Procedure:	<ol style="list-style-type: none"> 1. Shutdown the SUT via a Power Button press for more than 5 seconds. 2. Verify that the SUT is in S5/MeOn (CM3). 3. Verify that Intel® AMT on the SUT responds to version queries via all available network interfaces.
Pass Criteria:	<p>The test passes if:</p> <ul style="list-style-type: none"> • the SUT ends the test in S5. • the Intel® CSME is in MeOn (CM3). • Intel® AMT responds to version queries via all available network interfaces. <p>Note: Some systems may briefly move electrically to S0 before final transition to S5.</p>

ID:	ME_PM_20.8		
Title:	S5/CM3 to S5/CM3 via Power Button override (AC+DC, AC-only/PP2/LP3)		
Requirement:	Mandatory	Exemptions	None
Method:	Automated by Intel® PETS		
Objective:	This test checks the SUT power flow from S5/CM3 to S5/CM3 via Power Button override with the parameters outlined below.		
Configuration:	Intel® AMT should be provisioned via manual mode. This test assumes that either LAN-only, WLAN-only, or both LAN and WLAN network interfaces are available on the SUT.		
Parameters:	System Power Source		AC+DC or AC-only
	Power States	Initial	S5/MeOn (CM3)
		Final	S5/MeOn (CM3)
		Trigger	Power Button override
	Intel® AMT	Power Package	PP2 (Intel® ME on in S0, wake in Sx/AC)
		WLAN Link Policy	LP3 (Enabled in S0, Sx/AC) where available



ID:	ME_PM_20.8
Setup:	<ol style="list-style-type: none"> 1. Set the SUT power source to AC+DC where supported; otherwise AC-only. 2. Bring the SUT to the base state of S0/MeOn (CM0,CM0-PG), and confirm that the Host OS is available. 3. Set the active power package on the SUT to Power Package 2 (Intel® ME on in S0, wake in Sx/AC). 4. Set the Intel® AMT WLAN link policy on the SUT to Link Policy 3 (Enabled in S0, Sx/AC), if the WLAN network interface is available. 5. Ensure that the Host OS network device drivers are configured to not wake the SUT. This includes enabling ARP and/or NS Offload features where available to help prevent unexpected host wake events. 6. Verify that Intel® AMT on the SUT responds to version queries via all available network interfaces. 7. Shutdown the SUT via the Host OS. 8. Verify that the SUT is in S5/MeOn (CM3). 9. Verify that Intel® AMT on the SUT responds to version queries via all available network interfaces.
Procedure:	<ol style="list-style-type: none"> 1. Shutdown the SUT via a Power Button press for more than 5 seconds. 2. Verify that the SUT is in S5/MeOn (CM3). 3. Verify that Intel® AMT on the SUT responds to version queries via all available network interfaces.
Pass Criteria:	<p>The test passes if:</p> <ul style="list-style-type: none"> • the SUT ends the test in S5. • the Intel® CSME is in MeOn (CM3). • Intel® AMT responds to version queries via all available network interfaces. <p>Note: Some systems may briefly move electrically to S0 before final transition to S5.</p>

ID:	ME_PM_20.9		
Title:	S3/CM3-PG with AC Wake to S5/CM3-PG with AC Wake via Power Button override (DC-only/PP2/LP3)		
Requirement:	Mandatory	Exemptions	<div><input checked="" type="checkbox"/> Non-Mobile (AC-only) systems</div> <div><input checked="" type="checkbox"/> Modern Standby and InstantGo* systems</div>
Method:	Automated by Intel® PETS		
Objective:	This test checks the SUT power flow from S3/CM3-PG with Ac Wake to S5/CM3-PG with AC Wake via Power Button override with the parameters outlined below.		
Configuration:	This test assumes that either LAN-only, WLAN-only, or both LAN and WLAN network interfaces are available on the SUT.		
Parameters:	System Power Source		DC-only
	Power States	Initial	S3/CM3-PG with AC Wake
		Final	S5,Deep S5,G3/CM3-PG with AC Wake
		Trigger	Power Button override
	Intel® AMT	Power Package	PP2 (Intel® ME on in S0, wake in Sx/AC)
		WLAN Link Policy	LP3 (Enabled in S0, Sx/AC) where available



ID:	ME_PM_20.9
Setup:	<ol style="list-style-type: none"> 1. Set the SUT power source to AC+DC. 2. Bring the SUT to the base state of S0/MeOn (CM0,CM0-PG), and confirm that the Host OS is available. 3. Verify that a DC battery is connected to the SUT, and that it is charged. 4. Set the SUT power source to DC-only. 5. Set the active power package on the SUT to Power Package 2 (Intel® ME on in S0, wake in Sx/AC). 6. Set the Intel® AMT WLAN link policy on the SUT to Link Policy 3 (Enabled in S0, Sx/AC), if the WLAN network interface is available. 7. Ensure that the Host OS network device drivers are configured to not wake the SUT. This includes enabling ARP and/or NS Offload features where available to help prevent unexpected host wake events. Most especially, ensure that the Host OS Wireless Wake on LAN driver setting on the SUT is disabled, if the WLAN network interface is available. 8. Ensure that Intel® RMT is disabled, if running on an All-in-One (AIO) SUT with feature support. 9. Verify that Intel® AMT on the SUT responds to version queries via all available network interfaces. 10. Suspend the SUT via the Host OS. 11. Verify that the SUT is in S3/(CM3-PG) with AC Wake.
Procedure:	<ol style="list-style-type: none"> 1. Shutdown the SUT via a Power Button press for more than 5 seconds. 2. Verify that the SUT is in S5, Deep S5, G3/CM3-PG with AC Wake
Pass Criteria:	<p>The test passes if the SUT moves to S5 (or Deep S5 or G3), and the Intel® CSME is in CM3-PG.</p> <p>Note: Some systems may briefly move electrically to S0 before final transition to S5 (or Deep S5 or G3).</p>

ID:	ME_PM_20.10	
Title:	S4/CM3-PG with AC Wake to S5/CM3-PG with AC Wake via Power Button override (DC-only/PP2/LP3)	
Requirement:	Mandatory	Exemptions <input checked="" type="checkbox"/> Non-Mobile (AC-only) systems
Method:	Automated by Intel® PETS	
Objective:	This test checks the SUT power flow from S4/CM3-PG with AC Wake to S5/CM3-PG with AC Wake via Power Button override with the parameters outlined below.	
Configuration:	Intel® AMT should be provisioned via manual mode. If Deep S4, Deep S5, and/or G3 are supported on the SUT, please confirm the following: <ul style="list-style-type: none">the SUT and/or BIOS are properly configured to permit Deep S4/S5 or G3 entry.the correct Deep Sx policy is applied to the SUT profile in Intel® PETS. This test assumes that either LAN-only, WLAN-only, or both LAN and WLAN network interfaces are available on the SUT.	
Parameters:	System Power Source DC-only	
	Power States	Initial S4,S5,Deep S4,Deep S5,G3/CM3-PG with AC Wake
		Final S5,Deep S5,G3/CM3-PG with AC Wake
		Trigger Power Button override
	Intel® AMT	Power Package PP2 (Intel® ME on in S0, wake in Sx/AC)
		WLAN Link Policy LP3 (Enabled in S0, Sx/AC) where available



ID:	ME_PM_20.10
Setup:	<ol style="list-style-type: none"> 1. Set the SUT power source to AC+DC. 2. Bring the SUT to the base state of S0/MeOn (CM0,CM0-PG), and confirm that the Host OS is available. 3. Verify that a DC battery is connected to the SUT, and that it is charged. 4. Set the SUT power source to DC-only. 5. Set the active power package on the SUT to Power Package 2 (Intel® ME on in S0, wake in Sx/AC). 6. Set the Intel® AMT WLAN link policy on the SUT to Link Policy 3 (Enabled in S0, Sx/AC), if the WLAN network interface is available. 7. Ensure that the Host OS network device drivers are configured to not wake the SUT. This includes enabling ARP and/or NS Offload features where available to help prevent unexpected host wake events. 8. Verify that Intel® AMT on the SUT responds to version queries via all available network interfaces. 9. Hibernate the SUT via the Host OS. 10. Verify that the SUT is in S4, S5, Deep S4, Deep S5, G3/CM3-PG.with AC Wake
Procedure:	<ol style="list-style-type: none"> 1. Shutdown the SUT via a Power Button press for more than 5 seconds. 2. Verify that the SUT is in S5, Deep S5, G3/CM3-PG.with AC Wake
Pass Criteria:	<p>The test passes if the SUT moves to, if not already there, S5 (or Deep S5 or G3), and the Intel® CSME is in CM3-PG.</p> <p>Note: Some systems may briefly move electrically to S0 before final transition to S5 (or Deep S5 or G3).</p>

ID:	ME_PM_20.11	
Title:	S5/CM3-PG with AC Wake to S5/CM3-PG with AC Wake via Power Button override (DC-only/PP2/LP3)	
Requirement:	Mandatory	Exemptions <input checked="" type="checkbox"/> Non-Mobile (AC-only) systems
Method:	Automated by Intel® PETS	
Objective:	This test checks the SUT power flow from S5/CM3-PG to S5/CM3-PG via Power Button override with the parameters outlined below.	
Configuration:	<p>Intel® AMT should be provisioned via manual mode.</p> <p>If Deep S5 and/or G3 are supported on the SUT, please confirm the following:</p> <ul style="list-style-type: none"> • the SUT and/or BIOS are properly configured to permit Deep S5 or G3 entry. • the correct Deep Sx policy is applied to the SUT profile in Intel® PETS. <p>This test assumes that either LAN-only, WLAN-only, or both LAN and WLAN network interfaces are available on the SUT.</p>	
Parameters:	System Power Source DC-only	
	Power States	Initial S5, Deep S5, G3/MeOff (CM-Off)
		Final S5, Deep S5, G3/MeOff (CM-Off)
		Trigger Power Button override
	Intel® AMT	Power Package PP2 (Intel® ME on in S0, wake in Sx/AC)
		WLAN Link Policy LP3 (Enabled in S0, Sx/AC) where available
Setup:	<ol style="list-style-type: none"> 1. Set the SUT power source to AC+DC. 2. Bring the SUT to the base state of S0/MeOn (CM0,CM0-PG), and confirm that the Host OS is available. 3. Verify that a DC battery is connected to the SUT, and that it is charged. 4. Set the SUT power source to DC-only. 5. Set the active power package on the SUT to Power Package 2 (Intel® ME on in S0, wake in Sx/AC). 6. Set the Intel® AMT WLAN link policy on the SUT to Link Policy 3 (Enabled in S0, Sx/AC), if the WLAN network interface is available. 7. Ensure that the Host OS network device drivers are configured to not wake the SUT. This includes enabling ARP and/or NS Offload features where available to help prevent unexpected host wake events. 8. Verify that Intel® AMT on the SUT responds to version queries via all available network interfaces. 9. Shutdown the SUT via the Host OS. 10. Verify that the SUT is in S5, Deep S5, G3/CM3-PG. 	



ID:	ME_PM_20.11
Procedure:	<ol style="list-style-type: none"> 1. Shutdown the SUT via a Power Button press for more than 5 seconds. 2. Verify that the SUT is in S5, Deep S5, G3/CM3-PG.
Pass Criteria:	<p>The test passes if the SUT ends the test in S5 (or Deep S5 or G3), and the Intel® CSME is in MeOff (CM-Off).</p> <p>Note: Some systems may briefly move electrically to S0 before final transition to S5 (or Deep S5 or G3).</p>

ID:	ME_PM_20.21	
Title:	S0/CM0 to S5/CM3 via Power Button override (AC+DC, AC-only/PP2/LP2)	
Requirement:	Mandatory	Exemptions <input checked="" type="checkbox"/> Systems with a LAN-only network interface
Method:	Automated by Intel® PETS	
Objective:	This test checks the SUT power flow from S0/CM0 to S5/CM3 via Power Button override with the parameters outlined below.	
Configuration:	<p>Intel® AMT should be provisioned via manual mode.</p> <p>This test assumes that either WLAN-only, or both LAN and WLAN network interfaces are available on the SUT.</p>	
Parameters:	System Power Source	
	Power States	Initial S0/MeOn (CM0, CM0-PG)
		Final S5/MeOn (CM3)
		Trigger Power Button override
	Intel® AMT	Power Package PP2 (Intel® ME on in S0, wake in Sx/AC)
		WLAN Link Policy LP2 (Enabled in S0)
Setup:	<ol style="list-style-type: none"> 1. Set the SUT power source to AC+DC where supported; otherwise AC-only. 2. Bring the SUT to the base state of S0/MeOn (CM0,CM0-PG), and confirm that the Host OS is available. 3. Set the active power package on the SUT to Power Package 2 (Intel® ME on in S0, wake in Sx/AC). 4. Set the Intel® AMT WLAN link policy on the SUT to Link Policy 2 (Enabled in S0). 5. Ensure that the Host OS network device drivers are configured to not wake the SUT. This includes enabling ARP and/or NS Offload features where available to help prevent unexpected host wake events. 6. Verify that Intel® AMT on the SUT responds to version queries via all available network interfaces. 	
Procedure:	<ol style="list-style-type: none"> 1. Shutdown the SUT via a Power Button press for more than 5 seconds. 2. Verify that the SUT is in S5/MeOn (CM3). 3. Verify that Intel® AMT on the SUT responds to version query via the LAN network interface, if available. 4. Verify that Intel® AMT on the SUT does not respond to version query via the WLAN network interface. 	
Pass Criteria:	<p>The test passes if:</p> <ul style="list-style-type: none"> • the SUT moves to S5. • the Intel® CSME is in MeOn (CM3). • when in S5: <ul style="list-style-type: none"> — Intel® AMT on the SUT does respond to version queries via the LAN network interface, if available. — Intel® AMT on the SUT does not respond to version queries via the WLAN network interface. <p>Note: Some systems may briefly move electrically to S0 before final transition to S5.</p>	

ID:	ME_PM_20.22	
Title:	S3/CM3 to S5/CM3 via Power Button override (AC+DC, AC-only/PP2/LP2)	
Requirement:	Mandatory	Exemptions <input checked="" type="checkbox"/> Modern Standby and InstantGo* systems <input checked="" type="checkbox"/> Systems with a LAN-only network interface



ID:	ME_PM_20.22	
Method:	Automated by Intel® PETS	
Objective:	This test checks the SUT power flow from S3/CM3 to S5/CM3 via Power Button override with the parameters outlined below.	
Configuration:	Intel® AMT should be provisioned via manual mode. This test assumes that either WLAN-only, or both LAN and WLAN network interfaces are available on the SUT.	
Parameters:	System Power Source AC+DC or AC-only	
	Power States	Initial S3/MeOn (CM3)
		Final S5/MeOn (CM3)
		Trigger Power Button override
	Intel® AMT	Power Package PP2 (Intel® ME on in S0, wake in Sx/AC)
		WLAN Link Policy LP2 (Enabled in S0)
Setup:	<ol style="list-style-type: none"> Set the SUT power source to AC+DC where supported; otherwise AC-only. Bring the SUT to the base state of S0/MeOn (CM0,CM0-PG), and confirm that the Host OS is available. Set the active power package on the SUT to Power Package 2 (Intel® ME on in S0, wake in Sx/AC). Set the Intel® AMT WLAN link policy on the SUT to Link Policy 2 (Enabled in S0). Ensure that the Host OS network device drivers are configured to not wake the SUT. This includes enabling ARP and/or NS Offload features where available to help prevent unexpected host wake events. Most especially, ensure that the Host OS Wireless Wake on LAN driver setting on the SUT is disabled. Ensure that Intel® RMT is disabled, if running on a Desktop or All-in-One (AIO) SUT with feature support. Verify that Intel® AMT on the SUT responds to version queries via all available network interfaces. Suspend the SUT via the Host OS. Verify that the SUT is in S3/MeOn (CM3). Verify that Intel® AMT on the SUT responds to version query via the LAN network interface, if available. Verify that Intel® AMT on the SUT does not respond to version query via the WLAN network interface. 	
Procedure:	<ol style="list-style-type: none"> Shutdown the SUT via a Power Button press for more than 5 seconds. Verify that the SUT is in S5/MeOn (CM3). Verify that Intel® AMT on the SUT responds to version query via the LAN network interface, if available. 	
Pass Criteria:	<p>The test passes if:</p> <ul style="list-style-type: none"> the SUT moves to S5. the Intel® CSME is in MeOn (CM3). when in S5: <ul style="list-style-type: none"> Intel® AMT on the SUT does respond to version queries via the LAN network interface, if available. Intel® AMT on the SUT does not respond to version queries via the WLAN network interface. <p>Note: Some systems may briefly move electrically to S0 before final transition to S5.</p>	

ID:	ME_PM_20.23	
Title:	S3/CM3-PG to S5/CM3 via Power Button override (AC+DC, AC-only/PP2/LP2)	
Requirement:	Mandatory	Exemptions <ul style="list-style-type: none"> <input checked="" type="checkbox"/> Modern Standby and InstantGo* systems <input checked="" type="checkbox"/> Systems with a LAN-only network interface
Method:	Automated by Intel® PETS	
Objective:	This test checks the SUT power flow from S3/CM3-PG to S5/CM3 via Power Button override with the parameters outlined below.	
Configuration:	Intel® AMT should be provisioned via manual mode. This test assumes that either WLAN-only, or both LAN and WLAN network interfaces are available on the SUT.	



ID:	ME_PM_20.23	
Parameters:	System Power Source	AC+DC or AC-only
	Power States	Initial S3/MeOn (CM3)
		Final S5/MeOn (CM3)
		Trigger Power Button override
	Intel® AMT	Power Package PP2 (Intel® ME on in S0, wake in Sx/AC)
		WLAN Link Policy LP2 (Enabled in S0)
Setup:	<ol style="list-style-type: none"> 1. Set the SUT power source to AC+DC where supported; otherwise AC-only. 2. Bring the SUT to the base state of S0/MeOn (CM0,CM0-PG), and confirm that the Host OS is available. 3. Set the active power package on the SUT to Power Package 2 (Intel® ME on in S0, wake in Sx/AC). 4. Set the Intel® AMT WLAN link policy on the SUT to Link Policy 2 (Enabled in S0). 5. Ensure the Intel® AMT idle timeout on the SUT is set to 1 minute. 6. Ensure that the Host OS network device drivers are configured to not wake the SUT. This includes enabling ARP and/or NS Offload features where available to help prevent unexpected host wake events. Most especially, ensure that the Host OS Wireless Wake on LAN driver setting on the SUT is disabled. 7. Ensure that Intel® RMT is disabled, if running on a Desktop or All-in-One (AIO) SUT with feature support. 8. Verify that Intel® AMT on the SUT responds to version queries via all available network interfaces. 9. Suspend the SUT via the Host OS. 10. Verify that the SUT is in S3/MeOn (CM3). 11. Verify that Intel® AMT on the SUT responds to version query via the LAN network interface, if available. 12. Verify that Intel® AMT on the SUT does not respond to version query via the WLAN network interface. 13. Wait for 3 minutes to allow the Intel® ME on the SUT to move to CM3-PG after Intel® AMT idle timeout. 14. Verify that the Intel® ME on the SUT is in CM3-PG. 	
Procedure:	<ol style="list-style-type: none"> 1. Shutdown the SUT via a Power Button press for more than 5 seconds. 2. Verify that the SUT is in S5/MeOn (CM3). 3. Verify that Intel® AMT on the SUT responds to version query via the LAN network interface. 	
Pass Criteria:	<p>The test passes if:</p> <ul style="list-style-type: none"> • the SUT moves to S5. • the Intel® CSME is in MeOn (CM3). • when in S5: <ul style="list-style-type: none"> — Intel® AMT on the SUT does respond to version queries via the LAN network interface, if available. — Intel® AMT on the SUT does not respond to version queries via the WLAN network interface. <p>Note: Some systems may briefly move electrically to S0 before final transition to S5.</p>	

ID:	ME_PM_20.24
Title:	S4/CM3 to S5/CM3 via Power Button override (AC+DC, AC-only/PP2/LP2)
Requirement:	Mandatory Exemptions <input checked="" type="checkbox"/> Systems with a LAN-only network interface
Method:	Automated by Intel® PETS
Objective:	This test checks the SUT power flow from S4/CM3 to S5/CM3 via Power Button override with the parameters outlined below.
Configuration:	Intel® AMT should be provisioned via manual mode. This test assumes that either WLAN-only, or both LAN and WLAN network interfaces are available on the SUT.



ID:	ME_PM_20.24	
Parameters:	System Power Source	AC+DC or AC-only
	Power States	Initial S4,S5/MeOn (CM3)
		Final S5/MeOn (CM3)
		Trigger Power Button override
	Intel® AMT	Power Package PP2 (Intel® ME on in S0, wake in Sx/AC)
		WLAN Link Policy LP2 (Enabled in S0)
Setup:	<ol style="list-style-type: none"> 1. Set the SUT power source to AC+DC where supported; otherwise AC-only. 2. Bring the SUT to the base state of S0/MeOn (CM0,CM0-PG), and confirm that the Host OS is available. 3. Set the active power package on the SUT to Power Package 2 (Intel® ME on in S0, wake in Sx/AC). 4. Set the Intel® AMT WLAN link policy on the SUT to Link Policy 2 (Enabled in S0). 5. Ensure that the Host OS network device drivers are configured to not wake the SUT. This includes enabling ARP and/or NS Offload features where available to help prevent unexpected host wake events. 6. Verify that Intel® AMT on the SUT responds to version queries via all available network interfaces. 7. Hibernate the SUT via the Host OS. 8. Verify that the SUT is in S4, S5/MeOn (CM3). 9. Verify that Intel® AMT on the SUT responds to version query via the LAN network interface, if available. 10. Verify that Intel® AMT on the SUT does not respond to version query via the WLAN network interface. 	
Procedure:	<ol style="list-style-type: none"> 1. Shutdown the SUT via a Power Button press for more than 5 seconds. 2. Verify that the SUT is in S5/MeOn (CM3). 3. Verify that Intel® AMT on the SUT responds to version query via the LAN network interface. 4. Verify that Intel® AMT on the SUT does not respond to version query via the WLAN network interface. 	
Pass Criteria:	<p>The test passes if:</p> <ul style="list-style-type: none"> • the SUT moves to S5. • the Intel® CSME is in MeOn (CM3). • Intel® AMT responds to version queries via LAN network interfaces. <p>Note: Some systems may briefly move electrically to S0 before final transition to S5.</p>	

ID:	ME_PM_20.25	
Title:	S4/CM3-PG to S5/CM3 via Power Button override (AC+DC, AC-only/PP2/LP2)	
Requirement:	Mandatory	Exemptions <input checked="" type="checkbox"/> Systems with a LAN-only network interface
Method:	Automated by Intel® PETS	
Objective:	This test checks the SUT power flow from S4/CM3-PG to S5/CM3 via Power Button override with the parameters outlined below.	
Configuration:	<p>Intel® AMT should be provisioned via manual mode.</p> <p>This test assumes that either WLAN-only, or both LAN and WLAN network interfaces are available on the SUT.</p>	
Parameters:	System Power Source	AC+DC or AC-only
	Power States	Initial S4,S5/MeOff (CM3-PG)
		Final S5/MeOn (CM3)
		Trigger Power Button override
	Intel® AMT	Power Package PP2 (Intel® ME on in S0, wake in Sx/AC)
		WLAN Link Policy LP2 (Enabled in S0)



ID:	ME_PM_20.25
Setup:	<ol style="list-style-type: none"> 1. Set the SUT power source to AC+DC where supported; otherwise AC-only. 2. Bring the SUT to the base state of S0/MeOn (CM0,CM0-PG), and confirm that the Host OS is available. 3. Set the active power package on the SUT to Power Package 2 (Intel® ME on in S0, wake in Sx/AC). 4. Set the Intel® AMT WLAN link policy on the SUT to Link Policy 2 (Enabled in S0). 5. Ensure the Intel® AMT idle timeout on the SUT is set to 1 minute. 6. Ensure that the Host OS network device drivers are configured to not wake the SUT. This includes enabling ARP and/or NS Offload features where available to help prevent unexpected host wake events. 7. Verify that Intel® AMT on the SUT responds to version queries via all available network interfaces. 8. Hibernate the SUT via the Host OS. 9. Verify that the SUT is in S4, S5/MeOn (CM3). 10. Verify that Intel® AMT on the SUT responds to version query via the LAN network interface, if available. 11. Verify that Intel® AMT on the SUT does not respond to version query via the WLAN network interface. 12. Wait for 3 minutes to allow the Intel® ME on the SUT to move to CM3-PG after Intel® AMT idle timeout. 13. Verify that the Intel® ME on the SUT is in CM3-PG.
Procedure:	<ol style="list-style-type: none"> 1. Shutdown the SUT via a Power Button press for more than 5 seconds. 2. Verify that the SUT is in S5/MeOn (CM3). 3. Verify that Intel® AMT on the SUT responds to version query via the LAN network interface. 4. Verify that Intel® AMT on the SUT does not respond to version query via the WLAN network interface.
Pass Criteria:	<p>The test passes if:</p> <ul style="list-style-type: none"> • the SUT moves to S5. • the Intel® CSME is in MeOn (CM3). • Intel® AMT responds to version queries via LAN network interfaces. <p>Note: Some systems may briefly move electrically to S0 before final transition to S5.</p>

ID:	ME_PM_20.26		
Title:	S5/CM3-PG to S5/CM3 via Power Button override (AC+DC, AC-only/PP2/LP2)		
Requirement:	Mandatory	Exemptions	<input checked="" type="checkbox"/> Systems with a LAN-only network interface
Method:	Automated by Intel® PETS		
Objective:	This test checks the SUT power flow from S5/CM3-PG to S5/CM3 via Power Button override with the parameters outlined below.		
Configuration:	<p>Intel® AMT should be provisioned via manual mode.</p> <p>This test assumes that either WLAN-only, or both LAN and WLAN network interfaces are available on the SUT.</p>		
Parameters:	System Power Source		AC+DC or AC-only
	Power States	Initial	S5/MeOff (CM3-PG)
		Final	S5/MeOn (CM3)
		Trigger	Power Button override
	Intel® AMT	Power Package	PP2 (Intel® ME on in S0, wake in Sx/AC)
		WLAN Link Policy	LP2 (Enabled in S0)



ID:	ME_PM_20.26
Setup:	<ol style="list-style-type: none"> 1. Set the SUT power source to AC+DC where supported; otherwise AC-only. 2. Bring the SUT to the base state of S0/MeOn (CM0,CM0-PG), and confirm that the Host OS is available. 3. Set the active power package on the SUT to Power Package 2 (Intel® ME on in S0, wake in Sx/AC). 4. Set the Intel® AMT WLAN link policy on the SUT to Link Policy 2 (Enabled in S0). 5. Ensure the Intel® AMT idle timeout on the SUT is set to 1 minute. 6. Ensure that the Host OS network device drivers are configured to not wake the SUT. This includes enabling ARP and/or NS Offload features where available to help prevent unexpected host wake events. 7. Verify that Intel® AMT on the SUT responds to version queries via all available network interfaces. 8. Shutdown the SUT via the Host OS. 9. Verify that the SUT is in S5/MeOn (CM3). 10. Verify that Intel® AMT on the SUT responds to version query via the LAN network interface, if available. 11. Verify that Intel® AMT on the SUT does not respond to version query via the WLAN network interface. 12. Wait for 3 minutes to allow the Intel® ME on the SUT to move to CM3-PG after Intel® AMT idle timeout. 13. Verify that the Intel® ME on the SUT is in CM3-PG.
Procedure:	<ol style="list-style-type: none"> 1. Shutdown the SUT via a Power Button press for more than 5 seconds. 2. Verify that the SUT is in S5/MeOn (CM3). 3. Verify that Intel® AMT on the SUT responds to version query via the LAN network interface.
Pass Criteria:	<p>The test passes if:</p> <ul style="list-style-type: none"> • the SUT moves to S5. • the Intel® CSME is in MeOn (CM3). • Intel® AMT responds to version queries via all available network interfaces. <p>Note: Some systems may briefly move electrically to S0 before final transition to S5.</p>

ID:	ME_PM_20.27		
Title:	S5/CM3 to S5/CM3 via Power Button override (AC+DC, AC-only/PP2/LP2)		
Requirement:	Mandatory	Exemptions	<input checked="" type="checkbox"/> Systems with a LAN-only network interface
Method:	Automated by Intel® PETS		
Objective:	This test checks the SUT power flow from S5/CM3 to S5/CM3 via Power Button override with the parameters outlined below.		
Configuration:	<p>Intel® AMT should be provisioned via manual mode.</p> <p>This test assumes that either WLAN-only, or both LAN and WLAN network interfaces are available on the SUT.</p>		
Parameters:	System Power Source		AC+DC or AC-only
	Power States	Initial	S5/MeOn (CM3)
		Final	S5/MeOn (CM3)
		Trigger	Power Button override
	Intel® AMT	Power Package	PP2 (Intel® ME on in S0, wake in Sx/AC)
		WLAN Link Policy	LP2 (Enabled in S0)



ID:	ME_PM_20.27
Setup:	<ol style="list-style-type: none"> 1. Set the SUT power source to AC+DC where supported; otherwise AC-only. 2. Bring the SUT to the base state of S0/MeOn (CM0,CM0-PG), and confirm that the Host OS is available. 3. Set the active power package on the SUT to Power Package 2 (Intel® ME on in S0, wake in Sx/AC). 4. Set the Intel® AMT WLAN link policy on the SUT to Link Policy 2 (Enabled in S0). 5. Ensure that the Host OS network device drivers are configured to not wake the SUT. This includes enabling ARP and/or NS Offload features where available to help prevent unexpected host wake events. 6. Verify that Intel® AMT on the SUT responds to version queries via all available network interfaces. 7. Shutdown the SUT via the Host OS. 8. Verify that the SUT is in S5/MeOn (CM3). 9. Verify that Intel® AMT on the SUT responds to version query via the LAN network interface, if available. 10. Verify that Intel® AMT on the SUT does not respond to version query via the WLAN network interface.
Procedure:	<ol style="list-style-type: none"> 1. Shutdown the SUT via a Power Button press for more than 5 seconds. 2. Verify that the SUT is in S5/MeOn (CM3). 3. Verify that Intel® AMT on the SUT responds to version query via the LAN network interface.
Pass Criteria:	<p>The test passes if:</p> <ul style="list-style-type: none"> • the SUT moves to S5. • the Intel® CSME is in MeOn (CM3). • Intel® AMT responds to version queries via all available network interfaces. <p>Note: Some systems may briefly move electrically to S0 before final transition to S5.</p>

ID:	ME_PM_20.28		
Title:	S0/CM0 to G3/CM-Off via Power loss (DC-only/PP2/LP3)		
Requirement:	Mandatory	Exemptions	<input checked="" type="checkbox"/> Non-Mobile (AC-only) systems
Method:	Automated by Intel® PETS		
Objective:	This test checks the SUT power flow from S0/CM0 to G3/CM-Off via Power loss with the parameters outlined below.		
Configuration:	Intel® AMT should be provisioned via manual mode. If Deep S5 and/or G3 are supported on the SUT, please confirm the following: <ul style="list-style-type: none">the SUT and/or BIOS are properly configured to permit Deep S5 or G3 entry.the correct Deep Sx policy is applied to the SUT profile in Intel® PETS. This test assumes that either LAN-only, WLAN-only, or both LAN and WLAN network interfaces are available on the SUT.		
Parameters:	System Power Source		DC-only
	Power States	Initial	S0/MeOn (CM0, CM0-PG)
		Final	S5, Deep S5, G3/MeOff (CM-Off)
		Trigger	Power loss
	Intel® AMT	Power Package	PP2 (Intel® ME on in S0, wake in Sx/AC)
WLAN Link Policy		LP3 (Enabled in S0, Sx/AC) where available	
Setup:	<ol style="list-style-type: none">Set the SUT power source to AC+DC.Bring the SUT to the base state of S0/MeOn (CM0,CM0-PG), and confirm that the Host OS is available.Verify that a DC battery is connected to the SUT, and that it is charged.Set the SUT power source to DC-only.Set the active power package on the SUT to Power Package 2 (Intel® ME on in S0, wake in Sx/AC).Set the Intel® AMT WLAN link policy on the SUT to Link Policy 3 (Enabled in S0, Sx/AC), if the WLAN network interface is available.Ensure that the Host OS network device drivers are configured to not wake the SUT. This includes enabling ARP and/or NS Offload features where available to help prevent unexpected host wake events.Verify that Intel® AMT on the SUT responds to version queries via all available network interfaces.		



ID:	ME_PM_20.28
Procedure:	1. Put the system to S5/ G3 via Unconditional Power Loss. 2. Verify that the SUT is in S5, Deep S5, G3/MeOff (CM-Off).
Pass Criteria:	The test passes if the SUT moves to S5 (or Deep S5 or G3) on unconditional Power Loss, and the Intel® CSME moves to MeOff (CM-Off).

12.24 ME_PM_21: S3/CM-Off (with/Intel® ME Wake) to S3/CM-Off (Without Intel® ME Wake)

ID:	ME_PM_21.1		
Title:	S3/CM3-PG with AC Wake to S3/CM3-PG with AC Wake via Intel® AMT idle timeout (DC-only/PP2/LP3)		
Requirement:	Mandatory	Exemptions	<input checked="" type="checkbox"/> Non-Mobile (AC-only) systems <input checked="" type="checkbox"/> Modern Standby and InstantGo* systems
Method:	Automated by Intel® PETS		
Objective:	This test checks the SUT power flow from S3/CM3-PG to S3/CM-Off via Intel® AMT idle timeout with the parameters outlined below.		
Configuration:	This test assumes that either LAN-only, WLAN-only, or both LAN and WLAN network interfaces are available on the SUT.		
Parameters:	System Power Source		DC-only
	Power States	Initial	S3/CM3-PG
		Final	S3/CM3-PG
		Trigger	(AC-attach then) Intel® AMT idle timeout
	Intel® AMT	Power Package	PP2 (Intel® ME on in S0, wake in Sx/AC)
		WLAN Link Policy	LP3 (Enabled in S0, Sx/AC) where available
Setup:	<ol style="list-style-type: none"> Set the SUT power source to AC+DC. Bring the SUT to the base state of S0/MeOn (CM0,CM0-PG), and confirm that the Host OS is available. Verify that a DC battery is connected to the SUT, and that it is charged. Set the SUT power source to DC-only. Set the active power package on the SUT to Power Package 2 (Intel® ME on in S0, wake in Sx/AC). Set the Intel® AMT WLAN link policy on the SUT to Link Policy 3 (Enabled in S0, Sx/AC), if the WLAN network interface is available. Ensure the Intel® AMT idle timeout on the SUT is set to 1 minute. Ensure that the Host OS network device drivers are configured to not wake the SUT. This includes enabling ARP and/or NS Offload features where available to help prevent unexpected host wake events. Most especially, ensure that the Host OS Wireless Wake on LAN driver setting on the SUT is disabled, if the WLAN network interface is available. Ensure that Intel® RMT is disabled, if running on an All-in-One (AIO) SUT with feature support. Verify that Intel® AMT on the SUT responds to version queries via all available network interfaces. Suspend the SUT via the Host OS. Verify that the SUT is in S3/(CM3-PG) with AC Wake 		
Procedure:	<ol style="list-style-type: none"> Set the SUT power source to AC+DC. Verify that Intel® AMT on the SUT responds to version queries via all available network interfaces. Verify that the SUT is in S3/MeOn (CM3). Wait for 3 minutes to allow the Intel® ME on the SUT to move to CM3-PG after Intel® AMT idle timeout. Verify that the SUT is in S3/CM3-PG. 		
Pass Criteria:	The test passes if: <ul style="list-style-type: none"> the SUT remains in S3. when in S3/MeOn (CM3), Intel® AMT responds to version queries via all available network interfaces. the Intel® CSME ends the test in MeOff (CM3-PG). 		



12.25 ME_PM_22: S3/CM3-PG (with/ Intel® ME Wake) to S3/CM-Off (Without Intel® ME Wake)

ID:	ME_PM_22.1		
Title:	S3/CM3-PG to S3/CM3-PG with AC Wake via AC-detach (AC+DC/PP2/LP3)		
Requirement:	Mandatory	Exemptions	<input checked="" type="checkbox"/> Non-Mobile (AC-only) systems
			<input checked="" type="checkbox"/> Modern Standby and InstantGo* systems
Method:	Automated by Intel® PETS		
Objective:	This test checks the SUT power flow from S3/CM3-PG to S3/CM-Off via AC-detach with the parameters outlined below.		
Configuration:	This test assumes that either LAN-only, WLAN-only, or both LAN and WLAN network interfaces are available on the SUT.		
Parameters:	System Power Source		AC+DC
	Power States	Initial	S3/CM3-PG
		Final	S3/MeOff (CM-Off)
		Trigger	(Intel® AMT idle timeout then) AC-detach
	Intel® AMT	Power Package	PP2 (Intel® ME on in S0, wake in Sx/AC)
		WLAN Link Policy	LP3 (Enabled in S0, Sx/AC) where available
Setup:	1. Set the SUT power source to AC+DC .		
	2. Bring the SUT to the base state of S0/MeOn (CM0,CM0-PG), and confirm that the Host OS is available.		
	3. Verify that a DC battery is connected to the SUT, and that it is charged.		
	4. Set the active power package on the SUT to Power Package 2 (Intel® ME on in S0, wake in Sx/AC).		
	5. Set the Intel® AMT WLAN link policy on the SUT to Link Policy 3 (Enabled in S0, Sx/AC), if the WLAN network interface is available.		
	6. Ensure the Intel® AMT idle timeout on the SUT is set to 1 minute .		
	7. Ensure that the Host OS network device drivers are configured to not wake the SUT. This includes enabling ARP and/or NS Offload features where available to help prevent unexpected host wake events. Most especially, ensure that the Host OS Wireless Wake on LAN driver setting on the SUT is disabled , if the WLAN network interface is available.		
	8. Ensure that Intel® RMT is disabled , if running on an All-in-One (AIO) SUT with feature support.		
	9. Verify that Intel® AMT on the SUT responds to version queries via all available network interfaces.		
	10. Suspend the SUT via the Host OS.		
	11. Verify that the SUT is in S3/MeOn (CM3).		
	12. Verify that Intel® AMT on the SUT responds to version queries via all available network interfaces.		
	13. Wait for 3 minutes to allow the Intel® ME on the SUT to move to CM3-PG after Intel® AMT idle timeout.		
	14. Verify that the Intel® ME on the SUT is in CM3-PG.		
Procedure:	1. Set the SUT power source to DC-only.		
	2. Verify that the SUT is in S3/(CM3-PG) with AC Wake.		
	3. Verify that Intel® AMT on the SUT does not respond to version queries via any of the available network interfaces.		
Pass Criteria:	The test passes if:		
	<ul style="list-style-type: none">the SUT remains in S3.Intel® AMT does not respond to version queries via any available network interface.the Intel® CSME ends the test in MeOff (CM-Off).		



12.26 ME_PM_23: G3 or S4-S5/CM-Off (Without Intel® ME Wake) to S4-S5/CM-Off (with Intel® ME Wake)

ID:	ME_PM_23.1		
Title:	S4/CM3-PG with AC Wake to S4/CM3-PG with AC Wake via Intel® AMT idle timeout (DC-only/PP2/LP3)		
Requirement:	Mandatory	Exemptions	<input checked="" type="checkbox"/> Non-Mobile (AC-only) systems
Method:	Automated by Intel® PETS		
Objective:	This test checks the SUT power flow from S4/CM3-PG to S4/CM3-PG via Intel® AMT idle timeout with the parameters outlined below.		
Configuration:	<p>Intel® AMT should be provisioned via manual mode.</p> <p>If Deep S4, Deep S5, and/or G3 are supported on the SUT, please confirm the following:</p> <ul style="list-style-type: none"> the SUT and/or BIOS are properly configured to permit Deep S4/S5 or G3 entry. the correct Deep Sx policy is applied to the SUT profile in Intel® PETS. <p>This test assumes that either LAN-only, WLAN-only, or both LAN and WLAN network interfaces are available on the SUT.</p>		
Parameters:	System Power Source		DC-only
	Power States	Initial	S4, S5, Deep S4, Deep S5, G3/MeOff (CM-Off)
		Final	S4,S5/MeOff (CM3-PG)
		Trigger	(AC-attach then) Intel® AMT idle timeout
	Intel® AMT	Power Package	PP2 (Intel® ME on in S0, wake in Sx/AC)
		WLAN Link Policy	LP3 (Enabled in S0, Sx/AC) where available
Setup:	<ol style="list-style-type: none"> Set the SUT power source to AC+DC. Bring the SUT to the base state of S0/MeOn (CM0,CM0-PG), and confirm that the Host OS is available. Verify that a DC battery is connected to the SUT, and that it is charged. Set the SUT power source to DC-only. Set the active power package on the SUT to Power Package 2 (Intel® ME on in S0, wake in Sx/AC). Set the Intel® AMT WLAN link policy on the SUT to Link Policy 3 (Enabled in S0, Sx/AC), if the WLAN network interface is available. Ensure the Intel® AMT idle timeout on the SUT is set to 1 minute. Ensure that the Host OS network device drivers are configured to not wake the SUT. This includes enabling ARP and/or NS Offload features where available to help prevent unexpected host wake events. Verify that Intel® AMT on the SUT responds to version queries via all available network interfaces. Hibernate the SUT via the Host OS. Verify that the SUT is in S4, S5, Deep S4, Deep S5, G3/MeOff (CM-Off). 		
Procedure:	<ol style="list-style-type: none"> Set the SUT power source to AC+DC. Verify that Intel® AMT on the SUT responds to version queries via all available network interfaces. Verify that the SUT is in S4, S5/MeOn (CM3). Wait for 3 minutes to allow the Intel® ME on the SUT to move to CM3-PG after Intel® AMT idle timeout. Verify that the SUT is in S4, S5/CM3-PG. 		
Pass Criteria:	<p>The test passes if:</p> <ul style="list-style-type: none"> the SUT remains in S4 or S5 (or moves to S4 or S5 from Deep S4, Deep S5, or G3). when in S4,S5/MeOn (CM3), Intel® AMT responds to version queries via all available network interfaces. the Intel® CSME ends the test in MeOff (CM3-PG). 		

ID:	ME_PM_23.2
Title:	S5/CM3-PG to S5/CM3-PG via Intel® AMT idle timeout (AC+DC-only/PP2/LP3)



ID:	ME_PM_23.2	
Requirement:	Mandatory	Exemptions <input checked="" type="checkbox"/> Non-Mobile (AC-only) systems
Method:	Automated by Intel® PETS	
Objective:	This test checks the SUT power flow from S5/CM3-PG to S5/CM3-PG via Intel® AMT idle timeout with the parameters outlined below.	
Configuration:	<p>Intel® AMT should be provisioned via manual mode.</p> <p>If Deep S5 and/or G3 are supported on the SUT, please confirm the following:</p> <ul style="list-style-type: none"> the SUT and/or BIOS are properly configured to permit Deep S5 or G3 entry. the correct Deep Sx policy is applied to the SUT profile in Intel® PETS. <p>This test assumes that either LAN-only, WLAN-only, or both LAN and WLAN network interfaces are available on the SUT.</p>	
Parameters:	System Power Source AC+DC	
	Power States	Initial S5, Deep S5, G3/MeOff (CM-Off)
		Final S5/MeOff (CM3-PG)
		Trigger (AC-attach then) Intel® AMT idle timeout
	Intel® AMT	Power Package PP2 (Intel® ME on in S0, wake in Sx/AC)
		WLAN Link Policy LP3 (Enabled in S0, Sx/AC) where available
Setup:	<ol style="list-style-type: none"> Set the SUT power source to AC+DC. Bring the SUT to the base state of S0/MeOn (CM0,CM0-PG), and confirm that the Host OS is available. Verify that a DC battery is connected to the SUT, and that it is charged. Set the SUT power source to DC-only. Set the active power package on the SUT to Power Package 2 (Intel® ME on in S0, wake in Sx/AC). Set the Intel® AMT WLAN link policy on the SUT to Link Policy 3 (Enabled in S0, Sx/AC), if the WLAN network interface is available. Ensure the Intel® AMT idle timeout on the SUT is set to 1 minute. Ensure that the Host OS network device drivers are configured to not wake the SUT. This includes enabling ARP and/or NS Offload features where available to help prevent unexpected host wake events. Verify that Intel® AMT on the SUT responds to version queries via all available network interfaces. Shutdown the SUT via the Host OS. Verify that the SUT is in S5, Deep S5, G3/CM3-PG. 	
Procedure:	<ol style="list-style-type: none"> Set the SUT power source to AC+DC. Verify that Intel® AMT on the SUT responds to version queries via all available network interfaces. Verify that the SUT is in S5/MeOn (CM3). Wait for 3 minutes to allow the Intel® ME on the SUT to move to CM3-PG after Intel® AMT idle timeout. Verify that the SUT is in S5/CM3-PG. 	
Pass Criteria:	<p>The test passes if:</p> <ul style="list-style-type: none"> the SUT remains in S5 (or moves to S5 from Deep S5 or G3). when in S5/MeOn (CM3), Intel® AMT responds to version queries via all available network interfaces. the Intel® CSME ends the test in MeOff (CM3-PG). 	

ID:	ME_PM_23.3	
Title:	G3/CM-Off to S5/CM3-PG via Intel® AMT idle timeout (AC+DC/PP2/LP3)	
Requirement:	Mandatory	Exemptions <input checked="" type="checkbox"/> Non-Mobile (AC-only) systems
Method:	Automated by Intel® PETS	
Objective:	This test checks the SUT power flow from G3/CM-Off to S5/CM3-PG via Intel® AMT idle timeout with the parameters outlined below.	
Configuration:	<p>Intel® AMT should be provisioned via manual mode.</p> <p>Confirm that the BIOS is configured to move the SUT to S5 from G3 upon AC-attach.</p> <p>This test assumes that either LAN-only, WLAN-only, or both LAN and WLAN network interfaces are available on the SUT.</p>	



ID:	ME_PM_23.3		
Parameters:	System Power Source		AC+DC
	Power States	Initial	G3/MeOff (CM-Off)
		Final	S5/MeOff (CM3-PG)
		Trigger	(AC-attach then) Intel® AMT idle timeout
	Intel® AMT	Power Package	PP2 (Intel® ME on in S0, wake in Sx/AC)
WLAN Link Policy		LP3 (Enabled in S0, Sx/AC) where available	
Setup:	<div>1. Set the SUT power source to AC+DC.</div> <div>2. Bring the SUT to the base state of S0/MeOn (CM0,CM0-PG), and confirm that the Host OS is available.</div> <div>3. Verify that a DC battery is connected to the SUT, and that it is charged.</div> <div>4. Set the active power package on the SUT to Power Package 2 (Intel® ME on in S0, wake in Sx/AC).</div> <div>5. Set the Intel® AMT WLAN link policy on the SUT to Link Policy 3 (Enabled in S0, Sx/AC), if the WLAN network interface is available.</div> <div>6. Ensure the Intel® AMT idle timeout on the SUT is set to 1 minute.</div> <div>7. Ensure that the Host OS network device drivers are configured to not wake the SUT. This includes enabling ARP and/or NS Offload features where available to help prevent unexpected host wake events. Most especially, ensure that the Host OS Wireless Wake on LAN driver setting on the SUT is disabled, if the WLAN network interface is available.</div> <div>8. Verify that Intel® AMT on the SUT responds to version queries via all available network interfaces.</div> <div>9. Shutdown the SUT via the Host OS.</div> <div>10. Verify that the SUT is in S4, S5/MeOn (CM3).</div> <div>11. Verify that Intel® AMT on the SUT responds to version queries via all available network interfaces.</div> <div>12. Remove power from the SUT via AC-detach, and if necessary also via DC-detach. Wait for 10 seconds before continuing to allow full power drain from the SUT.</div> <div>13. Verify that the SUT is in G3/MeOff (CM-Off).</div> <div>14. Verify that Intel® AMT on the SUT does not respond to version queries via any of the available network interfaces.</div>		
Procedure:	<div>1. Set the SUT power source to AC+DC where supported; otherwise AC-only. For systems with DC-power support, consult the system design as it may be preferred to connect DC-power before AC-power.</div> <div>2. Verify that Intel® AMT on the SUT responds to version queries via all available network interfaces.</div> <div>3. Verify that the SUT is in S5/MeOn (CM3).</div> <div>4. Wait for 3 minutes to allow the Intel® ME on the SUT to move to CM3-PG after Intel® AMT idle timeout.</div> <div>5. Verify that the SUT is in S5/CM3-PG.</div>		
Pass Criteria:	<div>The test passes if:</div> <div><div>• the SUT moves to S5.</div><div>• when in S5/MeOn (CM3), Intel® AMT responds to version queries via all available network interfaces.</div><div>• the Intel® CSME ends the test in MeOff (CM3-PG).</div></div>		



12.27 ME_PM_24: S4-S5/CM-Off (with Intel® ME Wake) to S4-S5/CM-Off (Without Intel® ME Wake)

ID:	ME_PM_24.1	
Title:	S4/CM3-PG to S4/CM3-PG with AC Wake via AC-detach (AC+DC/PP2/LP3)	
Requirement:	Mandatory	Exemptions <input checked="" type="checkbox"/> Non-Mobile (AC-only) systems
Method:	Automated by Intel® PETS	
Objective:	This test checks the SUT power flow from S4/CM3-PG to S4/CM-Off via AC-detach with the parameters outlined below.	
Configuration:	<p>Intel® AMT should be provisioned via manual mode.</p> <p>If Deep S4, Deep S5, and/or G3 are supported on the SUT, please confirm the following:</p> <ul style="list-style-type: none"> the SUT and/or BIOS are properly configured to permit Deep S4/S5 or G3 entry. the correct Deep Sx policy is applied to the SUT profile in Intel® PETS. <p>This test assumes that either LAN-only, WLAN-only, or both LAN and WLAN network interfaces are available on the SUT.</p>	
Parameters:	System Power Source AC+DC	
	Power States	Initial S4,S5/MeOff (CM3-PG)
		Final S4,S5,Deep S4,Deep S5,G3/CM3-PG
		Trigger (Intel® AMT idle timeout then) AC-detach
	Intel® AMT	Power Package PP2 (Intel® ME on in S0, wake in Sx/AC)
		WLAN Link Policy LP3 (Enabled in S0, Sx/AC) where available
Setup:	<ol style="list-style-type: none"> Set the SUT power source to AC+DC. Bring the SUT to the base state of S0/MeOn (CM0,CM0-PG), and confirm that the Host OS is available. Verify that a DC battery is connected to the SUT, and that it is charged. Set the active power package on the SUT to Power Package 2 (Intel® ME on in S0, wake in Sx/AC). Set the Intel® AMT WLAN link policy on the SUT to Link Policy 3 (Enabled in S0, Sx/AC), if the WLAN network interface is available. Ensure the Intel® AMT idle timeout on the SUT is set to 1 minute. Ensure that the Host OS network device drivers are configured to not wake the SUT. This includes enabling ARP and/or NS Offload features where available to help prevent unexpected host wake events. Verify that Intel® AMT on the SUT responds to version queries via all available network interfaces. Hibernate the SUT via the Host OS. Verify that the SUT is in S4, S5/MeOn (CM3). Verify that Intel® AMT on the SUT responds to version queries via all available network interfaces. Wait for 3 minutes to allow the Intel® ME on the SUT to move to CM3-PG after Intel® AMT idle timeout. Verify that the Intel® ME on the SUT is in CM3-PG. 	
Procedure:	<ol style="list-style-type: none"> Set the SUT power source to DC-only. Verify that the SUT is in S4, S5, Deep S4, Deep S5, G3/CM3-PG with Ac Wake Verify that Intel® AMT on the SUT does not respond to version queries via any of the available network interfaces. 	
Pass Criteria:	<p>The test passes if:</p> <ul style="list-style-type: none"> the SUT remains in S4 or S5 (or moves to Deep S4, Deep S5, or G3). Intel® AMT does not respond to version queries via any available network interface. the Intel® CSME ends the test in MeOff (CM3-PG) with AC Wake. 	

ID:	ME_PM_24.2	
Title:	S5/CM3-PG to S5/CM3-PG with AC Wake via AC-detach (AC+DC/PP2/LP3)	
Requirement:	Mandatory	Exemptions <input checked="" type="checkbox"/> Non-Mobile (AC-only) systems
Method:	Automated by Intel® PETS	



ID:	ME_PM_24.2	
Objective:	This test checks the SUT power flow from S5/CM3-PG to S5/CM3-PG with Ac Wake via AC-detach with the parameters outlined below.	
Configuration:	<p>Intel® AMT should be provisioned via manual mode.</p> <p>If Deep S5 and/or G3 are supported on the SUT, please confirm the following:</p> <ul style="list-style-type: none"> the SUT and/or BIOS are properly configured to permit Deep S5 or G3 entry. the correct Deep Sx policy is applied to the SUT profile in Intel® PETS. <p>This test assumes that either LAN-only, WLAN-only, or both LAN and WLAN network interfaces are available on the SUT.</p>	
Parameters:	System Power Source AC+DC	
	Power States	Initial S5/MeOff (CM3-PG)
		Final S5,Deep S5,G3/CM3-PG with Ac wake
		Trigger (Intel® AMT idle timeout then) AC-detach
	Intel® AMT	Power Package PP2 (Intel® ME on in S0, wake in Sx/AC)
		WLAN Link Policy LP3 (Enabled in S0, Sx/AC) where available
Setup:	<ol style="list-style-type: none"> Set the SUT power source to AC+DC. Bring the SUT to the base state of S0/MeOn (CM0,CM0-PG), and confirm that the Host OS is available. Verify that a DC battery is connected to the SUT, and that it is charged. Set the active power package on the SUT to Power Package 2 (Intel® ME on in S0, wake in Sx/AC). Set the Intel® AMT WLAN link policy on the SUT to Link Policy 3 (Enabled in S0, Sx/AC), if the WLAN network interface is available. Ensure the Intel® AMT idle timeout on the SUT is set to 1 minute. Ensure that the Host OS network device drivers are configured to not wake the SUT. This includes enabling ARP and/or NS Offload features where available to help prevent unexpected host wake events. Verify that Intel® AMT on the SUT responds to version queries via all available network interfaces. Shutdown the SUT via the Host OS. Verify that the SUT is in S5/MeOn (CM3). Verify that Intel® AMT on the SUT responds to version queries via all available network interfaces. Wait for 3 minutes to allow the Intel® ME on the SUT to move to CM3-PG after Intel® AMT idle timeout. Verify that the Intel® ME on the SUT is in CM3-PG. 	
Procedure:	<ol style="list-style-type: none"> Set the SUT power source to DC-only. Verify that the SUT is in S5, Deep S5, G3/CM3-PG.with AC Wake. Verify that Intel® AMT on the SUT does not respond to version queries via any of the available network interfaces. 	
Pass Criteria:	<p>The test passes if:</p> <ul style="list-style-type: none"> the SUT remains in S5 (or moves to Deep S5 or G3). Intel® AMT does not respond to version queries via any available network interface. the Intel® CSME ends the test in MeOff (CM3-PG) with AC Wake. 	

12.28 ME_PM_25: S4–S5/CM-Off (Suspend Well Off) to S4–S5/CM-Off (with Host WoL) to S0/CM0 via Host WoL/WoWLAN

ID:	ME_PM_25.1	
Title:	S4/CM-Off to S0/CM0 via magic packet (DC-only/PP1/LP3)	
Requirement:	Mandatory Exemptions	<input checked="" type="checkbox"/> Non-Mobile (AC-only) systems
		<input checked="" type="checkbox"/> Systems without WoL and/or WoWLAN support
Method:	Automated by Intel® PETS	
Objective:	This test checks the SUT power flow from S4/CM-Off to S0/CM0 via magic packet with the parameters outlined below.	



ID:	ME_PM_25.1																
Configuration:	<p>Intel® AMT should be provisioned via manual mode.</p> <p>If Deep S4, Deep S5, and/or G3 are supported on the SUT, please confirm the following:</p> <ul style="list-style-type: none"> the SUT and/or BIOS are properly configured to permit Deep S4/S5 or G3 entry. the correct Deep Sx policy is applied to the SUT profile in Intel® PETS. <p>This test assumes that either LAN-only, WLAN-only, or both LAN and WLAN network interfaces are available on the SUT. Where both network interfaces are available, LAN is the initial active network interface in the test, and WLAN is the secondary network interface.</p>																
Parameters:	<table> <tr> <td colspan="2">System Power Source</td><td>DC-only</td></tr> <tr> <td rowspan="3">Power States</td><td>Initial</td><td>S4, S5, Deep S4, Deep S5, G3/MeOff (CM-Off)</td></tr> <tr> <td>Final</td><td>S0/MeOn (CM0, CM0-PG)</td></tr> <tr> <td>Trigger</td><td>Magic Packet receipt</td></tr> <tr> <td rowspan="2">Intel® AMT</td><td>Power Package</td><td>PP1 (Intel® ME on in S0)</td></tr> <tr> <td>WLAN Link Policy</td><td>LP3 (Enabled in S0, Sx/AC) where available</td></tr> </table>	System Power Source		DC-only	Power States	Initial	S4, S5, Deep S4, Deep S5, G3/MeOff (CM-Off)	Final	S0/MeOn (CM0, CM0-PG)	Trigger	Magic Packet receipt	Intel® AMT	Power Package	PP1 (Intel® ME on in S0)	WLAN Link Policy	LP3 (Enabled in S0, Sx/AC) where available	
System Power Source		DC-only															
Power States	Initial	S4, S5, Deep S4, Deep S5, G3/MeOff (CM-Off)															
	Final	S0/MeOn (CM0, CM0-PG)															
	Trigger	Magic Packet receipt															
Intel® AMT	Power Package	PP1 (Intel® ME on in S0)															
	WLAN Link Policy	LP3 (Enabled in S0, Sx/AC) where available															
Setup:	<ol style="list-style-type: none"> Set the SUT power source to AC+DC. Bring the SUT to the base state of S0/MeOn (CM0,CM0-PG), and confirm that the Host OS is available. Verify that a DC battery is connected to the SUT, and that it is charged. Set the SUT power source to DC-only. Set the active power package on the SUT to Power Package 1 (Intel® ME on in S0). Set the Intel® AMT WLAN link policy on the SUT to Link Policy 3 (Enabled in S0, Sx/AC), if the WLAN network interface is available. Ensure that, where available, only the Host OS Wake on LAN and/or Wake on Wireless LAN driver setting(s) are enabled on the SUT. All other network wake sources must be disabled. This includes enabling ARP and/or NS Offload features where available to help prevent unexpected host wake events. Verify that Intel® AMT on the SUT responds to version queries via all available network interfaces. Ensure yellow bang is not seen on Drivers in Device Manager 																
Procedure:	<ol style="list-style-type: none"> Hibernate the SUT via the Host OS. Verify that the SUT is in S4, S5, Deep S4, Deep S5, G3/MeOff (CM-Off). Set the SUT power source to AC+DC where supported; otherwise AC-only. For systems with DC-power support, consult the system design as it may be preferred to connect DC-power before AC-power. Verify that the SUT is in S4, S5, Deep S4, Deep S5, G3/MeOff (CM-Off). Send three magic packets, at 2 second intervals, by means of the active network interface. Verify that the SUT is in S0/MeOn (CM0,CM0-PG). Verify that the Host OS on the SUT is available. Verify that Intel® AMT on the SUT responds to version queries via all available network interfaces. Verify that windows booted from hibernate i.e. value should be 0x02. "run the following power shell command": Get-WinEvent -ProviderName Microsoft-Windows-Kernel-boot -MaxEvents 10 Where-Object {\$_.message -like "The boot type*"} Verify that the second nibble of the FWSTS2 register on the SUT have a value of 0x60xxxxxx. Ensure yellow bang is not seen on Drivers in Device Manager <p>If both LAN and WLAN network interfaces are available, repeat this test procedure with the WLAN interface set as the active network interface.</p>																
Pass Criteria:	<p>The test passes if:</p> <ul style="list-style-type: none"> the SUT moves from S4, S5, Deep S4, Deep S5, or G3 to S0. the Intel® CSME moves to MeOn (CM0). Intel® AMT responds to version queries via all available network interfaces. 																

ID:	ME_PM_25.2		
Title:	S5/CM-Off to S0/CM0 via magic packet (DC-only/PP1/LP3)		
Requirement:	Mandatory	Exemptions	<div><input checked="" type="checkbox"/> Non-Mobile (AC-only) systems</div> <div><input checked="" type="checkbox"/> Systems without WoL and/or WoWLAN support</div>
Method:	Automated by Intel® PETS		



ID:	ME_PM_25.2																
Objective:	This test checks the SUT power flow from S5/CM-Off to S0/CM0 via magic packet with the parameters outlined below.																
Configuration:	<p>Intel® AMT should be provisioned via manual mode.</p> <p>If Deep S5 and/or G3 are supported on the SUT, please confirm the following:</p> <ul style="list-style-type: none"> the SUT and/or BIOS are properly configured to permit Deep S5 or G3 entry. the correct Deep Sx policy is applied to the SUT profile in Intel® PETS. <p>This test assumes that either LAN-only, WLAN-only, or both LAN and WLAN network interfaces are available on the SUT. Where both network interfaces are available, LAN is the initial active network interface in the test, and WLAN is the secondary network interface.</p>																
Parameters:	<table> <tr> <th colspan="2">System Power Source</th><td>DC-only</td></tr> <tr> <th rowspan="3">Power States</th><th>Initial</th><td>S5, Deep S5, G3/MeOff (CM-Off)</td></tr> <tr> <th>Final</th><td>S0/MeOn (CM0, CM0-PG)</td></tr> <tr> <th>Trigger</th><td>Magic Packet receipt</td></tr> <tr> <th rowspan="2">Intel® AMT</th><th>Power Package</th><td>PP1 (Intel® ME on in S0)</td></tr> <tr> <th>WLAN Link Policy</th><td>LP3 (Enabled in S0, Sx/AC) where available</td></tr> </table>	System Power Source		DC-only	Power States	Initial	S5, Deep S5, G3/MeOff (CM-Off)	Final	S0/MeOn (CM0, CM0-PG)	Trigger	Magic Packet receipt	Intel® AMT	Power Package	PP1 (Intel® ME on in S0)	WLAN Link Policy	LP3 (Enabled in S0, Sx/AC) where available	
System Power Source		DC-only															
Power States	Initial	S5, Deep S5, G3/MeOff (CM-Off)															
	Final	S0/MeOn (CM0, CM0-PG)															
	Trigger	Magic Packet receipt															
Intel® AMT	Power Package	PP1 (Intel® ME on in S0)															
	WLAN Link Policy	LP3 (Enabled in S0, Sx/AC) where available															
Setup:	<ol style="list-style-type: none"> Set the SUT power source to AC+DC. Bring the SUT to the base state of S0/MeOn (CM0,CM0-PG), and confirm that the Host OS is available. Verify that a DC battery is connected to the SUT, and that it is charged. Set the SUT power source to DC-only. Set the active power package on the SUT to Power Package 1 (Intel® ME on in S0). Set the Intel® AMT WLAN link policy on the SUT to Link Policy 3 (Enabled in S0, Sx/AC), if the WLAN network interface is available. Ensure that, where available, only the Host OS Wake on LAN and/or Wake on Wireless LAN driver setting(s) are enabled on the SUT. All other network wake sources must be disabled. This includes enabling ARP and/or NS Offload features where available to help prevent unexpected host wake events. Verify that Intel® AMT on the SUT responds to version queries via all available network interfaces. Ensure yellow bang is not seen on Drivers in Device Manager 																
Procedure:	<ol style="list-style-type: none"> Shutdown the SUT via the Host OS. Verify that the SUT is in S5, Deep S5, G3/MeOff (CM-Off). Set the SUT power source to AC+DC where supported; otherwise AC-only. For systems with DC-power support, consult the system design as it may be preferred to connect DC-power before AC-power. Verify that the SUT is in S5, Deep S5, G3/MeOff (CM-Off). Send three magic packets, at 2 second intervals, by means of the active network interface. Verify that the SUT is in S0/MeOn (CM0,CM0-PG). Verify that the Host OS on the SUT is available. Verify that Intel® AMT on the SUT responds to version queries via all available network interfaces. Verify that the second nibble of the FWSTS2 register on the SUT have a value of 0x60xxxxxx. Ensure yellow bang is not seen on Drivers in Device Manager <p>If both LAN and WLAN network interfaces are available, repeat this test procedure with the WLAN interface set as the active network interface.</p>																
Pass Criteria:	<p>The test passes if:</p> <ul style="list-style-type: none"> the SUT moves from S5, (or Deep S5 or G3) to S0. the Intel® CSME moves to MeOn (CM0). Intel® AMT responds to version queries via all available network interfaces. 																



ID:	ME_PM_25.3																	
Title:	G3/CM-Off to S0/CM0 via magic packet (DC-only/PP1/LP3)																	
Requirement:	Mandatory	Exemptions	<div><input checked="" type="checkbox"/> Non-Mobile (AC-only) systems</div> <div><input checked="" type="checkbox"/> Systems without WoL and/or WoWLAN support</div>															
Method:	Automated by Intel® PETS																	
Objective:	This test checks the SUT power flow from G3/CM-Off to S0/CM0 via magic packet with the parameters outlined below.																	
Configuration:	<p>Intel® AMT should be provisioned via manual mode.</p> <p>If Deep S5 and/or G3 are supported on the SUT, please confirm the following:</p> <ul style="list-style-type: none">the SUT and/or BIOS are properly configured to permit Deep S5 or G3 entry.the correct Deep Sx policy is applied to the SUT profile in Intel® PETS. <p>Confirm that the Host OS is configured to shutdown the SUT upon Power Button press.</p> <p>This test assumes that either LAN-only, WLAN-only, or both LAN and WLAN network interfaces are available on the SUT. Where both network interfaces are available, LAN is the initial active network interface in the test, and WLAN is the secondary network interface.</p>																	
Parameters:	<table><tr><th colspan="2">System Power Source</th></tr><tr><td rowspan="3">Power States</td><td>Initial</td></tr><tr><td>Final</td></tr><tr><td>Trigger</td></tr><tr><td rowspan="2">Intel® AMT</td><td>Power Package</td></tr><tr><td>WLAN Link Policy</td></tr></table>	System Power Source		Power States	Initial	Final	Trigger	Intel® AMT	Power Package	WLAN Link Policy	<table><tr><td>DC-only</td></tr><tr><td>G3/MeOff (CM-Off)</td></tr><tr><td>S0/MeOn (CM0, CM0-PG)</td></tr><tr><td>Magic Packet receipt</td></tr><tr><td>PP1 (Intel® ME on in S0)</td></tr><tr><td>LP3 (Enabled in S0, Sx/AC) where available</td></tr></table>		DC-only	G3/MeOff (CM-Off)	S0/MeOn (CM0, CM0-PG)	Magic Packet receipt	PP1 (Intel® ME on in S0)	LP3 (Enabled in S0, Sx/AC) where available
System Power Source																		
Power States	Initial																	
	Final																	
	Trigger																	
Intel® AMT	Power Package																	
	WLAN Link Policy																	
DC-only																		
G3/MeOff (CM-Off)																		
S0/MeOn (CM0, CM0-PG)																		
Magic Packet receipt																		
PP1 (Intel® ME on in S0)																		
LP3 (Enabled in S0, Sx/AC) where available																		
Setup:	<div><div>1. Set the SUT power source to AC+DC.</div><div>2. Bring the SUT to the base state of S0/MeOn (CM0,CM0-PG), and confirm that the Host OS is available.</div><div>3. Verify that a DC battery is connected to the SUT, and that it is charged.</div><div>4. Set the SUT power source to DC-only.</div><div>5. Set the active power package on the SUT to Power Package 1 (Intel® ME on in S0).</div><div>6. Set the Intel® AMT WLAN link policy on the SUT to Link Policy 3 (Enabled in S0, Sx/AC), if the WLAN network interface is available.</div><div>7. Ensure that, where available, only the Host OS Wake on LAN and/or Wake on Wireless LAN driver setting(s) are enabled on the SUT. All other network wake sources must be disabled. This includes enabling ARP and/or NS Offload features where available to help prevent unexpected host wake events.</div><div>8. Verify that Intel® AMT on the SUT responds to version queries via all available network interfaces.</div><div>9. Ensure yellow bang is not seen on Drivers in Device Manager</div></div>																	
Procedure:	<div><div>1. Shutdown the SUT via the Host OS.</div><div>2. Verify that the SUT is in S5, Deep S5, G3/MeOff (CM-Off).</div><div>3. Remove power from the SUT via AC-detach, and if necessary also via DC-detach. Wait for 10 seconds before continuing to allow full power drain from the SUT.</div><div>4. Verify that the SUT is in G3/MeOff (CM-Off).</div><div>5. Set the SUT power source to AC+DC where supported; otherwise AC-only. For systems with DC-power support, consult the system design as it may be preferred to connect DC-power before AC-power.</div><div>6. Verify that the SUT is in S5, Deep S5, G3/MeOff (CM-Off).</div><div>7. Send three magic packets, at 2 second intervals, by means of the active network interface.</div><div>8. Verify that the SUT is in S0/MeOn (CM0,CM0-PG).</div><div>9. Verify that the Host OS on the SUT is available.</div><div>10. Verify that Intel® AMT on the SUT responds to version queries via all available network interfaces.</div><div>11. Verify that the second nibble of the FWSTS2 register on the SUT have a value of 0x60xxxxxx.</div><div>12. Ensure yellow bang is not seen on Drivers in Device Manager</div></div> <div>If both LAN and WLAN network interfaces are available, repeat this test procedure with the WLAN interface set as the active network interface.</div>																	



ID:	ME_PM_25.3
Pass Criteria:	<p>The test passes if:</p> <ul style="list-style-type: none"> the SUT moves from S5, (or Deep S5 or G3) to S0. the Intel® CSME moves to MeOn (CM0). Intel® AMT responds to version queries via all available network interfaces.

12.29 ME_PM_26: Warm Reset

ID:	ME_PM_26.5		
Title:	S0/CM0 to S0/CM0 via Reset Button press (or logic) (DC-only/PP1/LP3)		
Requirement:	Mandatory	Exemptions	<input checked="" type="checkbox"/> Non-Mobile (AC-only) systems
Method:	Automated by Intel® PETS		
Objective:	This test checks the SUT power flow from S0/CM0 to S0/CM0 via Reset Button press (or logic) with the parameters outlined below.		
Configuration:	<p>Intel® AMT should be provisioned via manual mode.</p> <p>This test assumes that either LAN-only, WLAN-only, or both LAN and WLAN network interfaces are available on the SUT.</p>		
Parameters:	System Power Source		DC-only
	Power States	Initial	S0/MeOn (CM0, CM0-PG)
		Final	S0/MeOn (CM0, CM0-PG)
		Trigger	Reset Button press (or logic)
	Intel® AMT	Power Package	PP1 (Intel® ME on in S0)
		WLAN Link Policy	LP3 (Enabled in S0, Sx/AC) where available
Setup:	<ol style="list-style-type: none"> Set the SUT power source to AC+DC. Bring the SUT to the base state of S0/MeOn (CM0,CM0-PG), and confirm that the Host OS is available. Verify that a DC battery is connected to the SUT, and that it is charged. Set the SUT power source to DC-only. Set the active power package on the SUT to Power Package 1 (Intel® ME on in S0). Set the Intel® AMT WLAN link policy on the SUT to Link Policy 3 (Enabled in S0, Sx/AC), if the WLAN network interface is available. Verify that Intel® AMT on the SUT responds to version queries via all available network interfaces. Ensure yellow bang is not seen on Drivers in Device Manager 		
Procedure:	<ol style="list-style-type: none"> Perform a warm reset of the SUT by pressing the Reset Button. For designs without a Reset Button, access to the system reset logic should be prepared via blue wire. Verify that the SUT is in S0/MeOn (CM0,CM0-PG). Wait 2 minutes before proceeding if the WLAN network interface is available. Because the Host OS may boot to error recovery screen following unexpected shutdown, the Host OS WLAN driver may not become available immediately. This delay allows enough time for Intel® AMT firmware to take control over the WLAN hardware and respond to manageability requests. Verify that Intel® AMT on the SUT responds to version queries via all available network interfaces. Verify that the second nibble of the FWSTS2 register on the SUT have a value of 0x62xxxxxx. Ensure yellow bang is not seen on Drivers in Device Manager 		
Pass Criteria:	<p>The test passes if:</p> <ul style="list-style-type: none"> the SUT is reset to S0. the Intel® CSME is available in MeOn (CM0, CM0-PG). Intel® AMT responds to version queries via all available network interfaces. 		



ID:	ME_PM_26.6	
Title:	S0/CM0 to S0/CM0 via Reset Button press (or logic) (AC+DC, AC-only/PP1/LP3)	
Requirement:	Mandatory	Exemptions None
Method:	Automated by Intel® PETS	
Objective:	This test checks the SUT power flow from S0/CM0 to S0/CM0 via Reset Button press (or logic) with the parameters outlined below.	
Configuration:	Intel® AMT should be provisioned via manual mode. This test assumes that either LAN-only, WLAN-only, or both LAN and WLAN network interfaces are available on the SUT.	
Parameters:	System Power Source AC+DC or AC-only	
	Power States	Initial S0/MeOn (CM0, CM0-PG)
		Final S0/MeOn (CM0, CM0-PG)
		Trigger Reset Button press (or logic)
	Intel® AMT	Power Package PP1 (Intel® ME on in S0)
		WLAN Link Policy LP3 (Enabled in S0, Sx/AC) where available
Setup:	<ol style="list-style-type: none"> 1. Set the SUT power source to AC+DC where supported; otherwise AC-only. 2. Bring the SUT to the base state of S0/MeOn (CM0,CM0-PG), and confirm that the Host OS is available. 3. Set the active power package on the SUT to Power Package 1 (Intel® ME on in S0). 4. Set the Intel® AMT WLAN link policy on the SUT to Link Policy 3 (Enabled in S0, Sx/AC), if the WLAN network interface is available. 5. Verify that Intel® AMT on the SUT responds to version queries via all available network interfaces. 6. Ensure yellow bang is not seen on Drivers in Device Manager 	
Procedure:	<ol style="list-style-type: none"> 1. Perform a warm reset of the SUT by pressing the Reset Button. For designs without a Reset Button, access to the system reset logic should be prepared via blue wire. 2. Verify that the SUT is in S0/MeOn (CM0,CM0-PG). 3. Wait 2 minutes before proceeding if the WLAN network interface is available. Because the Host OS may boot to error recovery screen following unexpected shutdown, the Host OS WLAN driver may not become available immediately. This delay allows enough time for Intel® AMT firmware to take control over the WLAN hardware and respond to manageability requests. 4. Verify that Intel® AMT on the SUT responds to version queries via all available network interfaces. 5. Verify that the second nibble of the FWSTS2 register on the SUT have a value of 0x69xxxxxx. 6. Ensure yellow bang is not seen on Drivers in Device Manager 	
Pass Criteria:	The test passes if: <ul style="list-style-type: none"> • the SUT is reset to S0. • the Intel® CSME is available in MeOn (CM0, CM0-PG). • Intel® AMT responds to version queries via all available network interfaces. 	

ID:	ME_PM_26.7	
Title:	S0/CM0 to S0/CM0 via Reset Button press (or logic) (DC-only/PP2/LP3)	
Requirement:	Mandatory	Exemptions <input checked="" type="checkbox"/> Non-Mobile (AC-only) systems
Method:	Automated by Intel® PETS	
Objective:	This test checks the SUT power flow from S0/CM0 to S0/CM0 via Reset Button press (or logic) with the parameters outlined below.	
Configuration:	Intel® AMT should be provisioned via manual mode. This test assumes that either LAN-only, WLAN-only, or both LAN and WLAN network interfaces are available on the SUT.	



ID:	ME_PM_26.7		
Parameters:	System Power Source		DC-only
	Power States	Initial	S0/MeOn (CM0, CM0-PG)
		Final	S0/MeOn (CM0, CM0-PG)
		Trigger	Reset Button press (or logic)
	Intel® AMT	Power Package	PP2 (Intel® ME on in S0, wake in Sx/AC)
		WLAN Link Policy	LP3 (Enabled in S0, Sx/AC) where available
Setup:	<ol style="list-style-type: none"> 1. Set the SUT power source to AC+DC. 2. Bring the SUT to the base state of S0/MeOn (CM0,CM0-PG), and confirm that the Host OS is available. 3. Verify that a DC battery is connected to the SUT, and that it is charged. 4. Set the SUT power source to DC-only. 5. Set the active power package on the SUT to Power Package 2 (Intel® ME on in S0, wake in Sx/AC). 6. Set the Intel® AMT WLAN link policy on the SUT to Link Policy 3 (Enabled in S0, Sx/AC), if the WLAN network interface is available. 7. Verify that Intel® AMT on the SUT responds to version queries via all available network interfaces. 8. Ensure yellow bang is not seen on Drivers in Device Manager 		
Procedure:	<ol style="list-style-type: none"> 1. Perform a warm reset of the SUT by pressing the Reset Button. For designs without a Reset Button, access to the system reset logic should be prepared via blue wire. 2. Verify that the SUT is in S0/MeOn (CM0,CM0-PG). 3. Wait 2 minutes before proceeding if the WLAN network interface is available. Because the Host OS may boot to error recovery screen following unexpected shutdown, the Host OS WLAN driver may not become available immediately. This delay allows enough time for Intel® AMT firmware to take control over the WLAN hardware and respond to manageability requests. 4. Verify that Intel® AMT on the SUT responds to version queries via all available network interfaces. 5. Verify that the second nibble of the FWSTS2 register on the SUT have a value of 0x69xxxxxx. 6. Ensure yellow bang is not seen on Drivers in Device Manager 		
Pass Criteria:	The test passes if: <ul style="list-style-type: none"> • the SUT is reset to S0. • the Intel® CSME is available in MeOn (CM0, CM0-PG). • Intel® AMT responds to version queries via all available network interfaces. 		

ID:	ME_PM_26.8		
Title:	S0/CM0 to S0/CM0 via Reset Button press (or logic) (AC+DC, AC-only/PP2/LP3)		
Requirement:	Mandatory	Exemptions	None
Method:	Automated by Intel® PETS		
Objective:	This test checks the SUT power flow from S0/CM0 to S0/CM0 via Reset Button press (or logic) with the parameters outlined below.		
Configuration:	Intel® AMT should be provisioned via manual mode. This test assumes that either LAN-only, WLAN-only, or both LAN and WLAN network interfaces are available on the SUT.		
Parameters:	System Power Source		AC+DC or AC-only
	Power States	Initial	S0/MeOn (CM0, CM0-PG)
		Final	S0/MeOn (CM0, CM0-PG)
		Trigger	Reset Button press (or logic)
	Intel® AMT	Power Package	PP2 (Intel® ME on in S0, wake in Sx/AC)
		WLAN Link Policy	LP3 (Enabled in S0, Sx/AC) where available



ID:	ME_PM_26.8
Setup:	<ol style="list-style-type: none"> 1. Set the SUT power source to AC+DC where supported; otherwise AC-only. 2. Bring the SUT to the base state of S0/MeOn (CM0,CM0-PG), and confirm that the Host OS is available. 3. Set the active power package on the SUT to Power Package 2 (Intel® ME on in S0, wake in Sx/AC). 4. Set the Intel® AMT WLAN link policy on the SUT to Link Policy 3 (Enabled in S0, Sx/AC), if the WLAN network interface is available. 5. Verify that Intel® AMT on the SUT responds to version queries via all available network interfaces. 6. Ensure yellow bang is not seen on Drivers in Device Manager
Procedure:	<ol style="list-style-type: none"> 1. Perform a warm reset of the SUT by pressing the Reset Button. For designs without a Reset Button, access to the system reset logic should be prepared via blue wire. 2. Verify that the SUT is in S0/MeOn (CM0,CM0-PG). 3. Wait 2 minutes before proceeding if the WLAN network interface is available. Because the Host OS may boot to error recovery screen following unexpected shutdown, the Host OS WLAN driver may not become available immediately. This delay allows enough time for Intel® AMT firmware to take control over the WLAN hardware and respond to manageability requests. 4. Verify that Intel® AMT on the SUT responds to version queries via all available network interfaces. 5. Verify that the second nibble of the FWSTS2 register on the SUT have a value of 0x69xxxxxx. 6. Ensure yellow bang is not seen on Drivers in Device Manager
Pass Criteria:	<p>The test passes if:</p> <ul style="list-style-type: none"> • the SUT is reset to S0. • the Intel® CSME is available in MeOn (CM0, CM0-PG). • Intel® AMT responds to version queries via all available network interfaces.

ID:	ME_PM_26.9	
Title:	S0/CM0 to S0/CM0 via Host OS restart (DC-only/PP1/LP3)	
Requirement:	Mandatory Exemptions <input checked="" type="checkbox"/> Non-Mobile (AC-only) systems	
Method:	Automated by Intel® PETS	
Objective:	This test checks the SUT power flow from S0/CM0 to S0/CM0 via Host OS restart with the parameters outlined below.	
Configuration:	<p>Intel® AMT should be provisioned via manual mode.</p> <p>This test assumes that either LAN-only, WLAN-only, or both LAN and WLAN network interfaces are available on the SUT.</p>	
Parameters:	System Power Source	DC-only
	Power States	Initial S0/MeOn (CM0, CM0-PG)
		Final S0/MeOn (CM0, CM0-PG)
		Trigger Host OS restart
	Intel® AMT	Power Package PP1 (Intel® ME on in S0)
		WLAN Link Policy LP3 (Enabled in S0, Sx/AC) where available
Setup:	<ol style="list-style-type: none"> 1. Set the SUT power source to AC+DC. 2. Bring the SUT to the base state of S0/MeOn (CM0,CM0-PG), and confirm that the Host OS is available. 3. Verify that a DC battery is connected to the SUT, and that it is charged. 4. Set the SUT power source to DC-only. 5. Set the active power package on the SUT to Power Package 1 (Intel® ME on in S0). 6. Set the Intel® AMT WLAN link policy on the SUT to Link Policy 3 (Enabled in S0, Sx/AC), if the WLAN network interface is available. 7. Verify that Intel® AMT on the SUT responds to version queries via all available network interfaces. 8. Ensure yellow bang is not seen on Drivers in Device Manager 	



ID:	ME_PM_26.9
Procedure:	<ol style="list-style-type: none"> 1. Perform a warm reset of the SUT via Host OS graceful restart. 2. Verify that the SUT is in S0/MeOn (CM0,CM0-PG). 3. Verify that Intel® AMT on the SUT responds to version queries via all available network interfaces. 4. Verify that the second nibble of the FWSTS2 register on the SUT have a value of 0x69xxxxxx. 5. Ensure yellow bang is not seen on Drivers in Device Manager
Pass Criteria:	<p>The test passes if:</p> <ul style="list-style-type: none"> • the SUT is reset to S0. • the Intel® CSME is available in MeOn (CM0, CM0-PG). • Intel® AMT responds to version queries via all available network interfaces.

ID:	ME_PM_26.10		
Title:	S0/CM0 to S0/CM0 via Host OS restart (AC+DC, AC-only/PP1/LP3)		
Requirement:	Mandatory	Exemptions	None
Method:	Automated by Intel® PETS		
Objective:	This test checks the SUT power flow from S0/CM0 to S0/CM0 via Host OS restart with the parameters outlined below.		
Configuration:	Intel® AMT should be provisioned via manual mode. This test assumes that either LAN-only, WLAN-only, or both LAN and WLAN network interfaces are available on the SUT.		
Parameters:	System Power Source		AC+DC or AC-only
	Power States	Initial	S0/MeOn (CM0, CM0-PG)
		Final	S0/MeOn (CM0, CM0-PG)
		Trigger	Host OS restart
	Intel® AMT	Power Package	PP1 (Intel® ME on in S0)
WLAN Link Policy		LP3 (Enabled in S0, Sx/AC) where available	
Setup:	<ol style="list-style-type: none">1. Set the SUT power source to AC+DC where supported; otherwise AC-only.2. Bring the SUT to the base state of S0/MeOn (CM0,CM0-PG), and confirm that the Host OS is available.3. Set the active power package on the SUT to Power Package 1 (Intel® ME on in S0).4. Set the Intel® AMT WLAN link policy on the SUT to Link Policy 3 (Enabled in S0, Sx/AC), if the WLAN network interface is available.5. Verify that Intel® AMT on the SUT responds to version queries via all available network interfaces.6. Ensure yellow bang is not seen on Drivers in Device Manager		
Procedure:	<ol style="list-style-type: none">1. Perform a warm reset of the SUT via Host OS graceful restart.2. Verify that the SUT is in S0/MeOn (CM0,CM0-PG).3. Verify that Intel® AMT on the SUT responds to version queries via all available network interfaces.4. Verify that the second nibble of the FWSTS2 register on the SUT have a value of 0x69xxxxx.5. Ensure yellow bang is not seen on Drivers in Device Manager		
Pass Criteria:	The test passes if: <ul style="list-style-type: none">• the SUT is reset to S0.• the Intel® CSME is available in MeOn (CM0, CM0-PG).• Intel® AMT responds to version queries via all available network interfaces.		

ID:	ME_PM_26.11
Title:	S0/CM0 to S0/CM0 via Host OS restart (DC-only/PP2/LP3)
Requirement:	Mandatory Exemptions <input checked="" type="checkbox"/> Non-Mobile (AC-only) systems
Method:	Automated by Intel® PETS



ID:	ME_PM_26.11	
Objective:	This test checks the SUT power flow from S0/CM0 to S0/CM0 via Host OS restart with the parameters outlined below.	
Configuration:	Intel® AMT should be provisioned via manual mode. This test assumes that either LAN-only, WLAN-only, or both LAN and WLAN network interfaces are available on the SUT.	
Parameters:	System Power Source	DC-only
	Power States	Initial S0/MeOn (CM0, CM0-PG)
		Final S0/MeOn (CM0, CM0-PG)
		Trigger Host OS restart
	Intel® AMT	Power Package PP2 (Intel® ME on in S0, wake in Sx/AC) WLAN Link Policy LP3 (Enabled in S0, Sx/AC) where available
Setup:	<ol style="list-style-type: none"> Set the SUT power source to AC+DC. Bring the SUT to the base state of S0/MeOn (CM0,CM0-PG), and confirm that the Host OS is available. Verify that a DC battery is connected to the SUT, and that it is charged. Set the SUT power source to DC-only. Set the active power package on the SUT to Power Package 2 (Intel® ME on in S0, wake in Sx/AC). Set the Intel® AMT WLAN link policy on the SUT to Link Policy 3 (Enabled in S0, Sx/AC), if the WLAN network interface is available. Verify that Intel® AMT on the SUT responds to version queries via all available network interfaces. Ensure yellow bang is not seen on Drivers in Device Manager 	
Procedure:	<ol style="list-style-type: none"> Perform a warm reset of the SUT via Host OS graceful restart. Verify that the SUT is in S0/MeOn (CM0,CM0-PG). Verify that Intel® AMT on the SUT responds to version queries via all available network interfaces. Verify that the second nibble of the FWSTS2 register on the SUT have a value of 0x69xxxxxx. Ensure yellow bang is not seen on Drivers in Device Manager 	
Pass Criteria:	The test passes if: <ul style="list-style-type: none"> the SUT is reset to S0. the Intel® CSME is available in MeOn (CM0, CM0-PG). Intel® AMT responds to version queries via all available network interfaces. 	

ID:	ME_PM_26.12	
Title:	S0/CM0 to S0/CM0 via Host OS restart (AC+DC, AC-only/PP2/LP3)	
Requirement:	Mandatory	Exemptions None
Method:	Automated by Intel® PETS	
Objective:	This test checks the SUT power flow from S0/CM0 to S0/CM0 via Host OS restart with the parameters outlined below.	
Configuration:	Intel® AMT should be provisioned via manual mode. This test assumes that either LAN-only, WLAN-only, or both LAN and WLAN network interfaces are available on the SUT.	
Parameters:	System Power Source	AC+DC or AC-only
	Power States	Initial S0/MeOn (CM0, CM0-PG)
		Final S0/MeOn (CM0, CM0-PG)
		Trigger Host OS restart
	Intel® AMT	Power Package PP2 (Intel® ME on in S0, wake in Sx/AC) WLAN Link Policy LP3 (Enabled in S0, Sx/AC) where available



ID:	ME_PM_26.12
Setup:	<ol style="list-style-type: none"> 1. Set the SUT power source to AC+DC where supported; otherwise AC-only. 2. Bring the SUT to the base state of S0/MeOn (CM0,CM0-PG), and confirm that the Host OS is available. 3. Set the active power package on the SUT to Power Package 2 (Intel® ME on in S0, wake in Sx/AC). 4. Set the Intel® AMT WLAN link policy on the SUT to Link Policy 3 (Enabled in S0, Sx/AC), if the WLAN network interface is available. 5. Verify that Intel® AMT on the SUT responds to version queries via all available network interfaces. 6. Ensure yellow bang is not seen on Drivers in Device Manager
Procedure:	<ol style="list-style-type: none"> 1. Perform a warm reset of the SUT via Host OS graceful restart. 2. Verify that the SUT is in S0/MeOn (CM0,CM0-PG). 3. Verify that Intel® AMT on the SUT responds to version queries via all available network interfaces. 4. Verify that the second nibble of the FWSTS2 register on the SUT have a value of 0x69xxxxxx. 5. Ensure yellow bang is not seen on Drivers in Device Manager
Pass Criteria:	<p>The test passes if:</p> <ul style="list-style-type: none"> • the SUT is reset to S0. • the Intel® CSME is available in MeOn (CM0, CM0-PG). • Intel® AMT responds to version queries via all available network interfaces.

ID:	ME_PM_26.13	
Title:	S0/CM0 to S0/CM0 via CF9 Warm Reset (AC+DC, AC-only/PP2/LP3)	
Requirement:	Mandatory	Exemptions None
Method:	Automated by Intel® PETS	
Objective:	This test checks the SUT power flow from S0/CM0 to S0/CM0 via CF9 Warm Reset with the parameters outlined below.	
Configuration:	<p>Intel® AMT should be provisioned via manual mode.</p> <p>This test assumes that either LAN-only, WLAN-only, or both LAN and WLAN network interfaces are available on the SUT.</p>	
Parameters:	System Power Source AC+DC or AC-only	
	Power States	Initial S0/MeOn (CM0, CM0-PG)
		Final S0/MeOn (CM0, CM0-PG)
		Trigger CF9 Warm Reset
	Intel® AMT	Power Package PP2 (Intel® ME on in S0, wake in Sx/AC)
		WLAN Link Policy LP3 (Enabled in S0, Sx/AC) where available
Setup:	<ol style="list-style-type: none"> 1. Set the SUT power source to AC+DC where supported; otherwise AC-only. 2. Bring the SUT to the base state of S0/MeOn (CM0,CM0-PG), and confirm that the Host OS is available. 3. Set the active power package on the SUT to Power Package 2 (Intel® ME on in S0, wake in Sx/AC). 4. Set the Intel® AMT WLAN link policy on the SUT to Link Policy 3 (Enabled in S0, Sx/AC), if the WLAN network interface is available. 5. Record the Host OS last boot time on the SUT (to verify reset execution). 6. Verify that Intel® AMT on the SUT responds to version queries via all available network interfaces. 7. Ensure yellow bang is not seen on Drivers in Device Manager 	



ID:	ME_PM_26.13
Procedure:	<ol style="list-style-type: none"> 1. Ensure that CF9h Global Reset (CF9GR) is cleared to 0b. 2. Perform a Warm reset of the SUT by writing 6h to I/O register CF9h. 3. Verify that the SUT is in S0/MeOn (CM0,CM0-PG). 4. Wait 2 minutes before proceeding if the WLAN network interface is available. Because the Host OS may boot to error recovery screen following unexpected shutdown, the Host OS WLAN driver may not become available immediately. This delay allows enough time for Intel® AMT firmware to take control over the WLAN hardware and respond to manageability requests. 5. Verify that Intel® AMT on the SUT responds to version queries via all available network interfaces. 6. Verify the Host OS last boot time on the SUT does not match the boot time recorded before reset, or that the Host OS is unavailable. 7. Ensure yellow bang is not seen on Drivers in Device Manager
Pass Criteria:	<p>The test passes if:</p> <ul style="list-style-type: none"> • the SUT is reset to S0. • the Intel® CSME is available in MeOn (CM0, CM0-PG). • Intel® AMT responds to version queries via all available network interfaces. • the Host OS last boot time does not match, or the Host OS is unavailable.

12.30 ME_PM_27: S0/CM0 or Sx/Mx to G3

ID:	ME_PM_27.1		
Title:	S0/CM0 to G3/CM-Off via Power loss (AC+DC, AC-only/PP1/LP2)		
Requirement:	Mandatory	Exemptions	None
Method:	Automated by Intel® PETS		
Objective:	This test checks the SUT power flow from S0/CM0 to G3/CM-Off via Power loss with the parameters outlined below.		
Configuration:	Intel® AMT should be provisioned via manual mode. This test assumes that either LAN-only, WLAN-only, or both LAN and WLAN network interfaces are available on the SUT.		
Parameters:	System Power Source		AC+DC or AC-only
	Power States	Initial	S0/MeOn (CM0, CM0-PG)
		Final	G3/MeOff (CM-Off)
		Trigger	Power loss
	Intel® AMT	Power Package	PP1 (Intel® ME on in S0)
WLAN Link Policy		LP2 (Enabled in S0) where available	
Setup:	1. Set the SUT power source to AC+DC where supported; otherwise AC-only . 2. Bring the SUT to the base state of S0/MeOn (CM0,CM0-PG), and confirm that the Host OS is available. 3. Set the active power package on the SUT to Power Package 1 (Intel® ME on in S0). 4. Set the Intel® AMT WLAN link policy on the SUT to Link Policy 2 (Enabled in S0), if the WLAN network interface is available. 5. Verify that Intel® AMT on the SUT responds to version queries via all available network interfaces.		
Procedure:	1. Remove power from the SUT via AC-detach, and if necessary also via DC-detach. Wait for 10 seconds before continuing to allow full power drain from the SUT. 2. Verify that the SUT is in G3/MeOff (CM-Off).		
Pass Criteria:	The test passes if the SUT moves from S0 to G3, and the Intel® CSME moves to MeOff (CM-Off).		



ID:	ME_PM_27.2	
Title:	S0/CM0 to G3/CM-Off via Power loss (AC+DC, AC-only/PP2/LP3)	
Requirement:	Mandatory	Exemptions None
Method:	Automated by Intel® PETS	
Objective:	This test checks the SUT power flow from S0/CM0 to G3/CM-Off via Power loss with the parameters outlined below.	
Configuration:	Intel® AMT should be provisioned via manual mode. This test assumes that either LAN-only, WLAN-only, or both LAN and WLAN network interfaces are available on the SUT.	
Parameters:	System Power Source AC+DC or AC-only	
	Power States	Initial S0/MeOn (CM0, CM0-PG)
		Final G3/MeOff (CM-Off)
		Trigger Power loss
	Intel® AMT	Power Package PP2 (Intel® ME on in S0, wake in Sx/AC)
		WLAN Link Policy LP3 (Enabled in S0, Sx/AC) where available
Setup:	<ol style="list-style-type: none"> 1. Set the SUT power source to AC+DC where supported; otherwise AC-only. 2. Bring the SUT to the base state of S0/MeOn (CM0,CM0-PG), and confirm that the Host OS is available. 3. Set the active power package on the SUT to Power Package 2 (Intel® ME on in S0, wake in Sx/AC). 4. Set the Intel® AMT WLAN link policy on the SUT to Link Policy 3 (Enabled in S0, Sx/AC), if the WLAN network interface is available. 5. Verify that Intel® AMT on the SUT responds to version queries via all available network interfaces. 	
Procedure:	<ol style="list-style-type: none"> 1. Remove power from the SUT via AC-detach, and if necessary also via DC-detach. Wait for 10 seconds before continuing to allow full power drain from the SUT. 2. Verify that the SUT is in G3/MeOff (CM-Off). 	
Pass Criteria:	The test passes if the SUT moves from S0 to G3, and the Intel® CSME moves to MeOff (CM-Off).	

ID:	ME_PM_27.3	
Title:	S5/CM3 to G3/CM-Off via Power loss after Host OS shutdown (AC+DC, AC-only/PP2/LP3)	
Requirement:	Mandatory	Exemptions None
Method:	Automated by Intel® PETS	
Objective:	This test checks the SUT power flow from S5/CM3 to G3/CM-Off via Power loss after Host OS shutdown with the parameters outlined below.	
Configuration:	Intel® AMT should be provisioned via manual mode. This test assumes that either LAN-only, WLAN-only, or both LAN and WLAN network interfaces are available on the SUT.	
Parameters:	System Power Source AC+DC or AC-only	
	Power States	Initial S5/CM3
		Final G3/MeOff (CM-Off)
		Trigger Power loss
	Intel® AMT	Power Package PP2 (Intel® ME on in S0, wake in Sx/AC)
		WLAN Link Policy LP3 (Enabled in S0, Sx/AC) where available



ID:	ME_PM_27.3
Setup:	<ol style="list-style-type: none"> 1. Set the SUT power source to AC+DC where supported; otherwise AC-only. 2. Bring the SUT to the base state of S0/MeOn (CM0,CM0-PG), and confirm that the Host OS is available. 3. Set the active power package on the SUT to Power Package 2 (Intel® ME on in S0, wake in Sx/AC). 4. Set the Intel® AMT WLAN link policy on the SUT to Link Policy 3 (Enabled in S0, Sx/AC), if the WLAN network interface is available. 5. Verify that Intel® AMT on the SUT responds to version queries via all available network interfaces. 6. Shutdown the SUT via the Host OS. 7. Verify that the SUT is in S5/MeOn (CM3). 8. Verify that Intel® AMT on the SUT responds to version queries via all available network interfaces.
Procedure:	<ol style="list-style-type: none"> 1. Remove power from the SUT via AC-detach, and if necessary also via DC-detach. Wait for 10 seconds before continuing to allow full power drain from the SUT. 2. Verify that the SUT is in G3/MeOff (CM-Off).
Pass Criteria:	The test passes if the SUT moves from S5 to G3, and the Intel® CSME moves to MeOff (CM-Off).

12.31 ME_PM_44: S0/CM0-PG, CM0 to S4-S5/CM-Off

ID:	ME_PM_44.3		
Title:	S0/CM0-PG to S4/CM-Off via Host OS hibernate (DC-only)		
Requirement:	Mandatory	Exemptions	<input checked="" type="checkbox"/> Non-Mobile (AC-only) systems <input checked="" type="checkbox"/> Systems with a LAN-only network interface
Method:	Automated by Intel® PETS with potential Test Operator Interaction.		
Objective:	This test checks the SUT power flow from S0/CM0-PG to S4/CM-Off via Host OS hibernate with the parameters outlined below.		
Configuration:	Intel® AMT should not be provisioned. If Deep S4, Deep S5, and/or G3 are supported on the SUT, please confirm the following: <ul style="list-style-type: none"> • the SUT and/or BIOS are properly configured to permit Deep S4/S5 or G3 entry. • the correct Deep Sx policy is applied to the SUT profile in Intel® PETS. This test assumes that either WLAN-only, or both LAN and WLAN network interfaces are available on the SUT.		
Parameters:	System Power Source		DC-only
	Power States	Initial	S0/MeOn (CM0-PG)
		Final	S4, S5, Deep S4, Deep S5, G3/MeOff (CM-Off)
		Trigger	Host OS hibernate
	Intel® AMT	Power Package WLAN Link Policy	[Intel® AMT is not provisioned.]



ID:	ME_PM_44.3
Setup:	<ol style="list-style-type: none"> 1. Set the SUT power source to AC+DC. 2. Bring the SUT to the base state of S0/MeOn (CM0,CM0-PG), and confirm that the Host OS is available. 3. Verify that a DC battery is connected to the SUT, and that it is charged. 4. Set the SUT power source to DC-only. 5. Ensure that Intel® AMT on the SUT is not provisioned. 6. Ensure that the Host OS is configured to not sleep on either AC or DC power. 7. Ensure that the Host OS network device drivers are configured to not wake the SUT. This includes enabling ARP and/or NS Offload features where available to help prevent unexpected host wake events. 8. Verify that the Host OS on the SUT is available. 9. If the SUT supports LAN connectivity, Test Operator Interaction required to disconnect the LAN cable. The Intel® ME cannot move to a power gated state while the LAN is physically connected. 10. Check that Intel® ME is in CM0-PG state for more than 50% within a time interval of 1 minute 11. Verify that the SUT is in S0/MeOn (CM0-PG).
Procedure:	<ol style="list-style-type: none"> 1. Hibernate the SUT via the Host OS. 2. Verify that the SUT is in S4, S5, Deep S4, Deep S5, G3/MeOff (CM-Off). 3. If the SUT supports LAN connectivity, Test Operator Interaction required to reconnect the LAN cable.
Pass Criteria:	The test passes if the SUT moves to S4, S5, Deep S4, Deep S5, or G3, and the Intel® CSME moves to MeOff (CM-Off).

ID:	ME_PM_44.4		
Title:	S0/CM0-PG to S4/CM-Off via Host OS hibernate (AC+DC, AC-only)		
Requirement:	Mandatory	Exemptions	<input checked="" type="checkbox"/> Systems with a LAN-only network interface
Method:	Automated by Intel® PETS with potential Test Operator Interaction		
Objective:	This test checks the SUT power flow from S0/CM0-PG to S4/CM-Off via Host OS hibernate with the parameters outlined below.		
Configuration:	Intel® AMT should not be provisioned. If Deep S4, Deep S5, and/or G3 are supported on the SUT, please confirm the following: <ul style="list-style-type: none">the SUT and/or BIOS are properly configured to permit Deep S4/S5 or G3 entry.the correct Deep Sx policy is applied to the SUT profile in Intel® PETS. This test assumes that either WLAN-only, or both LAN and WLAN network interfaces are available on the SUT.		
Parameters:	System Power Source		AC+DC or AC-only
	Power States	Initial	S0/MeOn (CM0-PG)
		Final	S4, S5, Deep S4, Deep S5, G3/MeOff (CM-Off)
		Trigger	Host OS hibernate
	Intel® AMT	Power Package	[Intel® AMT is not provisioned.]
WLAN Link Policy			
Setup:	<ol style="list-style-type: none">Set the SUT power source to AC+DC where supported; otherwise AC-only.Bring the SUT to the base state of S0/MeOn (CM0,CM0-PG), and confirm that the Host OS is available.Ensure that Intel® AMT on the SUT is not provisioned.Ensure that the Host OS is configured to not sleep on either AC (or DC, where available) power source configuration.Ensure that the Host OS network device drivers are configured to not wake the SUT. This includes enabling ARP and/or NS Offload features where available to help prevent unexpected host wake events.Verify that the Host OS on the SUT is available.If the SUT supports LAN connectivity, Test Operator Interaction required to disconnect the LAN cable. The Intel® ME cannot move to a power gated state while the LAN is physically connected.Check that Intel® ME is in CM0-PG state for more than 50% within a time interval of 1 minuteVerify that the SUT is in S0/MeOn (CM0-PG).		



ID:	ME_PM_44.4
Procedure:	<ol style="list-style-type: none"> 1. Hibernate the SUT via the Host OS. 2. Verify that the SUT is in S4, S5, Deep S4, Deep S5, G3/MeOff (CM-Off). 3. If the SUT supports LAN connectivity, Test Operator Interaction required to reconnect the LAN cable.
Pass Criteria:	The test passes if the SUT moves to S4, S5, Deep S4, Deep S5, or G3, and the Intel® CSME moves to MeOff (CM-Off).

ID:	ME_PM_44.5		
Title:	S0/CM0-PG to S5/CM-Off via Host OS shutdown (DC-only)		
Requirement:	Mandatory	Exemptions	<input checked="" type="checkbox"/> Non-Mobile (AC-only) systems <input checked="" type="checkbox"/> Systems with a LAN-only network interface
Method:	Automated by Intel® PETS with potential Test Operator Interaction		
Objective:	This test checks the SUT power flow from S0/CM0-PG to S5/CM-Off via Host OS shutdown with the parameters outlined below.		
Configuration:	Intel® AMT should not be provisioned. If Deep S5 and/or G3 are supported on the SUT, please confirm the following: <ul style="list-style-type: none"> • the SUT and/or BIOS are properly configured to permit Deep S5 or G3 entry. • the correct Deep Sx policy is applied to the SUT profile in Intel® PETS. This test assumes that either WLAN-only, or both LAN and WLAN network interfaces are available on the SUT.		
Parameters:	System Power Source		DC-only
	Power States	Initial	S0/MeOn (CM0-PG)
		Final	S5, Deep S5, G3/MeOff (CM-Off)
		Trigger	Host OS shutdown
	Intel® AMT	Power Package WLAN Link Policy	[Intel® AMT is not provisioned.]
Setup:	<ol style="list-style-type: none"> 1. Set the SUT power source to AC+DC. 2. Bring the SUT to the base state of S0/MeOn (CM0,CM0-PG), and confirm that the Host OS is available. 3. Verify that a DC battery is connected to the SUT, and that it is charged. 4. Set the SUT power source to DC-only. 5. Ensure that Intel® AMT on the SUT is not provisioned. 6. Ensure that the Host OS is configured to not sleep on either AC or DC power. 7. Ensure that the Host OS network device drivers are configured to not wake the SUT. This includes enabling ARP and/or NS Offload features where available to help prevent unexpected host wake events. 8. Verify that the Host OS on the SUT is available. 9. If the SUT supports LAN connectivity, Test Operator Interaction required to disconnect the LAN cable. The Intel® ME cannot move to a power gated state while the LAN is physically connected. 10. Check that Intel® ME is in CM0-PG state for more than 50% within a time interval of 1 minute 11. Verify that the SUT is in S0/MeOn (CM0-PG). 		
Procedure:	<ol style="list-style-type: none"> 1. Check that Intel® ME is in CM0-PG state for more than 50% within a time interval of 1 minute 2. Verify that the SUT is in S5, Deep S5, G3/MeOff (CM-Off). 3. If the SUT supports LAN connectivity, Test Operator Interaction required to reconnect the LAN cable. 		
Pass Criteria:	The test passes if the SUT moves to S5 (or Deep S5 or G3), and the Intel® CSME moves to MeOff (CM-Off).		



ID:	ME_PM_44.6	
Title:	S0/CM0-PG to S5/CM-Off via Host OS shutdown (AC+DC, AC-only)	
Requirement:	Mandatory	Exemptions <input checked="" type="checkbox"/> Systems with a LAN-only network interface
Method:	Automated by Intel® PETS with potential Test Operator Interaction	
Objective:	This test checks the SUT power flow from S0/CM0-PG to S5/CM-Off via Host OS shutdown with the parameters outlined below.	
Configuration:	Intel® AMT should not be provisioned. If Deep S5 and/or G3 are supported on the SUT, please confirm the following: <ul style="list-style-type: none">the SUT and/or BIOS are properly configured to permit Deep S5 or G3 entry.the correct Deep Sx policy is applied to the SUT profile in Intel® PETS. This test assumes that either WLAN-only, or both LAN and WLAN network interfaces are available on the SUT.	
Parameters:	System Power Source AC+DC or AC-only	
	Power States	Initial S0/MeOn (CM0-PG)
		Final S5, Deep S5, G3/MeOff (CM-Off)
		Trigger Host OS shutdown
	Intel® AMT	Power Package [Intel® AMT is not provisioned.]
		WLAN Link Policy
Setup:	<ol style="list-style-type: none">Set the SUT power source to AC+DC where supported; otherwise AC-only.Bring the SUT to the base state of S0/MeOn (CM0,CM0-PG), and confirm that the Host OS is available.Ensure that Intel® AMT on the SUT is not provisioned.Ensure that the Host OS is configured to not sleep on either AC (or DC, where available) power source configuration.Ensure that the Host OS network device drivers are configured to not wake the SUT. This includes enabling ARP and/or NS Offload features where available to help prevent unexpected host wake events.Verify that the Host OS on the SUT is available.If the SUT supports LAN connectivity, Test Operator Interaction required to disconnect the LAN cable. The Intel® ME cannot move to a power gated state while the LAN is physically connected.Check that Intel® ME is in CM0-PG state for more than 50% within a time interval of 1 minuteVerify that the SUT is in S0/MeOn (CM0-PG).	
Procedure:	<ol style="list-style-type: none">Shutdown the SUT via the Host OS.Verify that the SUT is in S5, Deep S5, G3/MeOff (CM-Off).If the SUT supports LAN connectivity, Test Operator Interaction required to reconnect the LAN cable.	
Pass Criteria:	The test passes if the SUT moves to S5 (or Deep S5 or G3), and the Intel® CSME moves to MeOff (CM-Off).	

ID:	ME_PM_44.7	
Title:	S0/CM0 to S5/CM-Off via Host OS shutdown (AC+DC, AC-only/PP1/LP1)	
Requirement:	Mandatory	Exemptions <input checked="" type="checkbox"/> Systems with a WLAN-only network interface
Method:	Automated by Intel® PETS with potential Test Operator Interaction	
Objective:	This test checks the SUT power flow from S0/CM0 to S5/CM-Off via Host OS shutdown with the parameters outlined below.	
Configuration:	Intel® AMT should not be provisioned. If Deep S5 and/or G3 are supported on the SUT, please confirm the following: <ul style="list-style-type: none">the SUT and/or BIOS are properly configured to permit Deep S5 or G3 entry.the correct Deep Sx policy is applied to the SUT profile in Intel® PETS. This test assumes that either LAN-only, or both LAN and WLAN network interfaces are available on the SUT.	



ID:	ME_PM_44.7	
Parameters:	System Power Source	AC+DC or AC-only
	Power States	Initial S0/MeOn (CM0)
		Final S5, Deep S5, G3/MeOff (CM-Off)
		Trigger Host OS shutdown
	Intel® AMT	Power Package PP1 (Intel® ME on in S0)
		WLAN Link Policy LP1 (Disabled) where available
Setup:	<ol style="list-style-type: none"> 1. Set the SUT power source to AC+DC where supported; otherwise AC-only. 2. Bring the SUT to the base state of S0/MeOn (CM0), and confirm that the Host OS is available. 3. Ensure that Intel® AMT on the SUT is provisioned. 4. Set the active power package on the SUT to Power Package 1 (Intel® ME on in S0). 5. Set the Intel® AMT WLAN link policy on the SUT to Link Policy 1 (Disabled), if the WLAN network interface is available. 6. Ensure that the Host OS is configured to not sleep on either AC (or DC, where available) power source configuration. 7. Ensure that the Host OS network device drivers are configured to not wake the SUT. This includes enabling ARP and/or NS Offload features where available to help prevent unexpected host wake events. 8. Verify that the Host OS on the SUT is available. 9. Wait for 3 minutes to allow the Intel® ME on the SUT to move to CM0-PG (as if it were allowed to enter the PG state). 10. Verify that the SUT is in S0/MeOn (CM0). 	
Procedure:	<ol style="list-style-type: none"> 1. Shutdown the SUT via the Host OS. 2. Verify that the SUT is in S5, Deep S5, G3/MeOff (CM-Off). 	
Pass Criteria:	The test passes if the SUT moves to S5 (or Deep S5 or G3), and the Intel® CSME moves to MeOff (CM-Off).	

12.32 ME_PM_45: G3 or S4–S5/CM-Off to S0/CM0-PG, CM0

ID:	ME_PM_45.3	
Title:	S4/CM-Off to S0/CM0-PG via Power Button press (DC-only)	
Requirement:	Mandatory	Exemptions <ul style="list-style-type: none"> <input checked="" type="checkbox"/> Non-Mobile (AC-only) systems <input checked="" type="checkbox"/> Systems with a LAN-only network interface
Method:	Automated by Intel® PETS with potential Test Operator Interaction	
Objective:	This test checks the SUT power flow from S4/CM-Off to S0/CM0-PG via Power Button press with the parameters outlined below.	
Configuration:	<p>Intel® AMT should not be provisioned.</p> <p>If Deep S4, Deep S5, and/or G3 are supported on the SUT, please confirm the following:</p> <ul style="list-style-type: none"> the SUT and/or BIOS are properly configured to permit Deep S4/S5 or G3 entry. the correct Deep Sx policy is applied to the SUT profile in Intel® PETS. <p>This test assumes that either WLAN-only, or both LAN and WLAN network interfaces are available on the SUT.</p>	
Parameters:	System Power Source	DC-only
	Power States	Initial S4, S5, Deep S4, Deep S5, G3/MeOff (CM-Off)
		Final S0/MeOn (CM0-PG)
		Trigger Power Button press
	Intel® AMT	[Intel® AMT is not provisioned.]



ID:	ME_PM_45.3
Setup:	<ol style="list-style-type: none"> 1. Set the SUT power source to AC+DC. 2. Bring the SUT to the base state of S0/MeOn (CM0,CM0-PG), and confirm that the Host OS is available. 3. Verify that a DC battery is connected to the SUT, and that it is charged. 4. Set the SUT power source to DC-only. 5. Ensure that Intel® AMT on the SUT is not provisioned. 6. Ensure that the Host OS is configured to not sleep on either AC or DC power. 7. Ensure that the Host OS network device drivers are configured to not wake the SUT. This includes enabling ARP and/or NS Offload features where available to help prevent unexpected host wake events. 8. Verify that the Host OS on the SUT is available. 9. If the SUT supports LAN connectivity, Test Operator Interaction required to disconnect the LAN cable. The Intel® ME cannot move to a power gated state while the LAN is physically connected. 10. Ensure yellow bang is not seen on Drivers in Device Manager 11. Hibernate the SUT via the Host OS. 12. Verify that the SUT is in S4, S5, Deep S4, Deep S5, G3/MeOff (CM-Off).
Procedure:	<ol style="list-style-type: none"> 1. Briefly press the Power Button on the SUT. 2. Verify that the SUT is in S0. 3. Verify that the Host OS on the SUT is available. 4. Check that Intel® ME is in CM0-PG state for more than 50% within a time interval of 1 minute 5. Verify that the SUT is in S0/MeOn (CM0-PG). 6. Verify that windows booted from hibernate i.e. value should be 0x02. "run the following power shell command": Get-WinEvent -ProviderName Microsoft-Windows-Kernel-boot -MaxEvents 10 Where-Object {\$_.message -like "The boot type*"} 7. If the SUT supports LAN connectivity, Test Operator Interaction required to reconnect the LAN cable. 8. Ensure yellow bang is not seen on Drivers in Device Manager
Pass Criteria:	The test passes if the SUT moves from S4, S5, Deep S4, Deep S5, or G3 to S0, and the Intel® CSME moves to MeOn (CM0-PG).

ID:	ME_PM_45.4	
Title:	S4/CM-Off to S0/CM0-PG via magic packet (AC+DC, AC-only)	
Requirement:	Mandatory	Exemptions <ul style="list-style-type: none"> <input checked="" type="checkbox"/> Systems without WoL and/or WoWLAN support <input checked="" type="checkbox"/> Systems with a LAN-only network interface
Method:	Automated by Intel® PETS with potential Test Operator Interaction	
Objective:	This test checks the SUT power flow from S4/CM-Off to S0/CM0-PG via magic packet with the parameters outlined below.	
Configuration:	<p>Intel® AMT should not be provisioned.</p> <p>If Deep S4, Deep S5, and/or G3 are supported on the SUT, please confirm the following:</p> <ul style="list-style-type: none"> the SUT and/or BIOS are properly configured to permit Deep S4/S5 or G3 entry. the correct Deep Sx policy is applied to the SUT profile in Intel® PETS. <p>This test assumes that either WLAN-only, or both LAN and WLAN network interfaces are available on the SUT. Where both network interfaces are available, LAN is the initial active network interface in the test, and WLAN is the secondary network interface.</p>	
Parameters:	System Power Source AC+DC or AC-only	
	Power States	Initial S4, S5, Deep S4, Deep S5, G3/MeOff (CM-Off)
		Final S0/MeOn (CM0-PG)
		Trigger Magic Packet receipt
	Intel® AMT	Power Package WLAN Link Policy <p>[Intel® AMT is not provisioned.]</p>



ID:	ME_PM_45.4
Setup:	<ol style="list-style-type: none"> 1. Set the SUT power source to AC+DC where supported; otherwise AC-only. 2. Bring the SUT to the base state of S0/MeOn (CM0,CM0-PG), and confirm that the Host OS is available. 3. Ensure that Intel® AMT on the SUT is not provisioned. 4. Ensure that the Host OS is configured to not sleep on either AC (or DC, where available) power source configuration. 5. Ensure that, where available, only the Host OS Wake on LAN and/or Wake on Wireless LAN driver setting(s) are enabled on the SUT. All other network wake sources must be disabled. This includes enabling ARP and/or NS Offload features where available to help prevent unexpected host wake events. 6. Verify that the Host OS on the SUT is available. 7. If the SUT supports LAN connectivity, Test Operator Interaction required to disconnect the LAN cable. The Intel® ME cannot move to a power gated state while the LAN is physically connected. 8. Ensure yellow bang is not seen on Drivers in Device Manager
Procedure:	<ol style="list-style-type: none"> 1. Hibernate the SUT via the Host OS. 2. Verify that the SUT is in S4, S5, Deep S4, Deep S5, G3/MeOff (CM-Off). 3. Send three magic packets, at 2 second intervals, by means of the active network interface. 4. Verify that the SUT is in S0. 5. Verify that the Host OS on the SUT is available. 6. Check that Intel® ME is in CM0-PG state for more than 50% within a time interval of 1 minute 7. Verify that the SUT is in S0/MeOn (CM0-PG). 8. Verify that windows booted from hibernate i.e. value should be 0x02. "run the following power shell command": Get-WinEvent -ProviderName Microsoft-Windows-Kernel-boot -MaxEvents 10 Where-Object {\$_.message -like "The boot type*"} 9. If the SUT supports LAN connectivity, Test Operator Interaction required to reconnect the LAN cable. 10. Ensure yellow bang is not seen on Drivers in Device Manager
Pass Criteria:	The test passes if the SUT moves from S4, S5, Deep S4, Deep S5, or G3 to S0, and the Intel® CSME moves to MeOn (CM0-PG).



ID:	ME_PM_45.5		
Title:	S5/CM-Off to S0/CM0-PG via Power Button press (DC-only)		
Requirement:	Mandatory	Exemptions	<input checked="" type="checkbox"/> Non-Mobile (AC-only) systems
			<input checked="" type="checkbox"/> Systems with a LAN-only network interface
Method:	Automated by Intel® PETS with potential Test Operator Interaction		
Objective:	This test checks the SUT power flow from S5/CM-Off to S0/CM0-PG via Power Button press with the parameters outlined below.		
Configuration:	Intel® AMT should not be provisioned. If Deep S5 and/or G3 are supported on the SUT, please confirm the following: <ul style="list-style-type: none">the SUT and/or BIOS are properly configured to permit Deep S5 or G3 entry.the correct Deep Sx policy is applied to the SUT profile in Intel® PETS. This test assumes that either WLAN-only, or both LAN and WLAN network interfaces are available on the SUT.		
Parameters:	System Power Source		DC-only
	Power States	Initial	S5, Deep S5, G3/MeOff (CM-Off)
		Final	S0/MeOn (CM0-PG)
		Trigger	Power Button press
	Intel® AMT	Power Package	[Intel® AMT is not provisioned.]
WLAN Link Policy			
Setup:	<ol style="list-style-type: none">Set the SUT power source to AC+DC.Bring the SUT to the base state of S0/MeOn (CM0,CM0-PG), and confirm that the Host OS is available.Verify that a DC battery is connected to the SUT, and that it is charged.Set the SUT power source to DC-only.Ensure that Intel® AMT on the SUT is not provisioned.Ensure that the Host OS is configured to not sleep on either AC or DC power.Ensure that the Host OS network device drivers are configured to not wake the SUT. This includes enabling ARP and/or NS Offload features where available to help prevent unexpected host wake events.Verify that the Host OS on the SUT is available.If the SUT supports LAN connectivity, Test Operator Interaction required to disconnect the LAN cable. The Intel® ME cannot move to a power gated state while the LAN is physically connected.Ensure yellow bang is not seen on Drivers in Device ManagerShutdown the SUT via the Host OS.Verify that the SUT is in S5, Deep S5, G3/MeOff (CM-Off).		
Procedure:	<ol style="list-style-type: none">Briefly press the Power Button on the SUT.Verify that the SUT is in S0.Verify that the Host OS on the SUT is available.Check that Intel® ME is in CM0-PG state for more than 50% within a time interval of 1 minuteVerify that the SUT is in S0/MeOn (CM0-PG).If the SUT supports LAN connectivity, Test Operator Interaction required to reconnect the LAN cable.Ensure yellow bang is not seen on Drivers in Device Manager		
Pass Criteria:	The test passes if the SUT moves from S5 (or Deep S5 or G3) to S0, and the Intel® CSME moves to MeOn (CM0-PG).		

ID:	ME_PM_45.7	
Title:	G3/CM-Off to S0/CM0-PG via Power Button press (DC-only)	
Requirement:	Mandatory Exemptions	<input checked="" type="checkbox"/> Non-Mobile (AC-only) systems <input checked="" type="checkbox"/> Systems with a LAN-only network interface
Method:	Automated by Intel® PETS with potential Test Operator Interaction	
Objective:	This test checks the SUT power flow from G3/CM-Off to S0/CM0-PG via Power Button press with the parameters outlined below.	



ID:	ME_PM_45.7		
Configuration:	<p>Intel® AMT should not be provisioned.</p> <p>If Deep S5 and/or G3 are supported on the SUT, please confirm the following:</p> <ul style="list-style-type: none">the SUT and/or BIOS are properly configured to permit Deep S5 or G3 entry.the correct Deep Sx policy is applied to the SUT profile in Intel® PETS. <p>This test assumes that either WLAN-only, or both LAN and WLAN network interfaces are available on the SUT.</p>		
Parameters:	System Power Source		DC-only
	Power States	Initial	G3/MeOff (CM-Off)
		Final	S0/MeOn (CM0-PG)
		Trigger	(DC-attach then) Power Button press
	Intel® AMT	Power Package	[Intel® AMT is not provisioned.]
WLAN Link Policy			
Setup:	<ol style="list-style-type: none">Set the SUT power source to AC+DC.Bring the SUT to the base state of S0/MeOn (CM0,CM0-PG), and confirm that the Host OS is available.Verify that a DC battery is connected to the SUT, and that it is charged.Set the SUT power source to DC-only.Ensure that Intel® AMT on the SUT is not provisioned.Ensure that the Host OS is configured to not sleep on either AC or DC power.Ensure that the Host OS network device drivers are configured to not wake the SUT. This includes enabling ARP and/or NS Offload features where available to help prevent unexpected host wake events.Verify that the Host OS on the SUT is available.If the SUT supports LAN connectivity, Test Operator Interaction required to disconnect the LAN cable. The Intel® ME cannot move to a power gated state while the LAN is physically connected.Ensure yellow bang is not seen on Drivers in Device ManagerShutdown the SUT via the Host OS.Verify that the SUT is in S5, Deep S5, G3/MeOff (CM-Off).Remove power from the SUT via DC-detach. Wait for 10 seconds before continuing to allow full power drain from the SUT.Verify that the SUT is in G3/MeOff (CM-Off).		
Procedure:	<ol style="list-style-type: none">Set the SUT power source to DC-only.Briefly press the Power Button on the SUT.Verify that the SUT is in S0.Verify that the Host OS on the SUT is available.Check that Intel® ME is in CM0-PG state for more than 50% within a time interval of 1 minuteVerify that the SUT is in S0/MeOn (CM0-PG).If the SUT supports LAN connectivity, Test Operator Interaction required to reconnect the LAN cable.Ensure yellow bang is not seen on Drivers in Device Manager		
Pass Criteria:	The test passes if the SUT moves from G3 through S5 (or Deep S5 or G3) to S0, and the Intel® CSME moves to MeOn (CM0-PG).		

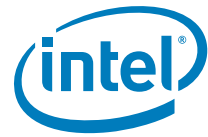
12.33 ME_PM_46: S0/CM0-PG, CM0 to S0/CM0-PG, CM0

ID:	ME_PM_46.1		
Title:	S0/CM0-PG to S0/CM0-PG via Host OS restart (DC-only)		
Requirement:	Mandatory	Exemptions	<input checked="" type="checkbox"/> Non-Mobile (AC-only) systems <input checked="" type="checkbox"/> Systems with a LAN-only network interface
Method:	Automated by Intel® PETS with potential Test Operator Interaction		
Objective:	This test checks the SUT power flow from S0/CM0-PG to S0/CM0-PG via Host OS restart with the parameters outlined below.		



ID:	ME_PM_46.1		
Configuration:	Intel® AMT should not be provisioned. This test assumes that either WLAN-only, or both LAN and WLAN network interfaces are available on the SUT.		
Parameters:	System Power Source		DC-only
	Power States	Initial	S0/MeOn (CM0-PG)
		Final	S0/MeOn (CM0-PG)
		Trigger	Host OS restart
	Intel® AMT	Power Package WLAN Link Policy	[Intel® AMT is not provisioned.]
Setup:	<ol style="list-style-type: none"> Set the SUT power source to AC+DC. Bring the SUT to the base state of S0/MeOn (CM0,CM0-PG), and confirm that the Host OS is available. Verify that a DC battery is connected to the SUT, and that it is charged. Set the SUT power source to DC-only. Ensure that Intel® AMT on the SUT is not provisioned. If SUT is provisioned, we have to unprovision and wait for 3 minutes for RSA key readiness, if SUT is not provisioned, no wait is needed. Ensure that the Host OS is configured to not sleep on either AC or DC power. Verify that the Host OS on the SUT is available. If the SUT supports LAN connectivity, Test Operator Interaction required to disconnect the LAN cable. The Intel® ME cannot move to a power gated state while the LAN is physically connected. Ensure yellow bang is not seen on Drivers in Device Manager Check that Intel® ME is in CM0-PG state for more than 50% within a time interval of 1 minute Verify that the SUT is in S0/MeOn (CM0-PG). 		
Procedure:	<ol style="list-style-type: none"> Perform a warm reset of the SUT via Host OS graceful restart. Verify that the SUT is in S0. Verify that the Host OS on the SUT is available. Check that Intel® ME is in CM0-PG state for more than 50% within a time interval of 1 minute Verify that the SUT is in S0/MeOn (CM0-PG). If the SUT supports LAN connectivity, Test Operator Interaction required to reconnect the LAN cable. Ensure yellow bang is not seen on Drivers in Device Manager 		
Pass Criteria:	The test passes if the SUT is reset to S0, and the Intel® CSME is available in MeOn (CM0-PG).		

ID:	ME_PM_46.2		
Title:	S0/CM0-PG to S0/CM0-PG via Host OS restart (AC+DC, AC-only)		
Requirement:	Mandatory	Exemptions	<input checked="" type="checkbox"/> Systems with a LAN-only network interface
Method:	Automated by Intel® PETS with potential Test Operator Interaction		
Objective:	This test checks the SUT power flow from S0/CM0-PG to S0/CM0-PG via Host OS restart with the parameters outlined below.		
Configuration:	Intel® AMT should not be provisioned. This test assumes that either WLAN-only, or both LAN and WLAN network interfaces are available on the SUT.		
Parameters:	System Power Source		AC+DC or AC-only
	Power States	Initial	S0/MeOn (CM0-PG)
		Final	S0/MeOn (CM0-PG)
		Trigger	Host OS restart
	Intel® AMT	Power Package WLAN Link Policy	[Intel® AMT is not provisioned.]



ID:	ME_PM_46.2
Setup:	<ol style="list-style-type: none"> 1. Set the SUT power source to AC+DC where supported; otherwise AC-only. 2. Bring the SUT to the base state of S0/MeOn (CM0,CM0-PG), and confirm that the Host OS is available. 3. Ensure that Intel® AMT on the SUT is not provisioned. 4. Ensure that the Host OS is configured to not sleep on either AC (or DC, where available) power source configuration. 5. Verify that the Host OS on the SUT is available. 6. If the SUT supports LAN connectivity, Test Operator Interaction required to disconnect the LAN cable. The Intel® ME cannot move to a power gated state while the LAN is physically connected. 7. Ensure yellow bang is not seen on Drivers in Device Manager 8. Check that Intel® ME is in CM0-PG state for more than 50% within a time interval of 1 minute 9. Verify that the SUT is in S0/MeOn (CM0-PG).
Procedure:	<ol style="list-style-type: none"> 1. Perform a warm reset of the SUT via Host OS graceful restart. 2. Verify that the SUT is in S0. 3. Verify that the Host OS on the SUT is available. 4. Check that Intel® ME is in CM0-PG state for more than 50% within a time interval of 1 minute 5. Verify that the SUT is in S0/MeOn (CM0-PG). 6. If the SUT supports LAN connectivity, Test Operator Interaction required to reconnect the LAN cable. 7. Ensure yellow bang is not seen on Drivers in Device Manager
Pass Criteria:	The test passes if the SUT is reset to S0, and the Intel® CSME is available in MeOn (CM0-PG).

ID:	ME_PM_46.3		
Title:	S0/CM0-PG to S0/CM0-PG via CF9 Cold Reset (DC-only)		
Requirement:	Mandatory	Exemptions	<div><input checked="" type="checkbox"/> Non-Mobile (AC-only) systems</div> <div><input checked="" type="checkbox"/> Systems with a LAN-only network interface</div>
Method:	Automated by Intel® PETS with potential Test Operator Interaction		
Objective:	This test checks the SUT power flow from S0/CM0-PG to S0/CM0-PG via CF9 Cold Reset with the parameters outlined below.		
Configuration:	Intel® AMT should not be provisioned. This test assumes that either WLAN-only, or both LAN and WLAN network interfaces are available on the SUT.		
Parameters:	System Power Source		DC-only
	Power States	Initial	S0/MeOn (CM0-PG)
		Final	S0/MeOn (CM0-PG)
		Trigger	CF9 Cold Reset
	Intel® AMT	Power Package	[Intel® AMT is not provisioned.]
WLAN Link Policy			
Setup:	<div><div>1. Set the SUT power source to AC+DC.</div><div>2. Bring the SUT to the base state of S0/MeOn (CM0,CM0-PG), and confirm that the Host OS is available.</div><div>3. Verify that a DC battery is connected to the SUT, and that it is charged.</div><div>4. Set the SUT power source to DC-only.</div><div>5. Ensure that Intel® AMT on the SUT is not provisioned.</div><div>6. Ensure that the Host OS is configured to not sleep on either AC or DC power.</div><div>7. Verify that the Host OS on the SUT is available.</div><div>8. Record the Host OS last boot time on the SUT (to verify reset execution).</div><div>9. If the SUT supports LAN connectivity, Test Operator Interaction required to disconnect the LAN cable. The Intel® ME cannot move to a power gated state while the LAN is physically connected.</div><div>10. Ensure yellow bang is not seen on Drivers in Device Manager</div><div>11. Check that Intel® ME is in CM0-PG state for more than 50% within a time interval of 1 minute</div><div>12. Verify that the SUT is in S0/MeOn (CM0-PG).</div></div>		



ID:	ME_PM_46.3
Procedure:	<ol style="list-style-type: none"> 1. Ensure that CF9h Global Reset (CF9GR) is cleared to 0b. 2. Perform a cold reset of the SUT by writing Eh to I/O register CF9h. 3. Verify that the SUT is in S0. 4. Verify that the Host OS on the SUT is available. 5. Verify the Host OS last boot time on the SUT does not match the boot time recorded before reset. 6. Check that Intel® ME is in CM0-PG state for more than 50% within a time interval of 1 minute 7. Verify that the SUT is in S0/MeOn (CM0-PG). 8. If the SUT supports LAN connectivity, Test Operator Interaction required to reconnect the LAN cable. 9. Ensure yellow bang is not seen on Drivers in Device Manager
Pass Criteria:	<p>The test passes if:</p> <ul style="list-style-type: none"> • the SUT is reset to S0. • and the Intel® CSME is available in MeOn (CM0-PG). • the Host OS last boot time does not match.

ID:	ME_PM_46.4									
Title:	S0/CM0-PG to S0/CM0-PG via CF9 Cold Reset (AC+DC, AC-only)									
Requirement:	Mandatory Exemptions <input checked="" type="checkbox"/> Systems with a LAN-only network interface									
Method:	Automated by Intel® PETS with potential Test Operator Interaction									
Objective:	This test checks the SUT power flow from S0/CM0-PG to S0/CM0-PG via CF9 Cold Reset with the parameters outlined below.									
Configuration:	<p>Intel® AMT should not be provisioned.</p> <p>This test assumes that either WLAN-only, or both LAN and WLAN network interfaces are available on the SUT.</p>									
Parameters:	<table> <tr> <th colspan="2">System Power Source</th></tr> <tr> <td rowspan="3">Power States</td><td>Initial S0/MeOn (CM0-PG)</td></tr> <tr> <td>Final S0/MeOn (CM0-PG)</td></tr> <tr> <td>Trigger CF9 Cold Reset</td></tr> <tr> <td rowspan="2">Intel® AMT</td><td>Power Package [Intel® AMT is not provisioned.]</td></tr> <tr> <td>WLAN Link Policy</td></tr> </table>	System Power Source		Power States	Initial S0/MeOn (CM0-PG)	Final S0/MeOn (CM0-PG)	Trigger CF9 Cold Reset	Intel® AMT	Power Package [Intel® AMT is not provisioned.]	WLAN Link Policy
System Power Source										
Power States	Initial S0/MeOn (CM0-PG)									
	Final S0/MeOn (CM0-PG)									
	Trigger CF9 Cold Reset									
Intel® AMT	Power Package [Intel® AMT is not provisioned.]									
	WLAN Link Policy									
Setup:	<ol style="list-style-type: none"> 1. Set the SUT power source to AC+DC where supported; otherwise AC-only. 2. Bring the SUT to the base state of S0/MeOn (CM0,CM0-PG), and confirm that the Host OS is available. 3. Ensure that Intel® AMT on the SUT is not provisioned. 4. Ensure that the Host OS is configured to not sleep on either AC (or DC, where available) power source configuration. 5. Verify that the Host OS on the SUT is available. 6. Record the Host OS last boot time on the SUT (to verify reset execution). 7. If the SUT supports LAN connectivity, Test Operator Interaction required to disconnect the LAN cable. The Intel® ME cannot move to a power gated state while the LAN is physically connected. 8. Ensure yellow bang is not seen on Drivers in Device Manager 9. Check that Intel® ME is in CM0-PG state for more than 50% within a time interval of 1 minute 10. Verify that the SUT is in S0/MeOn (CM0-PG). 									
Procedure:	<ol style="list-style-type: none"> 1. Ensure that CF9h Global Reset (CF9GR) is cleared to 0b. 2. Perform a cold reset of the SUT by writing Eh to I/O register CF9h. 3. Verify that the SUT is in S0. 4. Verify that the Host OS on the SUT is available. 5. Verify the Host OS last boot time on the SUT does not match the boot time recorded before reset. 6. Check that Intel® ME is in CM0-PG state for more than 50% within a time interval of 1 minute 7. Verify that the SUT is in S0/MeOn (CM0-PG). 8. If the SUT supports LAN connectivity, Test Operator Interaction required to reconnect the LAN cable. 9. Ensure yellow bang is not seen on Drivers in Device Manager 									



ID:	ME_PM_46.4
Pass Criteria:	<p>The test passes if:</p> <ul style="list-style-type: none"> the SUT is reset to S0. the Intel® CSME is available in MeOn (CM0-PG). the Host OS last boot time does not match.

ID:	ME_PM_46.5		
Title:	S0/CM0-PG to S0/CM0-PG via CF9 Global Reset (DC-only)		
Requirement:	Mandatory	Exemptions	<div><input checked="" type="checkbox"/> Non-Mobile (AC-only) systems</div> <div><input checked="" type="checkbox"/> Systems with a LAN-only network interface</div> <div><input checked="" type="checkbox"/> Systems not in Intel® ME manufacturing mode</div>
Method:	Automated by Intel® PETS with potential Test Operator Interaction		
Objective:	This test checks the SUT power flow from S0/CM0-PG to S0/CM0-PG via CF9 Global Reset with the parameters outlined below.		
Configuration:	Intel® AMT should not be provisioned. Intel® ME should be configured in manufacturing mode. Confirm that the BIOS has not set the CF9 Lockdown. This test assumes that either WLAN-only, or both LAN and WLAN network interfaces are available on the SUT.		
Parameters:	System Power Source		DC-only
	Power States	Initial	S0/MeOn (CM0-PG)
		Final	S0/MeOn (CM0-PG)
		Trigger	CF9 Global Reset
	Intel® AMT	Power Package	[Intel® AMT is not provisioned.]
WLAN Link Policy			
Setup:	<div>1. Set the SUT power source to AC+DC.</div> <div>2. Bring the SUT to the base state of S0/MeOn (CM0,CM0-PG), and confirm that the Host OS is available.</div> <div>3. Verify that a DC battery is connected to the SUT, and that it is charged.</div> <div>4. Set the SUT power source to DC-only.</div> <div>5. Ensure that Intel® AMT on the SUT is not provisioned.</div> <div>6. Ensure that the Host OS is configured to not sleep on either AC or DC power.</div> <div>7. Verify that the Host OS on the SUT is available.</div> <div>8. Record the Host OS last boot time on the SUT (to verify reset execution).</div> <div>9. Verify that the Intel® ME is configured in manufacturing mode.</div> <div>10. If the SUT supports LAN connectivity, Test Operator Interaction required to disconnect the LAN cable. The Intel® ME cannot move to a power gated state while the LAN is physically connected.</div> <div>11. Ensure yellow bang is not seen on Drivers in Device Manager</div> <div>12. Check that Intel® ME is in CM0-PG state for more than 50% within a time interval of 1 minute</div> <div>13. Verify that the SUT is in S0/MeOn (CM0-PG).</div> <div>14. Write 1b to CF6GR to enable global Reset.</div>		
Procedure:	<div>1. Ensure that CF9h Global Reset (CF9GR) is set to 1b to enable global reset.</div> <div>2. Perform a global reset of the SUT by writing either 6h or Eh to I/O register CF9h.</div> <div>3. Verify that the SUT is in S0.</div> <div>4. Verify that the Host OS on the SUT is available.</div> <div>5. Verify the Host OS last boot time on the SUT does not match the boot time recorded before reset.</div> <div>6. Check that Intel® ME is in CM0-PG state for more than 50% within a time interval of 1 minute</div> <div>7. Verify that the SUT is in S0/MeOn (CM0-PG).</div> <div>8. If the SUT supports LAN connectivity, Test Operator Interaction required to reconnect the LAN cable.</div> <div>9. Ensure yellow bang is not seen on Drivers in Device Manager</div>		



ID:	ME_PM_46.5
Pass Criteria:	<p>The test passes if:</p> <ul style="list-style-type: none"> the SUT is reset to S0. and the Intel® CSME is available in MeOn (CM0-PG). the Host OS last boot time does not match.

ID:	ME_PM_46.6		
Title:	S0/CM0-PG to S0/CM0-PG via CF9 Global Reset (AC+DC, AC-only)		
Requirement:	Mandatory	Exemptions	<input checked="" type="checkbox"/> Systems with a LAN-only network interface <input checked="" type="checkbox"/> Systems not in Intel® ME manufacturing mode
Method:	Automated by Intel® PETS with potential Test Operator Interaction		
Objective:	This test checks the SUT power flow from S0/CM0-PG to S0/CM0-PG via CF9 Global Reset with the parameters outlined below.		
Configuration:	<p>Intel® AMT should not be provisioned.</p> <p>Intel® ME should be configured in manufacturing mode.</p> <p>Confirm that the BIOS has not set the CF9 Lockdown.</p> <p>This test assumes that either WLAN-only, or both LAN and WLAN network interfaces are available on the SUT.</p>		
Parameters:	System Power Source		AC+DC or AC-only
	Power States	Initial	S0/MeOn (CM0-PG)
		Final	S0/MeOn (CM0-PG)
		Trigger	CF9 Global Reset
	Intel® AMT	Power Package WLAN Link Policy	[Intel® AMT is not provisioned.]
Setup:	<ol style="list-style-type: none"> Set the SUT power source to AC+DC where supported; otherwise AC-only. Bring the SUT to the base state of S0/MeOn (CM0,CM0-PG), and confirm that the Host OS is available. Ensure that Intel® AMT on the SUT is not provisioned. Ensure that the Host OS is configured to not sleep on either AC (or DC, where available) power source configuration. Verify that the Host OS on the SUT is available. Record the Host OS last boot time on the SUT (to verify reset execution). Verify that the Intel® ME is configured in manufacturing mode. If the SUT supports LAN connectivity, Test Operator Interaction required to disconnect the LAN cable. The Intel® ME cannot move to a power gated state while the LAN is physically connected. Ensure yellow bang is not seen on Drivers in Device Manager Check that Intel® ME is in CM0-PG state for more than 50% within a time interval of 1 minute Verify that the SUT is in S0/MeOn (CM0-PG). Write 1b to CF6GR to enable global Reset. 		
Procedure:	<ol style="list-style-type: none"> Ensure that CF9h Global Reset (CF9GR) is set to 1b to enable global reset. Perform a global reset of the SUT by writing either 6h or Eh to I/O register CF9h. Verify that the SUT is in S0. Verify that the Host OS on the SUT is available. Verify the Host OS last boot time on the SUT does not match the boot time recorded before reset. Check that Intel® ME is in CM0-PG state for more than 50% within a time interval of 1 minute Verify that the SUT is in S0/MeOn (CM0-PG). If the SUT supports LAN connectivity, Test Operator Interaction required to reconnect the LAN cable. Ensure yellow bang is not seen on Drivers in Device Manager 		
Pass Criteria:	<p>The test passes if:</p> <ul style="list-style-type: none"> the SUT is reset to S0. and the Intel® CSME is available in MeOn (CM0-PG). the Host OS last boot time does not match. 		



ID:	ME_PM_46.7	
Title:	S0/CM0 to S0/CM0 via Host OS restart (AC+DC, AC-only)	
Requirement:	Mandatory	Exemptions <input checked="" type="checkbox"/> Systems with a WLAN-only network interface
Method:	Automated by Intel® PETS with potential Test Operator Interaction	
Objective:	This test checks the SUT power flow from S0/CM0 to S0/CM0 via Host OS restart with the parameters outlined below.	
Configuration:	Intel® AMT should not be provisioned. This test assumes that either LAN-only, WLAN-only, or both LAN and WLAN network interfaces are available on the SUT.	
Parameters:	System Power Source AC+DC or AC-only	
	Power States	Initial S0/MeOn (CM0)
		Final S0/MeOn (CM0)
		Trigger Host OS restart
	Intel® AMT	Power Package PP1 (Intel® ME on in S0)
		WLAN Link Policy LP1 (Disabled) where available
Setup:	<ol style="list-style-type: none"> Set the SUT power source to AC+DC where supported; otherwise AC-only. Bring the SUT to the base state of S0/MeOn (CM0,CM0-PG), and confirm that the Host OS is available. Ensure that Intel® AMT on the SUT is provisioned. Set the active power package on the SUT to Power Package 1 (Intel® ME on in S0). Set the Intel® AMT WLAN link policy on the SUT to Link Policy 1 (Disabled), if the WLAN network interface is available. Ensure that the Host OS is configured to not sleep on either AC (or DC, where available) power source configuration. Verify that the Host OS on the SUT is available. Ensure yellow bang is not seen on Drivers in Device Manager Wait for 3 minutes to allow the Intel® ME on the SUT to move to CM0-PG (as if it were allowed to enter the PG state). Verify that the SUT is in S0/MeOn (CM0). 	
Procedure:	<ol style="list-style-type: none"> Perform a warm reset of the SUT via Host OS graceful restart. Verify that the SUT is in S0. Verify that the Host OS on the SUT is available. Wait for 3 minutes to allow the Intel® ME on the SUT to move to CM0-PG (as if it were allowed to enter the PG state). Verify that the SUT is in S0/MeOn (CM0). Ensure yellow bang is not seen on Drivers in Device Manager 	
Pass Criteria:	The test passes if the SUT is reset to S0, and the Intel® CSME is available in MeOn (CM0).	

12.34 ME_PM_50: S0/CM0 to Sx/(CM3 or CM-Off) to S0/CM0 via AC Attach

ID:	ME_PM_50.1	
Title:	S0/CM0 to S3/CM3 to S0/CM0 via AC-attach (PP2/LP3)	
Requirement:	Mandatory	Exemptions <input checked="" type="checkbox"/> Non-Mobile (AC-only) systems <input checked="" type="checkbox"/> Modern Standby and InstantGo* systems
Method:	Automated by Intel® PETS	
Objective:	This test checks the SUT power flow from S0/CM0 to S3/CM3 to S0/CM0 via AC-attach with the parameters outlined below.	
Configuration:	This test assumes that either LAN-only, WLAN-only, or both LAN and WLAN network interfaces are available on the SUT.	



ID:	ME_PM_50.1	
Parameters:	System Power Source DC-only	
	Power States	Initial S0/MeOn (CM0)
		Final S0/MeOn (CM0)
		Trigger AC-attach in S3 state
	Intel® AMT	Power Package PP2 (Intel® ME on in S0, wake in Sx/AC)
		WLAN Link Policy LP3 (Enabled in S0, Sx/AC) where available
Setup:	<ol style="list-style-type: none"> Set the SUT power source to AC+DC. Bring the SUT to the base state of S0/MeOn (CM0,CM0-PG), and confirm that the Host OS is available. Verify that a DC battery is connected to the SUT, and that it is charged. Set the SUT power source to DC-only. Set the active power package on the SUT to Power Package 2 (Intel® ME on in S0, wake in Sx/AC). Set the Intel® AMT WLAN link policy on the SUT to Link Policy 3 (Enabled in S0, Sx/AC), if the WLAN network interface is available. Ensure that the Host OS network device drivers are configured to not wake the SUT. This includes enabling ARP and/or NS Offload features where available to help prevent unexpected host wake events. Most especially, ensure that the Host OS Wireless Wake on LAN driver setting on the SUT is disabled, if the WLAN network interface is available. Ensure that Intel® RMT is disabled, if running on an All-in-One (AIO) SUT with feature support. Verify that Intel® AMT on the SUT responds to version queries via all available network interfaces. Record the Host OS last boot time on the SUT (to verify successful return to S3) Ensure yellow bang is not seen on Drivers in Device Manager 	
Procedure:	<ol style="list-style-type: none"> Suspend the SUT via the Host OS. Verify that the SUT is in S3/MeOff (CM-Off). Set the SUT power source to AC+DC Verify that the SUT is in S3/MeOn (CM3). Verify that Intel® AMT on the SUT responds to version queries via all available network interfaces. Briefly press the Power Button on the SUT. Verify that the SUT is in S0/MeOn (CM0,CM0-PG). Verify that the Host OS on the SUT is available. Verify the Host OS last boot time on the SUT matches the boot time recorded before entry into S3. Verify that Intel® AMT on the SUT responds to version queries via all available network interfaces. Ensure yellow bang is not seen on Drivers in Device Manager 	
Pass Criteria:	The test passes if the Intel® CSME functions properly when AC Source attached in S3 state.	
ID:	ME_PM_50.2	
Title:	S0/CM0 to S4/CM3 to S0/CM0 via AC-attach (PP2/LP3)	
Requirement:	Mandatory	Exemptions <input checked="" type="checkbox"/> Non-Mobile (AC-only) systems
		<input checked="" type="checkbox"/> Modern Standby and InstantGo* systems
Method:	Automated by Intel® PETS	
Objective:	This test checks the SUT power flow from S0/CM0 to S4/CM3 to S0/CM0 via AC-attach with the parameters outlined below.	
Configuration:	<p>Intel® AMT should be provisioned via manual mode.</p> <p>If Deep S4, Deep S5, and/or G3 are supported on the SUT, please confirm the following:</p> <ul style="list-style-type: none"> the SUT and/or BIOS are properly configured to permit Deep S4/S5 or G3 entry. the correct Deep Sx policy is applied to the SUT profile in Intel® PETS. <p>This test assumes that either LAN-only, WLAN-only, or both LAN and WLAN network interfaces are available on the SUT.</p>	



ID:	ME_PM_50.2	
Parameters:	System Power Source DC-only	
	Power States	Initial S0/MeOn (CM0)
		Final S0/MeOn (CM0)
		Trigger AC-attach in S4 state
	Intel® AMT	Power Package PP2 (Intel® ME on in S0, wake in Sx/AC)
		WLAN Link Policy LP3 (Enabled in S0, Sx/AC) where available
Setup:	<ol style="list-style-type: none"> Set the SUT power source to AC+DC. Bring the SUT to the base state of S0/MeOn (CM0,CM0-PG), and confirm that the Host OS is available. Verify that a DC battery is connected to the SUT, and that it is charged. Set the SUT power source to DC-only. Set the active power package on the SUT to Power Package 2 (Intel® ME on in S0, wake in Sx/AC). Set the Intel® AMT WLAN link policy on the SUT to Link Policy 3 (Enabled in S0, Sx/AC), if the WLAN network interface is available. Ensure that the Host OS network device drivers are configured to not wake the SUT. This includes enabling ARP and/or NS Offload features where available to help prevent unexpected host wake events. Most especially, ensure that the Host OS Wireless Wake on LAN driver setting on the SUT is disabled, if the WLAN network interface is available. Ensure that Intel® RMT is disabled, if running on an All-in-One (AIO) SUT with feature support. Verify that Intel® AMT on the SUT responds to version queries via all available network interfaces. Ensure yellow bang is not seen on Drivers in Device Manager 	
Procedure:	<ol style="list-style-type: none"> Hibernate the SUT via the Host OS. Verify that the SUT is in S4/MeOff (CM-Off). Set the SUT power source to AC+DC Verify that the SUT is in S4/MeOn (CM3). Verify that Intel® AMT on the SUT responds to version queries via all available network interfaces. Briefly press the Power Button on the SUT. Verify that the SUT is in S0/MeOn (CM0,CM0-PG). Verify that the Host OS on the SUT is available. Verify that windows booted from hibernate i.e. value should be 0x02. "run the following power shell command": Get-WinEvent -ProviderName Microsoft-Windows-Kernel-boot -MaxEvents 10 Where-Object {\$_.message -like "The boot type*"} Verify that Intel® AMT on the SUT responds to version queries via all available network interfaces. Ensure yellow bang is not seen on Drivers in Device Manager 	
Pass Criteria:	The test passes if the Intel® CSME functions properly when AC Source attached in S4 state.	

ID:	ME_PM_50.3	
Title:	S0/CM0 to S5/CM3 to S0/CM0 via AC-attach (PP2/LP3)	
Requirement:	Mandatory	Exemptions <input checked="" type="checkbox"/> Non-Mobile (AC-only) systems <input checked="" type="checkbox"/> Modern Standby and InstantGo* systems
Method:	Automated by Intel® PETS	
Objective:	This test checks the SUT power flow from S0/CM0 to S5/CM3 to S0/CM0 via AC-attach with the parameters outlined below.	
Configuration:	<p>Intel® AMT should be provisioned via manual mode.</p> <p>If Deep S5 and/or G3 are supported on the SUT, please confirm the following:</p> <ul style="list-style-type: none"> the SUT and/or BIOS are properly configured to permit Deep S5 or G3 entry. the correct Deep Sx policy is applied to the SUT profile in Intel® PETS. <p>This test assumes that either LAN-only, WLAN-only, or both LAN and WLAN network interfaces are available on the SUT.</p>	



ID:	ME_PM_50.3	
Parameters:	System Power Source DC-only	
	Power States	Initial S0/MeOn (CM0)
		Final S0/MeOn (CM0)
		Trigger AC-attach in S5 state
	Intel® AMT	Power Package PP2 (Intel® ME on in S0, wake in Sx/AC)
		WLAN Link Policy LP3 (Enabled in S0, Sx/AC) where available
Setup:	<ol style="list-style-type: none"> Set the SUT power source to AC+DC. Bring the SUT to the base state of S0/MeOn (CM0,CM0-PG), and confirm that the Host OS is available. Verify that a DC battery is connected to the SUT, and that it is charged. Set the SUT power source to DC-only. Set the active power package on the SUT to Power Package 2 (Intel® ME on in S0, wake in Sx/AC). Set the Intel® AMT WLAN link policy on the SUT to Link Policy 3 (Enabled in S0, Sx/AC), if the WLAN network interface is available. Ensure that the Host OS network device drivers are configured to not wake the SUT. This includes enabling ARP and/or NS Offload features where available to help prevent unexpected host wake events. Most especially, ensure that the Host OS Wireless Wake on LAN driver setting on the SUT is disabled, if the WLAN network interface is available. Ensure that Intel® RMT is disabled, if running on an All-in-One (AIO) SUT with feature support. Verify that Intel® AMT on the SUT responds to version queries via all available network interfaces. Ensure yellow bang is not seen on Drivers in Device Manager 	
Procedure:	<ol style="list-style-type: none"> Shutdown the SUT via the Host OS. Verify that the SUT is in S5, Deep S5, G3/MeOff (CM-Off). Set the SUT power source to AC+DC Verify that the SUT is in S5/MeOn (CM3). Verify that Intel® AMT on the SUT responds to version queries via all available network interfaces. Briefly press the Power Button on the SUT. Verify that the SUT is in S0/MeOn (CM0,CM0-PG). Verify that the Host OS on the SUT is available. Verify that Intel® AMT on the SUT responds to version queries via all available network interfaces. Ensure yellow bang is not seen on Drivers in Device Manager 	
Pass Criteria:	The test passes if the Intel® CSME functions properly when AC Source attached in S5 state.	

ID:	ME_PM_50.4	
Title:	S0/CM0 to S3/CM-Off to S0/CM0 via AC-attach (PP1)	
Requirement:	Mandatory	Exemptions <input checked="" type="checkbox"/> Non-Mobile (AC-only) systems <input checked="" type="checkbox"/> Modern Standby and InstantGo* systems
Method:	Automated by Intel® PETS	
Objective:	This test checks the SUT power flow from S0/CM0 to S3/CM-Off to S0/CM0 via AC-attach with the parameters outlined below.	
Configuration:	This test assumes that either LAN-only, WLAN-only, or both LAN and WLAN network interfaces are available on the SUT.	
Parameters:	System Power Source DC-only	
	Power States	Initial S0/MeOn (CM0)
		Final S0/MeOn (CM0)
		Trigger AC-attach in S3 state
	Intel® AMT	Power Package PP1 (Intel® ME on in S0)
		WLAN Link Policy LP3 (Enabled in S0, Sx/AC) where available



ID:	ME_PM_50.4	
Setup:	<ol style="list-style-type: none"> Set the SUT power source to AC+DC. Bring the SUT to the base state of S0/MeOn (CM0,CM0-PG), and confirm that the Host OS is available. Verify that a DC battery is connected to the SUT, and that it is charged. Set the SUT power source to DC-only. Set the active power package on the SUT to Power Package 1 (Intel® ME on in S0). Set the Intel® AMT WLAN link policy on the SUT to Link Policy 3 (Enabled in S0, Sx/AC), if the WLAN network interface is available. Ensure that the Host OS network device drivers are configured to not wake the SUT. This includes enabling ARP and/or NS Offload features where available to help prevent unexpected host wake events. Most especially, ensure that the Host OS Wireless Wake on LAN driver setting on the SUT is disabled, if the WLAN network interface is available. Ensure that Intel® RMT is disabled, if running on an All-in-One (AIO) SUT with feature support. Verify that Intel® AMT on the SUT responds to version queries via all available network interfaces. Record the Host OS last boot time on the SUT (to verify successful return to S3) Ensure yellow bang is not seen on Drivers in Device Manager 	
Procedure:	<ol style="list-style-type: none"> Suspend the SUT via the Host OS. Verify that the SUT is in S3/MeOff (CM-Off). Set the SUT power source to AC+DC. Verify that the SUT is in S3/MeOff (CM-Off). Verify that Intel® AMT on the SUT does not respond to version queries via any of the available network interfaces. Briefly press the Power Button on the SUT. Verify that the SUT is in S0/MeOn (CM0,CM0-PG). Verify that the Host OS on the SUT is available. Verify the Host OS last boot time on the SUT matches the boot time recorded before entry into S3. Verify that Intel® AMT on the SUT responds to version queries via all available network interfaces. Ensure yellow bang is not seen on Drivers in Device Manager 	
Pass Criteria:	The test passes if the Intel® CSME functions properly i.e. stays MeOff when AC Source attached in S3 state.	

ID:	ME_PM_50.5	
Title:	S0/CM0 to S4/CM-Off to S0/CM0 via AC-attach (PP1)	
Requirement:	Mandatory	Exemptions <ul style="list-style-type: none"> <input checked="" type="checkbox"/> Non-Mobile (AC-only) systems <input checked="" type="checkbox"/> Modern Standby and InstantGo* systems
Method:	Automated by Intel® PETS	
Objective:	This test checks the SUT power flow from S0/CM0 to S4/CM-Off to S0/CM0 via AC-attach with the parameters outlined below.	
Configuration:	<p>Intel® AMT should be provisioned via manual mode.</p> <p>If Deep S4, Deep S5, and/or G3 are supported on the SUT, please confirm the following:</p> <ul style="list-style-type: none"> the SUT and/or BIOS are properly configured to permit Deep S4/S5 or G3 entry. the correct Deep Sx policy is applied to the SUT profile in Intel® PETS. <p>This test assumes that either LAN-only, WLAN-only, or both LAN and WLAN network interfaces are available on the SUT.</p>	
Parameters:	System Power Source	
	Power States	Initial S0/MeOn (CM0)
		Final S0/MeOn (CM0)
		Trigger AC-attach in S4 state
	Intel® AMT	Power Package PP1 (Intel® ME on in S0) WLAN Link Policy LP3 (Enabled in S0, Sx/AC) where available



ID:	ME_PM_50.5	
Setup:	<ol style="list-style-type: none"> 1. Set the SUT power source to AC+DC. 2. Bring the SUT to the base state of S0/MeOn (CM0,CM0-PG), and confirm that the Host OS is available. 3. Verify that a DC battery is connected to the SUT, and that it is charged. 4. Set the SUT power source to DC-only. 5. Set the active power package on the SUT to Power Package 1 (Intel® ME on in S0). 6. Set the Intel® AMT WLAN link policy on the SUT to Link Policy 3 (Enabled in S0, Sx/AC), if the WLAN network interface is available. 7. Ensure that the Host OS network device drivers are configured to not wake the SUT. This includes enabling ARP and/or NS Offload features where available to help prevent unexpected host wake events. Most especially, ensure that the Host OS Wireless Wake on LAN driver setting on the SUT is disabled, if the WLAN network interface is available. 8. Ensure that Intel® RMT is disabled, if running on an All-in-One (AIO) SUT with feature support. 9. Verify that Intel® AMT on the SUT responds to version queries via all available network interfaces. 10. Ensure yellow bang is not seen on Drivers in Device Manager 	
Procedure:	<ol style="list-style-type: none"> 1. Hibernate the SUT via the Host OS. 2. Verify that the SUT is in S4/MeOff (CM-Off). 3. Set the SUT power source to AC+DC. 4. Verify that the SUT is in S4/MeOff (CM-Off). 5. Verify that Intel® AMT on the SUT does not respond to version queries via any of the available network interfaces. 6. Briefly press the Power Button on the SUT. 7. Verify that the SUT is in S0/MeOn (CM0,CM0-PG). 8. Verify that the Host OS on the SUT is available. 9. Verify that windows booted from hibernate i.e. value should be 0x02. "run the following power shell command": Get-WinEvent -ProviderName Microsoft-Windows-Kernel-boot -MaxEvents 10 Where-Object {\$_.message -like "The boot type*"}. 10. Verify that Intel® AMT on the SUT responds to version queries via all available network interfaces. 11. Ensure yellow bang is not seen on Drivers in Device Manager 	
Pass Criteria:	The test passes if the Intel® CSME functions properly i.e. stays MEOff when AC Source attached in S4 state.	

ID:	ME_PM_50.6	
Title:	S0/CM0 to S5/CM-Off to S0/CM0 via AC-attach (PP1)	
Requirement:	Mandatory	Exemptions <input checked="" type="checkbox"/> Non-Mobile (AC-only) systems <input checked="" type="checkbox"/> Modern Standby and InstantGo* systems
Method:	Automated by Intel® PETS	
Objective:	This test checks the SUT power flow from S0/CM0 to S5/CM-Off to S0/CM0 via AC-attach with the parameters outlined below.	
Configuration:	<p>Intel® AMT should be provisioned via manual mode.</p> <p>If Deep S5 and/or G3 are supported on the SUT, please confirm the following:</p> <ul style="list-style-type: none"> • the SUT and/or BIOS are properly configured to permit Deep S5 or G3 entry. • the correct Deep Sx policy is applied to the SUT profile in Intel® PETS. <p>This test assumes that either LAN-only, WLAN-only, or both LAN and WLAN network interfaces are available on the SUT.</p>	
Parameters:	System Power Source	
	Power States	Initial S0/MeOn (CM0)
		Final S0/MeOn (CM0)
		Trigger AC-attach in S5 state
	Intel® AMT	Power Package PP1 (Intel® ME on in S0)
		WLAN Link Policy LP3 (Enabled in S0, Sx/AC) where available



ID:	ME_PM_50.6	
Setup:	<ol style="list-style-type: none"> 1. Set the SUT power source to AC+DC. 2. Bring the SUT to the base state of S0/MeOn (CM0,CM0-PG), and confirm that the Host OS is available. 3. Verify that a DC battery is connected to the SUT, and that it is charged. 4. Set the SUT power source to DC-only. 5. Set the active power package on the SUT to Power Package 1 (Intel® ME on in S0). 6. Set the Intel® AMT WLAN link policy on the SUT to Link Policy 3 (Enabled in S0, Sx/AC), if the WLAN network interface is available. 7. Ensure that the Host OS network device drivers are configured to not wake the SUT. This includes enabling ARP and/or NS Offload features where available to help prevent unexpected host wake events. Most especially, ensure that the Host OS Wireless Wake on LAN driver setting on the SUT is disabled, if the WLAN network interface is available. 8. Ensure that Intel® RMT is disabled, if running on an All-in-One (AIO) SUT with feature support. 9. Verify that Intel® AMT on the SUT responds to version queries via all available network interfaces. 10. Ensure yellow bang is not seen on Drivers in Device Manager 	
Procedure:	<ol style="list-style-type: none"> 1. Shutdown the SUT via the Host OS. 2. Verify that the SUT is in S5, Deep S5, G3/MeOff (CM-Off). 3. Set the SUT power source to AC+DC. 4. Verify that the SUT is in S5, Deep S5, G3/MeOff (CM-Off). 5. Verify that Intel® AMT on the SUT does not respond to version queries via any of the available network interfaces. 6. Briefly press the Power Button on the SUT. 7. Verify that the SUT is in S0/MeOn (CM0,CM0-PG). 8. Verify that the Host OS on the SUT is available. 9. Verify that Intel® AMT on the SUT responds to version queries via all available network interfaces. 10. Ensure yellow bang is not seen on Drivers in Device Manager 	
Pass Criteria:	The test passes if the Intel® CSME functions properly i.e. stays MeOff when AC Source attached in S5 state.	
ID:	ME_PM_50.7	
Title:	S0/CM0 to S3/CM-Off to S0/CM0 via AC-attach	
Requirement:	Mandatory	Exemptions <input checked="" type="checkbox"/> Non-Mobile (AC-only) systems <input checked="" type="checkbox"/> Modern Standby and InstantGo* systems
Method:	Automated by Intel® PETS	
Objective:	This test checks the SUT power flow from S0/CM0 to S3/CM-Off to S0/CM0 via AC-attach with the parameters outlined below.	
Configuration:	This test assumes that either LAN-only, WLAN-only, or both LAN and WLAN network interfaces are available on the SUT.	
Parameters:	System Power Source	
	Power States	Initial S0/MeOn (CM0)
		Final S0/MeOn (CM0)
		Trigger AC-attach in S3 state
	Intel® AMT	Power Package [Intel® AMT is not provisioned.]
		WLAN Link Policy [Intel® AMT is not provisioned.]



ID:	ME_PM_50.7	
Setup:	<ol style="list-style-type: none"> 1. Set the SUT power source to AC+DC. 2. Bring the SUT to the base state of S0/MeOn (CM0,CM0-PG), and confirm that the Host OS is available. 3. Verify that a DC battery is connected to the SUT, and that it is charged. 4. Set the SUT power source to DC-only. 5. Ensure Intel (R) AMT is not provisioned. 6. Ensure that the Host OS network device drivers are configured to not wake the SUT. This includes enabling ARP and/or NS Offload features where available to help prevent unexpected host wake events. Most especially, ensure that the Host OS Wireless Wake on LAN driver setting on the SUT is disabled, if the WLAN network interface is available. 7. Ensure that Intel® RMT is disabled, if running on an All-in-One (AIO) SUT with feature support. 8. Record the Host OS last boot time on the SUT (to verify successful return to S3) 9. Ensure yellow bang is not seen on Drivers in Device Manager 	
Procedure:	<ol style="list-style-type: none"> 1. Suspend the SUT via the Host OS. 2. Verify that the SUT is in S3/MeOff (CM-Off). 3. Set the SUT power source to AC+DC. 4. Verify that the SUT is in S3/MeOff (CM-Off). 5. Briefly press the Power Button on the SUT. 6. Verify that the SUT is in S0/MeOn (CM0,CM0-PG). 7. Verify that the Host OS on the SUT is available. 8. Verify the Host OS last boot time on the SUT matches the boot time recorded before entry into S3. 9. Ensure yellow bang is not seen on Drivers in Device Manager 	
Pass Criteria:	The test passes if the Intel® CSME functions properly i.e. stays MeOff when AC Source attached in S3 state.	

ID:	ME_PM_50.8																
Title:	S0/CM0 to S4/CM-Off to S0/CM0 via AC-attach																
Requirement:	Mandatory	Exemptions <ul style="list-style-type: none"> <input checked="" type="checkbox"/> Non-Mobile (AC-only) systems <input checked="" type="checkbox"/> Modern Standby and InstantGo* systems 															
Method:	Automated by Intel® PETS																
Objective:	This test checks the SUT power flow from S0/CM0 to S4/CM-Off to S0/CM0 via AC-attach with the parameters outlined below.																
Configuration:	<p>Intel® AMT should be not provisioned</p> <p>If Deep S4, Deep S5, and/or G3 are supported on the SUT, please confirm the following:</p> <ul style="list-style-type: none"> the SUT and/or BIOS are properly configured to permit Deep S4/S5 or G3 entry. the correct Deep Sx policy is applied to the SUT profile in Intel® PETS. <p>This test assumes that either LAN-only, WLAN-only, or both LAN and WLAN network interfaces are available on the SUT.</p>																
Parameters:	<table border="1"> <tr> <td colspan="2">System Power Source</td><td>DC-only</td></tr> <tr> <td rowspan="3">Power States</td><td>Initial</td><td>S0/MeOn (CM0)</td></tr> <tr> <td>Final</td><td>S0/MeOn (CM0)</td></tr> <tr> <td>Trigger</td><td>AC-attach in S4 state</td></tr> <tr> <td rowspan="2">Intel® AMT</td><td>Power Package</td><td>[Intel® AMT is not provisioned.]</td></tr> <tr> <td>WLAN Link Policy</td><td>[Intel® AMT is not provisioned.]</td></tr> </table>		System Power Source		DC-only	Power States	Initial	S0/MeOn (CM0)	Final	S0/MeOn (CM0)	Trigger	AC-attach in S4 state	Intel® AMT	Power Package	[Intel® AMT is not provisioned.]	WLAN Link Policy	[Intel® AMT is not provisioned.]
System Power Source		DC-only															
Power States	Initial	S0/MeOn (CM0)															
	Final	S0/MeOn (CM0)															
	Trigger	AC-attach in S4 state															
Intel® AMT	Power Package	[Intel® AMT is not provisioned.]															
	WLAN Link Policy	[Intel® AMT is not provisioned.]															
Setup:	<ol style="list-style-type: none"> 1. Set the SUT power source to AC+DC. 2. Bring the SUT to the base state of S0/MeOn (CM0,CM0-PG), and confirm that the Host OS is available. 3. Verify that a DC battery is connected to the SUT, and that it is charged. 4. Set the SUT power source to DC-only. 5. Ensure Intel (R) AMT is not provisioned. 6. Ensure that the Host OS network device drivers are configured to not wake the SUT. This includes enabling ARP and/or NS Offload features where available to help prevent unexpected host wake events. Most especially, ensure that the Host OS Wireless Wake on LAN driver setting on the SUT is disabled, if the WLAN network interface is available. 7. Ensure that Intel® RMT is disabled, if running on an All-in-One (AIO) SUT with feature support. 8. Ensure yellow bang is not seen on Drivers in Device Manager 																



ID:	ME_PM_50.8																
Procedure:	<ol style="list-style-type: none"> 1. Hibernate the SUT via the Host OS. 2. Verify that the SUT is in S4/MeOff (CM-Off). 3. Set the SUT power source to AC+DC. 4. Verify that the SUT is in S4/MeOff (CM-Off). 5. Briefly press the Power Button on the SUT. 6. Verify that the SUT is in S0/MeOn (CM0,CM0-PG). 7. Verify that windows booted from hibernate i.e. value should be 0x02. "run the following power shell command": Get-WinEvent -ProviderName Microsoft-Windows-Kernel-boot -MaxEvents 10 Where-Object {\$_.message -like "The boot type*"} 8. Verify that the Host OS on the SUT is available. 9. Ensure yellow bang is not seen on Drivers in Device Manager 																
Pass Criteria:	The test passes if the Intel® CSME functions properly i.e. stays MeOff when AC Source attached in S4 state.																
ID:	ME_PM_50.9																
Title:	S0/CM0 to S5/CM-Off to S0/CM0 via AC-attach																
Requirement:	Mandatory	Exemptions <ul style="list-style-type: none"> <input checked="" type="checkbox"/> Non-Mobile (AC-only) systems <input checked="" type="checkbox"/> Modern Standby and InstantGo* systems 															
Method:	Automated by Intel® PETS																
Objective:	This test checks the SUT power flow from S0/CM0 to S5/CM-Off to S0/CM0 via AC-attach with the parameters outlined below.																
Configuration:	<p>Intel® AMT should be not provisioned</p> <p>If Deep S5 and/or G3 are supported on the SUT, please confirm the following:</p> <ul style="list-style-type: none"> • the SUT and/or BIOS are properly configured to permit Deep S5 or G3 entry. • the correct Deep Sx policy is applied to the SUT profile in Intel® PETS. <p>This test assumes that either LAN-only, WLAN-only, or both LAN and WLAN network interfaces are available on the SUT.</p>																
Parameters:	<table border="1"> <thead> <tr> <th colspan="2">System Power Source</th><th>DC-only</th></tr> </thead> <tbody> <tr> <td rowspan="3">Power States</td><td>Initial</td><td>S0/MeOn (CM0)</td></tr> <tr> <td>Final</td><td>S0/MeOn (CM0)</td></tr> <tr> <td>Trigger</td><td>AC-attach in S5 state</td></tr> <tr> <td rowspan="2">Intel® AMT</td><td>Power Package</td><td>[Intel® AMT is not provisioned.]</td></tr> <tr> <td>WLAN Link Policy</td><td>[Intel® AMT is not provisioned.]</td></tr> </tbody> </table>		System Power Source		DC-only	Power States	Initial	S0/MeOn (CM0)	Final	S0/MeOn (CM0)	Trigger	AC-attach in S5 state	Intel® AMT	Power Package	[Intel® AMT is not provisioned.]	WLAN Link Policy	[Intel® AMT is not provisioned.]
System Power Source		DC-only															
Power States	Initial	S0/MeOn (CM0)															
	Final	S0/MeOn (CM0)															
	Trigger	AC-attach in S5 state															
Intel® AMT	Power Package	[Intel® AMT is not provisioned.]															
	WLAN Link Policy	[Intel® AMT is not provisioned.]															
Setup:	<ol style="list-style-type: none"> 1. Set the SUT power source to AC+DC. 2. Bring the SUT to the base state of S0/MeOn (CM0,CM0-PG), and confirm that the Host OS is available. 3. Verify that a DC battery is connected to the SUT, and that it is charged. 4. Set the SUT power source to DC-only. 5. Ensure Intel (R) AMT is not provisioned. 6. Ensure that the Host OS network device drivers are configured to not wake the SUT. This includes enabling ARP and/or NS Offload features where available to help prevent unexpected host wake events. Most especially, ensure that the Host OS Wireless Wake on LAN driver setting on the SUT is disabled, if the WLAN network interface is available. 7. Ensure that Intel® RMT is disabled, if running on an All-in-One (AIO) SUT with feature support. 8. Ensure yellow bang is not seen on Drivers in Device Manager 																
Procedure:	<ol style="list-style-type: none"> 1. Shutdown the SUT via the Host OS. 2. Verify that the SUT is in S5, Deep S5, G3/MeOff (CM-Off). 3. Set the SUT power source to AC+DC. 4. Verify that the SUT is in S5, Deep S5, G3/MeOff (CM-Off). 5. Briefly press the Power Button on the SUT. 6. Verify that the SUT is in S0/MeOn (CM0,CM0-PG). 7. Verify that the Host OS on the SUT is available. 8. Ensure yellow bang is not seen on Drivers in Device Manager 																
Pass Criteria:	The test passes if the Intel® CSME functions properly i.e. stays MeOff when AC Source attached in S5 state.																



12.35 ME_PM_51: S0/CM0 to Sx/CM-Off to S0/CM0 via AC Detach in Sx State.

ID:	ME_PM_51.1																	
Title:	S0/CM0 to S3/CM-Off to S0/CM0 via AC-detach (PP2/LP3)																	
Requirement:	Mandatory	Exemptions	<input checked="" type="checkbox"/> Non-Mobile (AC-only) systems <input checked="" type="checkbox"/> Modern Standby and InstantGo* systems															
Method:	Automated by Intel® PETS																	
Objective:	This test checks the SUT power flow from S0/CM0 to S3/CM-Off to S0/CM0 via AC-detach with the parameters outlined below.																	
Configuration:	This test assumes that either LAN-only, WLAN-only, or both LAN and WLAN network interfaces are available on the SUT.																	
Parameters:	<table><tr><td colspan="2">System Power Source</td><td>DC-only</td></tr><tr><td rowspan="3">Power States</td><td>Initial</td><td>S0/MeOn (CM0)</td></tr><tr><td>Final</td><td>S0/MeOn (CM0)</td></tr><tr><td>Trigger</td><td>AC-detach in S3 state</td></tr><tr><td rowspan="2">Intel® AMT</td><td>Power Package</td><td>PP2 (Intel® ME on in S0, wake in Sx/AC)</td></tr><tr><td>WLAN Link Policy</td><td>LP3 (Enabled in S0, Sx/AC) where available</td></tr></table>			System Power Source		DC-only	Power States	Initial	S0/MeOn (CM0)	Final	S0/MeOn (CM0)	Trigger	AC-detach in S3 state	Intel® AMT	Power Package	PP2 (Intel® ME on in S0, wake in Sx/AC)	WLAN Link Policy	LP3 (Enabled in S0, Sx/AC) where available
System Power Source		DC-only																
Power States	Initial	S0/MeOn (CM0)																
	Final	S0/MeOn (CM0)																
	Trigger	AC-detach in S3 state																
Intel® AMT	Power Package	PP2 (Intel® ME on in S0, wake in Sx/AC)																
	WLAN Link Policy	LP3 (Enabled in S0, Sx/AC) where available																
Setup:	<ol style="list-style-type: none">1. Set the SUT power source to AC+DC.2. Bring the SUT to the base state of S0/MeOn (CM0,CM0-PG), and confirm that the Host OS is available.3. Set the active power package on the SUT to Power Package 2 (Intel® ME on in S0, wake in Sx/AC).4. Set the Intel® AMT WLAN link policy on the SUT to Link Policy 3 (Enabled in S0, Sx/AC), if the WLAN network interface is available.5. Ensure that the Host OS network device drivers are configured to not wake the SUT. This includes enabling ARP and/or NS Offload features where available to help prevent unexpected host wake events. Most especially, ensure that the Host OS Wireless Wake on LAN driver setting on the SUT is disabled, if the WLAN network interface is available.6. Ensure that Intel® RMT is disabled, if running on an All-in-One (AIO) SUT with feature support.7. Verify that Intel® AMT on the SUT responds to version queries via all available network interfaces.8. Record the Host OS last boot time on the SUT (to verify successful return to S3)9. Ensure yellow bang is not seen on Drivers in Device Manager																	
Procedure:	<ol style="list-style-type: none">1. Suspend the SUT via the Host OS.2. Verify that the SUT is in S3/MeOn (CM3).3. Verify that a DC battery is connected to the SUT, and that it is charged.4. Set the SUT power source to DC-only.5. Verify that the SUT is in S3/MeOff (CM-Off).6. Set the SUT power source to AC+DC.7. Verify that the SUT is in S3/MeOn (CM3).8. Briefly press the Power Button on the SUT.9. Verify that the SUT is in S0/MeOn (CM0,CM0-PG).10. Verify that the Host OS on the SUT is available.11. Verify the Host OS last boot time on the SUT matches the boot time recorded before entry into S3.12. Verify that Intel® AMT on the SUT responds to version queries via all available network interfaces.13. Ensure yellow bang is not seen on Drivers in Device Manager																	
Pass Criteria:	The test passes if the Intel® CSME becomes Me-Off when AC Detached in S3 state and becomes MeOn after AC attached in S3 state.																	

ID:	ME_PM_51.2		
Title:	S0/CM0 to S4/CM-Off to S0/CM0 via AC-detach (PP2/LP3)		
Requirement:	Mandatory	Exemptions	<input checked="" type="checkbox"/> Non-Mobile (AC-only) systems <input checked="" type="checkbox"/> Modern Standby and InstantGo* systems
Method:	Automated by Intel® PETS		



ID:	ME_PM_51.2																
Objective:	This test checks the SUT power flow from S0/CM0 to S4/CM-Off to S0/CM0 via AC-detach with the parameters outlined below.																
Configuration:	<p>Intel® AMT should be provisioned via manual mode.</p> <p>If Deep S4, Deep S5, and/or G3 are supported on the SUT, please confirm the following:</p> <ul style="list-style-type: none"> the SUT and/or BIOS are properly configured to permit Deep S4/S5 or G3 entry. the correct Deep Sx policy is applied to the SUT profile in Intel® PETS. <p>This test assumes that either LAN-only, WLAN-only, or both LAN and WLAN network interfaces are available on the SUT.</p>																
Parameters:	<table border="1"> <tr> <td colspan="2">System Power Source</td><td>DC-only</td></tr> <tr> <td rowspan="3">Power States</td><td>Initial</td><td>S0/MeOn (CM0)</td></tr> <tr> <td>Final</td><td>S0/MeOn (CM0)</td></tr> <tr> <td>Trigger</td><td>AC-detach in S4 state</td></tr> <tr> <td rowspan="2">Intel® AMT</td><td>Power Package</td><td>PP2 (Intel® ME on in S0, wake in Sx/AC)</td></tr> <tr> <td>WLAN Link Policy</td><td>LP3 (Enabled in S0, Sx/AC) where available</td></tr> </table>		System Power Source		DC-only	Power States	Initial	S0/MeOn (CM0)	Final	S0/MeOn (CM0)	Trigger	AC-detach in S4 state	Intel® AMT	Power Package	PP2 (Intel® ME on in S0, wake in Sx/AC)	WLAN Link Policy	LP3 (Enabled in S0, Sx/AC) where available
System Power Source		DC-only															
Power States	Initial	S0/MeOn (CM0)															
	Final	S0/MeOn (CM0)															
	Trigger	AC-detach in S4 state															
Intel® AMT	Power Package	PP2 (Intel® ME on in S0, wake in Sx/AC)															
	WLAN Link Policy	LP3 (Enabled in S0, Sx/AC) where available															
Setup:	<ol style="list-style-type: none"> Set the SUT power source to AC+DC. Bring the SUT to the base state of S0/MeOn (CM0,CM0-PG), and confirm that the Host OS is available. Set the active power package on the SUT to Power Package 2 (Intel® ME on in S0, wake in Sx/AC). Set the Intel® AMT WLAN link policy on the SUT to Link Policy 3 (Enabled in S0, Sx/AC), if the WLAN network interface is available. Ensure that the Host OS network device drivers are configured to not wake the SUT. This includes enabling ARP and/or NS Offload features where available to help prevent unexpected host wake events. Most especially, ensure that the Host OS Wireless Wake on LAN driver setting on the SUT is disabled, if the WLAN network interface is available. Ensure that Intel® RMT is disabled, if running on an All-in-One (AIO) SUT with feature support. Verify that Intel® AMT on the SUT responds to version queries via all available network interfaces. Ensure yellow bang is not seen on Drivers in Device Manager 																
Procedure:	<ol style="list-style-type: none"> Hibernate the SUT via the Host OS. Verify that the SUT is in S4/MeOn (CM3). Verify that a DC battery is connected to the SUT, and that it is charged. Set the SUT power source to DC-only. Verify that the SUT is in S4/MeOff (CM-Off). Set the SUT power source to AC+DC. Verify that the SUT is in S4/MeOn (CM3). Briefly press the Power Button on the SUT. Verify that the SUT is in S0/MeOn (CM0,CM0-PG). Verify that the Host OS on the SUT is available. Verify that windows booted from hibernate i.e. value should be 0x02. "run the following power shell command": Get-WinEvent -ProviderName Microsoft-Windows-Kernel-boot -MaxEvents 10 Where-Object {\$_.message -like "The boot type*"} Verify that Intel® AMT on the SUT responds to version queries via all available network interfaces. Ensure yellow bang is not seen on Drivers in Device Manager 																
Pass Criteria:	The test passes if the Intel® CSME becomes Me-Off when AC Detached in S4 state and becomes MeOn after AC attached in S4 state.																

ID:	ME_PM_51.3	
Title:	S0/CM0 to S5/CM-Off to S0/CM0 via AC-detach (PP2/LP3)	
Requirement:	Mandatory	Exemptions <ul style="list-style-type: none"> <input checked="" type="checkbox"/> Non-Mobile (AC-only) systems <input checked="" type="checkbox"/> Modern Standby and InstantGo* systems
Method:	Automated by Intel® PETS	
Objective:	This test checks the SUT power flow from S0/CM0 to S5/CM-Off to S0/CM0 via AC-detach with the parameters outlined below.	



ID:	ME_PM_51.3		
Configuration:	<p>Intel® AMT should be provisioned via manual mode.</p> <p>If Deep S5 and/or G3 are supported on the SUT, please confirm the following:</p> <ul style="list-style-type: none">the SUT and/or BIOS are properly configured to permit Deep S5 or G3 entry.the correct Deep Sx policy is applied to the SUT profile in Intel® PETS. <p>This test assumes that either LAN-only, WLAN-only, or both LAN and WLAN network interfaces are available on the SUT.</p>		
Parameters:	System Power Source		DC-only
	Power States	Initial	S0/MeOn (CM0)
		Final	S0/MeOn (CM0)
		Trigger	AC-detach in S5 state
	Intel® AMT	Power Package	PP2 (Intel® ME on in S0, wake in Sx/AC)
WLAN Link Policy		LP3 (Enabled in S0, Sx/AC) where available	
Setup:	<ol style="list-style-type: none">Set the SUT power source to AC+DC.Bring the SUT to the base state of S0/MeOn (CM0,CM0-PG), and confirm that the Host OS is available.Set the active power package on the SUT to Power Package 2 (Intel® ME on in S0, wake in Sx/AC).Set the Intel® AMT WLAN link policy on the SUT to Link Policy 3 (Enabled in S0, Sx/AC), if the WLAN network interface is available.Ensure that the Host OS network device drivers are configured to not wake the SUT. This includes enabling ARP and/or NS Offload features where available to help prevent unexpected host wake events. Most especially, ensure that the Host OS Wireless Wake on LAN driver setting on the SUT is disabled, if the WLAN network interface is available.Ensure that Intel® RMT is disabled, if running on an All-in-One (AIO) SUT with feature support.Verify that Intel® AMT on the SUT responds to version queries via all available network interfaces.Ensure yellow bang is not seen on Drivers in Device Manager		
Procedure:	<ol style="list-style-type: none">Shutdown the SUT via the Host OS.Verify that the SUT is in S5/MeOn (CM3).Verify that a DC battery is connected to the SUT, and that it is charged.Set the SUT power source to DC-only.Verify that the SUT is in S5, Deep S5, G3/MeOff (CM-Off).Set the SUT power source to AC+DC.Verify that the SUT is in S5/MeOn (CM3).Briefly press the Power Button on the SUT.Verify that the SUT is in S0/MeOn (CM0,CM0-PG).Verify that the Host OS on the SUT is available.Verify that Intel® AMT on the SUT responds to version queries via all available network interfaces.Ensure yellow bang is not seen on Drivers in Device Manager		
Pass Criteria:	The test passes if the Intel® CSME becomes Me-Off when AC Detached in S5 state and becomes MeOn after AC attached in S5 state.		

ID:	ME_PM_51.4		
Title:	S0/CM0 to S3/CM-Off to S0/CM0 via AC-detach (PP1)		
Requirement:	Mandatory	Exemptions	<input checked="" type="checkbox"/> Non-Mobile (AC-only) systems <input checked="" type="checkbox"/> Modern Standby and InstantGo* systems
Method:	Automated by Intel® PETS		
Objective:	This test checks the SUT power flow from S0/CM0 to S3/CM-Off to S0/CM0 via AC-detach with the parameters outlined below.		
Configuration:	This test assumes that either LAN-only, WLAN-only, or both LAN and WLAN network interfaces are available on the SUT.		



ID:	ME_PM_51.4	
Parameters:	System Power Source	
		DC-only
	Power States	Initial S0/MeOn (CM0)
		Final S0/MeOn (CM0)
		Trigger AC-detach in S3 state
Intel® AMT	Power Package	PP1 (Intel® ME on in S0)
	WLAN Link Policy	LP3 (Enabled in S0, Sx/AC) where available
Setup:	<ol style="list-style-type: none"> 1. Set the SUT power source to AC+DC. 2. Bring the SUT to the base state of S0/MeOn (CM0,CM0-PG), and confirm that the Host OS is available. 3. Set the active power package on the SUT to Power Package 1 (Intel® ME on in S0). 4. Set the Intel® AMT WLAN link policy on the SUT to Link Policy 3 (Enabled in S0, Sx/AC), if the WLAN network interface is available. 5. Ensure that the Host OS network device drivers are configured to not wake the SUT. This includes enabling ARP and/or NS Offload features where available to help prevent unexpected host wake events. Most especially, ensure that the Host OS Wireless Wake on LAN driver setting on the SUT is disabled, if the WLAN network interface is available. 6. Ensure that Intel® RMT is disabled, if running on an All-in-One (AIO) SUT with feature support. 7. Verify that Intel® AMT on the SUT responds to version queries via all available network interfaces. 8. Record the Host OS last boot time on the SUT (to verify successful return to S3) 9. Ensure yellow bang is not seen on Drivers in Device Manager 	
Procedure:	<ol style="list-style-type: none"> 1. Suspend the SUT via the Host OS. 2. Verify that the SUT is in S3/MeOff (CM-Off). 3. Verify that a DC battery is connected to the SUT, and that it is charged. 4. Set the SUT power source to DC-only. 5. Verify that the SUT is in S3/MeOff (CM-Off). 6. Set the SUT power source to AC+DC. 7. Verify that the SUT is in S3/MeOff (CM-Off). 8. Briefly press the Power Button on the SUT. 9. Verify that the SUT is in S0/MeOn (CM0,CM0-PG). 10. Verify that the Host OS on the SUT is available. 11. Verify the Host OS last boot time on the SUT matches the boot time recorded before entry into S3. 12. Verify that Intel® AMT on the SUT responds to version queries via all available network interfaces. 13. Ensure yellow bang is not seen on Drivers in Device Manager 	
Pass Criteria:	The test passes if the Intel® CSME stays MeOff when Ac Detached in S3 state and stays MeOff when attached AC Source in S3 state.	
ID:	ME_PM_51.5	
Title:	S0/CM0 to S4/CM-Off to S0/CM0 via AC-detach (PP1)	
Requirement:	Mandatory	Exemptions <input checked="" type="checkbox"/> Non-Mobile (AC-only) systems
		<input checked="" type="checkbox"/> Modern Standby and InstantGo* systems
Method:	Automated by Intel® PETS	
Objective:	This test checks the SUT power flow from S0/CM0 to S4/CM-Off to S0/CM0 via AC-detach with the parameters outlined below.	
Configuration:	<p>Intel® AMT should be provisioned via manual mode.</p> <p>If Deep S4, Deep S5, and/or G3 are supported on the SUT, please confirm the following:</p> <ul style="list-style-type: none"> • the SUT and/or BIOS are properly configured to permit Deep S4/S5 or G3 entry. • the correct Deep Sx policy is applied to the SUT profile in Intel® PETS. <p>This test assumes that either LAN-only, WLAN-only, or both LAN and WLAN network interfaces are available on the SUT.</p>	



ID:	ME_PM_51.5	
Parameters:	System Power Source	
		DC-only
	Power States	Initial S0/MeOn (CM0)
		Final S0/MeOn (CM0)
		Trigger AC-detach in S4 state
Intel® AMT	Power Package	PP1 (Intel® ME on in S0)
	WLAN Link Policy	LP3 (Enabled in S0, Sx/AC) where available
Setup:	<ol style="list-style-type: none"> Set the SUT power source to AC+DC. Bring the SUT to the base state of S0/MeOn (CM0,CM0-PG), and confirm that the Host OS is available. Set the active power package on the SUT to Power Package 1 (Intel® ME on in S0). Set the Intel® AMT WLAN link policy on the SUT to Link Policy 3 (Enabled in S0, Sx/AC), if the WLAN network interface is available. Ensure that the Host OS network device drivers are configured to not wake the SUT. This includes enabling ARP and/or NS Offload features where available to help prevent unexpected host wake events. Most especially, ensure that the Host OS Wireless Wake on LAN driver setting on the SUT is disabled, if the WLAN network interface is available. Ensure that Intel® RMT is disabled, if running on an All-in-One (AIO) SUT with feature support. Verify that Intel® AMT on the SUT responds to version queries via all available network interfaces. Ensure yellow bang is not seen on Drivers in Device Manager 	
Procedure:	<ol style="list-style-type: none"> Hibernate the SUT via the Host OS. Verify that the SUT is in S4/MeOff (CM-Off). Verify that a DC battery is connected to the SUT, and that it is charged. Set the SUT power source to DC-only. Verify that the SUT is in S4/MeOff (CM-Off). Set the SUT power source to AC+DC. Verify that the SUT is in S4/MeOff (CM-Off). Briefly press the Power Button on the SUT. Verify that the SUT is in S0/MeOn (CM0,CM0-PG). Verify that the Host OS on the SUT is available. Verify that windows booted from hibernate i.e. value should be 0x02. "run the following power shell command": Get-WinEvent -ProviderName Microsoft-Windows-Kernel-boot -MaxEvents 10 Where-Object {\$_.message -like "The boot type*"} Verify that Intel® AMT on the SUT responds to version queries via all available network interfaces. Ensure yellow bang is not seen on Drivers in Device Manager 	
Pass Criteria:	The test passes if the Intel® CSME stays MeOff when Ac Detached in S4 state and stays MeOff when attached AC Source in S4 state.	
ID:	ME_PM_51.6	
Title:	S0/CM0 to S5/CM-Off to S0/CM0 via AC-detach (PP1)	
Requirement:	Mandatory	Exemptions <input checked="" type="checkbox"/> Non-Mobile (AC-only) systems <input checked="" type="checkbox"/> Modern Standby and InstantGo* systems
Method:	Automated by Intel® PETS	
Objective:	This test checks the SUT power flow from S0/CM0 to S5/CM-Off to S0/CM0 via AC-detach with the parameters outlined below.	
Configuration:	<p>Intel® AMT should be provisioned via manual mode.</p> <p>If Deep S5 and/or G3 are supported on the SUT, please confirm the following:</p> <ul style="list-style-type: none"> the SUT and/or BIOS are properly configured to permit Deep S5 or G3 entry. the correct Deep Sx policy is applied to the SUT profile in Intel® PETS. <p>This test assumes that either LAN-only, WLAN-only, or both LAN and WLAN network interfaces are available on the SUT.</p>	



ID:	ME_PM_51.6	
Parameters:	System Power Source	
		DC-only
	Power States	Initial S0/MeOn (CM0)
		Final S0/MeOn (CM0)
		Trigger AC-detach in S5 state
Intel® AMT	Power Package	PP1 (Intel® ME on in S0)
	WLAN Link Policy	LP3 (Enabled in S0, Sx/AC) where available
Setup:	<ol style="list-style-type: none"> 1. Set the SUT power source to AC+DC. 2. Bring the SUT to the base state of S0/MeOn (CM0,CM0-PG), and confirm that the Host OS is available. 3. Set the active power package on the SUT to Power Package 1 (Intel® ME on in S0). 4. Set the Intel® AMT WLAN link policy on the SUT to Link Policy 3 (Enabled in S0, Sx/AC), if the WLAN network interface is available. 5. Ensure that the Host OS network device drivers are configured to not wake the SUT. This includes enabling ARP and/or NS Offload features where available to help prevent unexpected host wake events. Most especially, ensure that the Host OS Wireless Wake on LAN driver setting on the SUT is disabled, if the WLAN network interface is available. 6. Ensure that Intel® RMT is disabled, if running on an All-in-One (AIO) SUT with feature support. 7. Verify that Intel® AMT on the SUT responds to version queries via all available network interfaces. 8. Ensure yellow bang is not seen on Drivers in Device Manager 	
Procedure:	<ol style="list-style-type: none"> 1. Suspend the SUT via the Host OS. 2. Verify that the SUT is in S5, Deep S5, G3/MeOff (CM-Off). 3. Verify that a DC battery is connected to the SUT, and that it is charged. 4. Set the SUT power source to DC-only. 5. Verify that the SUT is in S5, Deep S5, G3/MeOff (CM-Off). 6. Set the SUT power source to AC+DC. 7. Verify that the SUT is in S5, Deep S5, G3/MeOff (CM-Off). 8. Briefly press the Power Button on the SUT. 9. Verify that the SUT is in S0/MeOn (CM0,CM0-PG). 10. Verify that the Host OS on the SUT is available. 11. Verify that Intel® AMT on the SUT responds to version queries via all available network interfaces. 12. Ensure yellow bang is not seen on Drivers in Device Manager 	
Pass Criteria:	The test passes if the Intel® CSME stays MeOff when Ac Detached in S5 state and stays MeOff when attached AC Source in S5 state.	

§ §



13 Intel® Trusted Execution Technology (Intel® TXT)

13.1 Introduction

This chapter describes a validation strategy for Intel® Trusted Execution Technology (Intel® TXT) on the Client platforms.

Intel Trusted Execution Technology is part of Intel's Safer Computing Initiative. Intel® TXT provides a security foundation to build protections against software based attacks. For the Client platforms, Intel® TXT provides the capabilities to create a measured launched environment (MLE) and have that MLE verified against a good known environment. For more information, refer to the *Intel® TXT Measured Launched Environment Developer's Guide* in <http://www.intel.com/content/www/us/en/software-developers/intel-txt-software-development-guide.html>.

This chapter is intended for validation purposes. The objective is to provide validation professionals with additional insight into Intel® TXT by highlighting key validation considerations in a bottom-up approach.

This chapter is not a technology overview and does not supplant the existing Intel® TXT collaterals. The readers are expected to be familiar with Intel® TXT and to use this document as a validation supplement to develop their own validation plan.

Intel TXT BIOS Writers Guide should be used to for reference. Document #572782

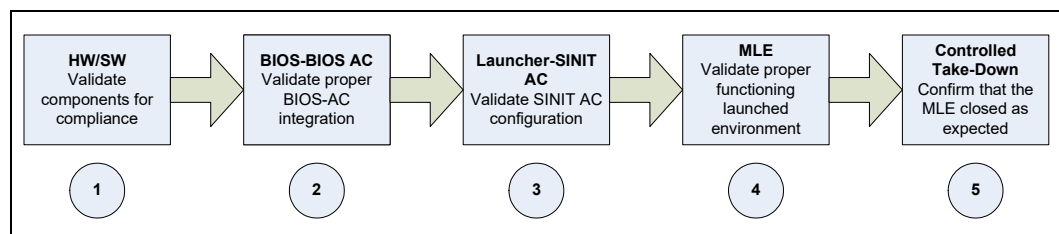
13.1.1 Validation Flow

At the processor and chipset level, Intel Corporation applies rigorous validation to ensure these components perform to specification. Feature focused and random test suites are executed on individual components and in comparable pairing to make sure adequate validation coverage is achieved at both component and platform levels.

The infrastructure that is required to validate the processor and chipset at this silicon level requires extensive development. Due to the effort and the complexity, this low level validation of Intel® TXT is outside the scope of this validation guide. Only the portion of the flow that is applicable by platform suppliers (OEM/ODM) will be described.

To validate Intel® TXT on client platforms, consider the sequence of events that make up an Intel® TXT verified launch (TXT-VL). This is because TXT-VL effectively utilizes the key hardware and software components that define the Intel® TXT feature.

Figure 13-1 diagrams the key components that make up a TXT-VL. The starting point is the Intel® TXT enabled hardware and software components. Second is proper integration of a BIOS AC module into the system BIOS. Third is correct configuration of the system, by the environment launcher to run the SINIT AC module. Fourth is the measured launch environment (MLE) operation. The last stage is a controlled take-down of the MLE.


Figure 13-1. Intel® TXT Verified Launch/Validation Flow


NOTE: Intel® TXT VL will vary depending on the MLE start-up process, however the steps described above will be consistent across MLE launching mechanism.

This document uses the Intel® TXT VL flow as the framework for this bottom-up strategy. The following sections highlight the validation considerations for each step in the flow.

13.2 Pre-requisite

Before proceeding with the checkout process described in this document, there are a few conditions and preparations that should be done to make the checkout most productive.

13.2.1 TPM 1.2 NV Indices Defined and Locked

Note: **The AUX and PS indices creation should not be done as part of the validation process.** Absence of these indices on the SUT indicates that the index creation process either in manufacturing or other processes defined by the platform supplier is not functional.

Make sure the AUX and PS indices are defined as described in “Intel Initiatives Trusted Platform Module (TPM) NV Storage Interface Usage” document. These indices are critical components of the Intel® TXT infrastructure. How and when these indices are defined is up to of the platform supplier. The Intel® TXT requires that the AUX and PS indices are defined in the NV space and that the NV space is enabled and the indices locked before Intel® TXT is used. Refer to the *Intel Initiatives TPM NV Storage Interface Usage* document for information on this requirement.

For the **BIOS development environment**, Intel Corporation provides the TPM provision reference tool as part of the ACM package (refer to Bin directory of the ACM). These scripts that can be used to provision the TPM as required for TXT. Refer to Appendix B.1 “Provisioning the TPM for TXT”.

13.2.2 TPM 2.0 Indices Defined and Hierarchies

Unlike TPM 1.2, where the OEM had to create TPM objects (Example: AUX and PS Policy NVRAM Indexes) and then lock the TPM preventing anyone from deleting or modifying their definitions, TPM 2.0 defines 3 hierarchies that are independent of each other. These are the Platform Hierarchy, Storage Hierarchy, and Endorsement Hierarchy. The Platform Hierarchy is dedicated for the platform vendor, while the Storage Hierarchy and Endorsement Hierarchy are dedicated for the platform owner. This document only deals with the Platform Hierarchy (PH). Each hierarchy has its own



authorization value (AuthValue) and authorization policy (authPolicy). More on authorization policies later, but authPolicy is an alternative way to demonstrate authorization to use the PH.

This means that there is no longer the notion of a LOCKED TPM and the OEM will now be able to add, delete, and provision its TPM objects at any time.

However, **PS index should be locked for TPM 2.0 using PS2 attributes and Production ACMS.** PS2 definition is the preferred choice for OEM/ODM.

PS Index is not required for CBnT Platforms (CML-S, TGL, RKL, Etc).

Unlike the other hierarchies, which have persistent authorization values, the PH authValue and authPolicy are cleared each time the platform resets. It is the BIOS responsibility to establish the PH authValue (and optionally the PH authPolicy) on each platform reset.

The notion is that BIOS will set PH authValue to a random value, use that value, if it needs to perform any operations that require PH authorization and then flush that value from memory (or store it in a protected location) before any executing any untrusted code (option ROMs, boot code, and so forth.).

If the customer platform BIOS chooses to use a random value for platformAuth value, the TPM 2.0 provisioning tool must be modified to match Platform Policy Digest. OR the customer can choose to make a special BIOS mode where platformAuth.

For the BIOS development environment, Intel Corporation provides the TPM provision reference tool as part of the ACM package (refer to Bin directory of the ACM). These scripts that can be used to provision the TPM as required for TXT. Refer to Appendix B.1 "Provisioning the TPM for TXT".

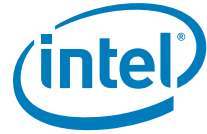
13.2.3 BIOS Setting

Intel® TXT is dependent on Intel® VT, Intel® VT-d a discrete TPM and requires all Processors and Cores to be enabled. Steps to enable TXT in system BIOS:

1. Intel® VT => Enabled
2. Intel® VT-d => Enabled
3. Trusted Platform Module => Enabled
4. If Platform supports dTPM and PTT then follow steps 6 and 7.
5. PCH-FW Configuration => TPM Device Selection => dTPM (Discrete TPM)
6. TPM Configuration => Current TPM Selected Device => 1.2 or 2.0 => Enabled

(Ensure TPM has been correctly provisioned before enabling TXT)

7. Intel® TXT => Enabled
8. DMAR => Disabled
 - a. This is only required for EFI Shell testing. DMAR can be enabled when booting to OS Environment (Tboot, Windows, etc.)



13.2.4 Unblocking Mechanism

A key feature for Intel® TXT on client platforms is *secret protection*. Secret protection relies on the BIOS properly invoking the BIOS AC – SCLEAN. Improperly implemented BIOS can leave the system in a blocked state.

Until BIOS implementation has been thoroughly evaluated, it is beneficial to have a mechanism to unblock the system. The system can be unblocked using a BIOS debugger, such as XDP/ITP or using a BIOS version that unconditionally invoke SCLEAN.

Additional method that may work to unblock a system is to replace the TPM. An unblocking mechanism should be defined before executing the secret protection checkout described in this document.

13.2.5 SINIT ACM

The SINIT ACM is a critical component of the Intel® TXT architecture. Intel® TXT requires this software component for the verified launch feature. Verify that user have the compatible SINIT ACM for the platform being tested. This module is required for the measured launch test cases. Invoking measured launch (SENDER) with an incompatible SINIT ACM will result in an Intel® TXT reset. SINIT ACM can only be launched from a storage device. Running SINIT ACM from flash is not a POR feature on client platforms.

TXTINFO64.efi or TxtBtgInfo.efi can be used to determine SINIT ACM compatibility:

```
EFI> txtinfo64.efi -a <ACM-filename>
```

```
EFI> TxtBtgInfo.efi -a <ACM-filename>
```

13.3 Hardware and Software Components

13.3.1 Check Component Compliance

First validation step is to determine, if the Intel® TXT hardware and software components are enabled and are compatible.

The hardware checks include:

1. Validate that the processor supports SMX and VMX.
2. Verify that the chipset is Intel® TXT capable.
3. Confirm that processor and chipset are compatible.
 - a. Use an engineering sample (ES) CPU with an ES chipset, or a production sample (QS) CPU with a QS chipset.
4. Confirm that the TPM is TCG 1.2 or TPM 2.0 is TCG 2.0 compliant to the extent required by Intel® TXT.
5. TPM should be provisioned using the corresponding scripts released with the ACM package.

**For software checks:**

1. Verify the chipset compatible BIOS ACM is being used.
2. Verify the chipset compatible SINIT ACM is being used.
3. BIOS ACM and SINIT ACM types have to match i.e. Debug with Debug, NPW with NPW, and Production with Production, respectively.

The table below summarizes the allowed combination of hardware and software components (Refer TXT ACM packages for TPM Provisioning tools and instructions):

CPU	PCH	BIOS ACM	TPM Provisioning Type	TPM Lock Required (TPM 1.2 Only)	SINIT ACM	Platform Milestone
ES	ES	Debug (Pre Production)	Pre-Production	No	Debug (Pre Production)	Pre Alpha, Alpha, Beta
QS	QS	NPW (Non Production Worthy)	Production	No	NPW (Non Production Worthy)	PC (Production Candidate)
QS	QS	Production	Production	Yes	Production	PV (Production Version)

13.3.1.1 Processor

TXINFO64.efi, TxtBtGinfo.efi or the CPUID instruction can be used to determine, if the processor is Intel® TXT capable (i.e., supports SMX and VMX).

For more information on CPUID, refer Chapter 3, "Instruction Set Reference, A-M," in the *Intel® 64 and IA-32 Software Developer Manual*, Volume 2A.

13.3.1.2 Chipset

TXINFO64.efi, TxtBtGinfo.efi or the SMX GETSEC[CAPABILITIES] instruction can be used to determine, if the chipset supports Intel® TXT.

For more information on the GETSEC[CAPABILITIES], refer Section 6.2.2.1, "Getsec(Capabilities)" in the *Intel® 64 and IA-32 Software Developer Manual*, Volume 2B.

13.3.1.3 AC Modules

To determine AC module compatibility, check the *Vendor ID* and *Module ID* fields in the AC module header. Make sure they match the chipset *Vendor ID* and *Device ID* of the platform. TXINFO64.efi or TxtBtGinfo.efi will also report the BIOS ACM compatibility. To determine SINIT ACM compatibility, refer to [Section 13.2.5, "SINIT ACM."](#)

For more information on AC Module Identification, refer to the *Intel® Trusted Execution Technology BIOS Specification*.



13.3.1.4 Intel® TXT and Boot Guard Compatibility

Only Production Boot Guard Profiles (0/4/5) are supported for use with TXT. Boot Guard Profile is configured in the FIT during SPI image creation.

13.3.1.5 Intel® TXT and Software Guard Extensions (SGX) Compatibility

If both Intel® TXT and Software Guard Extensions (SGX) are intended to be used on the same platform, a SGX index will be needed for BIOS to keep track of SINIT security version number (SVN), when SINIT ACM is not part of the BIOS code*. This can be done by running SGX script concurrently with TXT TPM provisioning scripts that can be located in the ACM package posted on VIP.

Note: Use the TPM provisioning scripts from the ACM package corresponding to the platform as the TXT TPM provisioning scripts are unique for each platform generation. TPM provisioning via scripts or BIOS needs to happen prior running SGX application.

Refer to Intel® Software Guard Extensions (Intel® SGX) Technology Overview and BIOS Support Summary for more information on SGX.

BIOS Based TPM Provisioning # 550711, will provides details on how to provision the TPM through BIOS.

Note: This collateral is guidance, not a reference tool.

13.4 Tools

13.4.1 Validation Tools

The method described in this document uses the following development tools provided by Intel Corporation.

getsec64.efi can be used to confirm that the systems' hardware and software components can support a measured/verified launch.

txtinfo64.efi is a tool that can be used to investigate common status of TXT capable platform. This tool is also available as part of the *Intel® TXT BIOS Development Kit*. This tool is used on Legacy ACM platforms (CML-U/H and before)

TxtBtgInfo64.efi is a tool that can be used to investigate common status of TXT capable platform. This tool is used on CBnT ACM platforms (CML-S and After)

secrets64.efi a tool that can be used to set the secret flag in the Intel® TXT MLE. This tool is also available as part of the *Intel® TXT BIOS Development Kit*.

MLE – A MLE such as Trusted Boot (**tboot**) LiveImage, which can be used to confirm that BIOS has properly configured Intel® TXT to launch the measured environment. Refer to [Section 13.12.1](#) for tool location.

Trace Enabled ACMs - Under certain debug scenarios it is important to use specially designed trace enabled BIOS ACM or SINIT ACM to capture the internal state of ACM execution during an erroneous condition. These engineering trace enabled ACMs are only provided for special debug purpose on case by case basis.



Note: ACM serial out debug message requires BIOS to explicitly use **0x3F8** port for capturing the serial log.

13.4.1.1 TXTINFO64 Log

For the EFI-shell environment, Intel provides the *txtinfo64.efi* tool. Execute *txtinfo64.efi* in an EFI-shell as follow:

```
EFI> txtinfo64 -c:a
```

```
*****
*                               *
*          CPU Information      *
*                               *
*****
CPU 00 -- ILP
-----
APIC ID                = 0x0
CUID                   = 0x406E2
IA32_BIOS_SIGN_ID      = 0xF
CUID.1.ECX[6] (SMX)    = 1
CUID.1.ECX[5] (VMX)    = 1
CUID.7.EBX[2] (SGX)    = 1
IA32_MTRRCAP[11] (SMRR) = 1
IA32_PLATFORM_ID[52:50] = 0x7
TXT_CTRL_STS MSR[0]    = 1

IA32_FEATURE_CONTROL 3Ah:
[15]  SGX Enable       = 0
[15]  SENTER Global Enable = 1
[14:8] SENTER Local Function Enable = 0x7F
[3]    SMRR Enable     = 0
[2]    Enable VMX outside SMX = 1
[1]    Enable VMX inside SMX = 1
[0]    Lock            = 1

GETSEC[CAPABILITIES] = 0x1FD
Intel(R) TXT-capable chipset is present = 1
ENTERACCS is available = 1
EXITAC is available    = 1
SENTER is available     = 1
SEXIT is available     = 1
PARAMETERS is available = 1
SMCTRL is available     = 1
WAKEUP is available     = 1

CPU[01]...
CPU[02]...
CPU[03]...
-----
APIC ID                = 0x3
CUID                   = 0x406E2
IA32_BIOS_SIGN_ID      = 0xF
```

Confirm **all the processors** detected on the platform are capable and enabled for Intel® TXT. Key checks:

- SMX/VMX supported
- MSR must have SENTER enabled
- All getsec capabilities must be available



```

CPUID.1.ECX[6] (SMX)                = 1
CPUID.1.ECX[5] (VMX)                = 1
CPUID.7.EBX[2] (SGX)                = 1
IA32_MTRRCAP[11] (SMRR)             = 1
IA32_PLATFORM_ID[52:50]              = 0x7
TXT_CTRL_STS MSR[0]                  = 1

IA32_FEATURE_CONTROL 3Ah:
[15]   SGX Enable                    = 0
[15]   SENTER Global Enable          = 1
[14:8] SENTER Local Function Enable  = 0x7F
[3]    SMRR Enable                   = 0
[2]    Enable VMX outside SMX        = 1
[1]    Enable VMX inside SMX         = 1
[0]    Lock                          = 1

GETSEC[CAPABILITIES]                 = 0x1FD
Intel(R) TXT-capable chipset is present = 1
ENTERACCS is available                = 1
EXITAC is available                   = 1
SENER is available                    = 1
SEXIT is available                    = 1
PARAMETERS is available               = 1
SMCTRL is available                   = 1
WAKEUP is available                   = 1

```

```

*****
*                Chipset Information                *
*****
MCH DID                = 0x190C
MCH RID                = 0x3
PCH DID                = 0x9D46
PCH RID                = 0x10
TXT Enable              = 1
MCHBAR + 0x50FC        = 0x8F
B0:D0:F0:0x5C          = 0xAC000047
B0:D0:F0:0xB8          = 0xAC000001
B0:D22:F0:0x6C         = 0x0

```

Chipset
must also
be Intel®
TXT
enabled

```

*****
*                TXT Registers                *
*****
TXT.STS
[16] LOCALITY2-OPEN.STS = 0
[15] LOCALITY1-OPEN.STS = 0
[14] LOCALITY3-OPEN.STS = 0
[11] MEM-CONFIG-OK.STS  = 0
[7]  PRIVATE-OPEN.STS   = 0
[6]  MEM-CONFIG-LOCK.STS = 0
[5]  BASE.LOCKED.STS    = 0

```



```
[4] MEM.UNLOCK.STS = 1
[1] SEXIT.DONE.STS = 1
[0] SENTER.DONE.STS = 0

TXT.ESTS
[6] WAKE-ERROR.STS = 0
[1] ROGUE.STS = 0
[0] TXT_RESET.STS = 0

TXT.ERRORCODE = 0x0
[31] Valid/Invalid = 1
[30] Processor/External = 1
[14:10] ACM Error Code = 0x0
[9:4] ACM Progress Code = 0x0 SINIT Exit Point
[3:0] AC Module Type = 0x1 SINIT

TXT.VER.EMIF[31] = 0
TXT.DIDVID = 0xB0068086
TXT.SINIT.BASE = 0xABED0000
TXT.SINIT.SIZE = 0x00050000
TXT.HEAP.BASE = 0xABF20000
TXT.HEAP.SIZE = 0x000E0000
TXT.DPR = 0xAC000041
TXT.PUBLIC_KEY:
12 CD 5D 03 4E 12 56 50 F1 CC 35 92 23 2E 8E A3
B7 F9 DE 4C 42 4D 5F AF BA 02 D9 CD FD 48 80 B1

*****
* Heap Structures *
*****

BIOS Data
-----
Size = 0x56
Version = 0x6
BiosSinitSize = 0x0
LcpPdBase = 0x0
LcpPdSize = 0x0
NumberOfLogicalProcessors = 0x4
SinitFlags = 0x0
MleFlags = 0x2
[0] TXT/VT-x/VT-d ACPI PPI specification = 0

ExtDataElements:
HEAP_EXT_DATA_ELEMENT.Type = 1
HEAP_EXT_DATA_ELEMENT.Size = E
BIOS spec version element:
Major = 2
Minor = 1
Revision = 0
HEAP_EXT_DATA_ELEMENT.Type = 2
HEAP_EXT_DATA_ELEMENT.Size = 14
BIOS ACM element:
```

Confirm these registers are programmed according the Intel® TXT BIOS Specification

Verify the LCP Version is as required by the SINIT ACM

If TXTINFO is invoked within an Intel® TXT measured environment, this area will display important heap information setup by the Intel® TXT MLE



```

NumAcms                = 0x1
BiosAcm #0 address      = 0xFFF89000

```

```

*****
*                      TPM Information                      *
*****
TPM Offsets from FED40000h:
-----
ACCESS 0h
[0] tpmEstablishment           = 0
[5] activeLocality             = 0
[7] tpmRegValidSts             = 0

VID 0F00h                      = 0x1114
DID 0F02h                      = 0x3203
RID 0F04h                      = 0xFC

...

Platform Supplier 0x50000001 (PS Index)
02 02 00 01 13 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 02 00 00 00 00 00 00 00 00 00
00 00

...

AUX 0x50000003
FF FF FF FF 09 12 14 20 06 B0 00 80 00 01 FF FF
FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF
AF F1 65 2A FF 3C C7 3D 52 B2 9B 44 C5 A7 55 4A
BD 4F 1D 43 84 19 00 00 FF FF FF FF FF FF FF FF
...

```

TPM summary,
confirm:

- AUX and PS indices are defined
- TPM Enabled and activated
- Indices are locked on production systems

Note: PS and Aux Index values will change depending on TPM 1.2 vs. 2.0, Provisioning process and ACM loaded to BIOS

Make sure the Intel® TXT checks are passing before proceeding measured launch

```

-----
SUCCESS: TXT is enabled in the BIOS and platform appears ready for TXT.
-----

```

13.4.1.2 TxtBtgINFO Log

For the EFI-shell environment, Intel provides the *txtbtginfo.efi* tool. Execute *txtbtginfo.efi* in an EFI-shell as follow:

```
EFI> txtbtginfo.efi -c a
```

```

*****
TXTBTGINFO v0.7.31
Built: Jan 28 2020 09:04:16
Intel Corporation
Copyright (c) 2010-2019
*****

```



CPU Type 0x000A0650: Comet Lake
CPU Stepping 0x3: D
CPU 00 -- ILP

```
-----
APIC ID                               = 0x0
CUIDID                               = 0xA0653
8Bh IA32_BIOS_SIGN_ID                 = 0xCC
CUIDID.1.ECX[6] (SMX)                 = 0x1
CUIDID.1.ECX[5] (VMX)                 = 0x1
CUIDID.7.EBX[2] (SGX)                 = 0x1
FEh IA32_MTRRCAP[11] (SMRR)           = 0x1
17h IA32_PLATFORM_ID[52:50]           = 0x1
2E7h TXT_CTRL_STS[0]                  = 0x1
3Ah IA32_FEATURE_CONTROL:
[18]   SGX Enable                     = 0x0
[15]   SENTER Global Enable           = 0x1
[14:8] SENTER Local Function Enable   = 0x7F
[3]    SMRR Enable                     = 0x0
[2]    Enable VMX outside SMX         = 0x1
[1]    Enable VMX inside SMX          = 0x1
[0]    Lock                            = 0x1
GETSEC[CAPABILITIES]                  = 0x1FD
Intel(R) TXT-capable chipset is present = 0x1
ENTERACCS is available                 = 0x1
EXITAC is available                    = 0x1
SENTER is available                    = 0x1
SEXIT is available                     = 0x1
PARAMETERS is available                = 0x1
SMCTRL is available                    = 0x1
WAKEUP is available                    = 0x1
13Ah BOOT_GUARD_SACM_INFO              = 0x7D
-----
```

Confirm **all the processors** detected on the platform are capable and enabled for Intel® TXT. Key checks:

- SMX/VMX supported
- MSR must have SENTER enabled
- All getsec capabilities must be available

TXT.PUBLIC_KEY_HASH:
C1 4A 4B 4B E9 B8 AA 00
1B 65 37 7F E6 89 D2 52
E6 C6 8D CD 66 D3 7B CE
1D A9 76 98 67 D1 0C FD

CPU 01 -- RLP

...

*****Chipset Information*****

```
MCH/IMC DID (PCI 0:0:0:2 [15:0])      = 0x9B53
MCH/IMC RID (PCI 0:0:0:8 [7:0])        = 0x3
ICH/PCH DID (PCI 0:1F:0:2 [15:0])      = 0x687
ICH/PCH RID (PCI 0:1F:0:8 [7:0])        = 0x0

PCU CR Debug Interface                 = 0x40000000
```

*****Registers Information*****

TXT Registers info (Offsets from public space at 0xFED30000):



```

STS: Locality 2 open (0 [16])      0x0
STS: Locality 1 open (0 [15])      0x0
STS: Locality 3 open (0 [14])      0x0
STS: SMM open (0 [13])             0x0
STS: PMRC lock (0 [12])            0x0
STS: Mem CFG OK (0 [11])           0x0
STS: NTP enable (0 [10])           0x0
STS: Private open (0 [7])          0x0
STS: Mem CFG lock (0 [6])          0x0
STS: Mem unlock (0 [4])            0x1
STS: SExit Done (0 [1])            0x1
STS: SEnter Done (0 [0])           0x0
TXT debug mode (200 [31]) 0=debug  0x1
ESTS: Wake error (8 [6])           0x0
ESTS: Rogue status (8 [1])         0x0
ESTS: TXT Reset (8 [0])            0x0
TXT Errorcode (30 [31:0])          0x00000000
    Class Code                     0x0
    Major code                     0x0
    Minor code                     0x0
    Module type                    0x0
TXT ACM status (A0 [63:0])          0x9800000080000000
TXT ACM Errorcode (328 [31:0])      0x008D0000
    Class Code                     0x0
    Major code                     0x0
    Minor code                     0x8D
    Module type                    0x0
VID (110 [15:0])                   0x8086
DID (110 [31:16])                   0xB008
RID (110 [47:32])                   0x1

```

```

DPR Capable (200 [26])             0x1
PMRC Capable (200 [19])            0x0
SINIT base (270 [64:0])            0x9BEC0000
SINIT size (278 [64:0])            0x50000
HEAP base (300 [64:0])             0x9BF10000
HEAP size (308 [64:0])             0xF0000
MSEG base (310 [64:0])             0x0
MSEG size (318 [64:0])             0x0
Top of DPR (330 [31:20][19:0=0])   0x9C000000
DPR size (330 [11:4])              0x4
DPR lock (330 [0])                 0x1

```

Confirm these registers are programmed according the Intel® TXT BIOS Specification

BootGuard Registers (Offsets from public space at 0xFED30000):
 BOOTSTATUS register offset 0xA0: 0x9800000080000000

```

[63] S-ACM success                  : 0x1
[62] CPU error                      : 0x0
[61] CPU hot plug                   : 0x0
[60] TXT policy disable             : 0x1
[59] BIOS trusted                   : 0x1
[47] Memory power down executed: 0x0
[46:32] ACM interal use             : 0x0
[31] BtG startup success            : 0x1
[30] TXT startup success            : 0x0
[29:0] ACM interal use              : 0x0

```



ACM_STATUS register offset 0x328: 0x8D0000

[31] Valid	: 0x0
[30:28] Reserved	: 0x0
[27:16] Minor Error Code	: 0x8D
[15] ACM Started	: 0x0
[14:10] Type2/Major Error Code	: 0x0
[9:4] Type2/Class Code	: 0x0
[3:0] Type2/Module Type	: 0x0

ACM_POLICY_STATUS register offset 0x378: 0x2000D831

[63:37] Reserved	: 0x0
[36] TPM Startup locality	: 0x0
[35] CPU co-signing enabled	: 0x0
[34:32] S-CRTM Status	: 0x0
[31:30] Reserved	: 0x0

[29] IBB DMA Protection	: 0x1
[28:27] Resereved	: 0x0

[26:25] Memory Scrub Policy	: 0x0
[24:20] TXT profile	: 0x0
[19] Backup action	: 0x0
[18:16] Reserved	: 0x0
[15] TPM Success	: 0x1
[14:13] TPM Type	: 0x2

BootPolicies

[12] FWSTS4[11]	: 0x1
[11] BP.RSTR.PBE	: 0x1
[10] BP.RSTR.DBI	: 0x0
[9] BP.RSTR.DCD	: 0x0
[8] BP.TYPE.BM	: 0x0
[7] BP.TYPE.T	: 0x0
[6] BP.TYPE.HAP	: 0x0
[5] BP.TYPE.V	: 0x1
[4] BP.TYPE.M	: 0x1
[3:0] KMID	: 0x1

MSR 13Ah ANC_SACM_INFO : 0x30000007D

[35] No Reset Secrets Protect	: 0x0
[34] ServerTXTCapability	: 0x0
[32] BootGuardCapability	: 0x1
[7] ModuleRevoked	: 0x0
[6] Verified Boot	: 0x1
[5] Measured Boot	: 0x1
[4] FACB	: 0x1
[3] TPMSuccess	: 0x1
[2:1] TPMType	: 0x2
[0] NEMEnabled	: 0x1

MEI-Host Firmware Status Register

40h Host Firmware Status Register #1 0x90000255

[31] D0i3 Support Valid	: 0x1
[30] D3 Support Valid	: 0x0
[29:28] CURRENT POWER SOURCE	: 0x1



```

[27] BIST RESET REQUEST           : 0x0
[26] BIST Test State              : 0x0
[25] Reserved                     : 0x0
[24] Intel ME Boot Options Present : 0x0
[23:20] RESET Count               : 0x0
[19:16] Intel ME Current Operation Mode : 0x0
[15:12] Error Code                : 0x0
[11] FW UPD In Progress           : 0x0
[10] FT BUP LD FLR                : 0x0
[9] FWInitComplete                : 0x1
[8:6] Intel ME Current Operation State : 0x1
[5] FPT Bad                       : 0x0
[4] Manufacturing Mode            : 0x1
[3:0] Intel ME Current Working State : 0x5

48h Host Firmware Status Register #2 0x8B108106
[31:28] Phase                     : 0x8
[27:24] Current PmEvent           : 0xB
[23:16] Status Data               : 0x10
[15] Listener change for host notify : 0x1
[14] IFU Fault Tolerance test state : 0x0
[13] Reserved                     : 0x0
[12] Firmware Update Forced Safe Boot : 0x0
[11] IPU needed state              : 0x0
[10] ME Power Gating Indicator     : 0x0
[9] Low Power State                : 0x0
[8] CPU Replaced Valid             : 0x1
[7] Warm Reset Request             : 0x0
[6] MFS Failure                    : 0x0
[5] Reserved                       : 0x0
[4] CPU Replaced STS                : 0x0
[3] Invoke MEBX                    : 0x0
[2:1] ICC Programming status        : 0x3
[0] NFTP Load Failure detection field : 0x0

60h Host Firmware Status Register #3 0x30
[31:0] Reserved                    : 0x30

64h Host Firmware Status Register #4 0x4000
[31:16] Reserved                   : 0x0
[15] Boot Guard Self-Test           : 0x0
[14] Boot Guard FWSTS Valid         : 0x1
[13] Reserved                       : 0x0
[12] All TPMs Disconnected          : 0x0
[11] Reserved                       : 0x0
[10] Sx Resume Type                 : 0x0
[9] Enforcement Flow                 : 0x0
[8:0] Reserved                      : 0x0

68h Host Firmware Status Register #5 0x1F03
[31] Start Enforcement              : 0x0
[30:29] Reserved                   : 0x0
[28:25] INC_BPM_SVN                 : 0x0
[24:21] INC_KM_SVN                  : 0x0
[20:17] INC_ACM_SVN                 : 0x0

```



```
[16] S-CRTM Indicator           : 0x0
[15:9] Startup Module Timeout Count : 0xF
[8] Boot Guard ACM DONE STS      : 0x1
[7:3] Error Status Code         : 0x0
[2] Result Code Source           : 0x0
[1] Valid Bit                    : 0x1
[0] Boot Guard ACM Active STS    : 0x1
```

6Ch Host Firmware Status Register #6 0x4440BC9

```
[31] TXT Support                 : 0x0
[30] FPF Soc Config Lock         : 0x0
[29] Field Programmable Fuses Disable : 0x0
[28] Boot Guard Disable          : 0x0
[27] Error                       : 0x0
[26] BSP BPM Execution Status     : 0x1
[25:22] Key Manifest ID          : 0x1
[21:18] BPMSVN                   : 0x1
[17:14] KMSVN                    : 0x0
[13:10] ACMSVN                   : 0x2
[9] Verified Boot Policy         : 0x1
[8] Measured Boot Policy         : 0x1
[7:6] Error Enforcement Policy   : 0x3
[5:4] Reserved                   : 0x0
[3] Protect BIOS Environment Policy : 0x1
[2] BSP Initialization Disabled   : 0x0
[1] CPU Debug Disabled           : 0x0
[0] Force Boot Guard ACM Boot Policy : 0x1
```

Boot Profile

```
F | M | V | ENF
1 | 1 | 1 | 03
```

```
*****TPM 2.0 Information*****
TPM info (Offsets from 0xFED40000):
ACCESS 0h
[7] tpmRegValidSts             1
[6] Reserved                   0
[5] activeLocality              1
[4] beenSeized                  0
[3] Seize                       0
[2] pendingRequest              0
[1] requestUse                  0
[0] tpmEstablishment            1

NvIndex                        = 0x1C10103
NameAlg                        = 0xB
Attributes                      = 0x62040408
[31] TPMA_NV_READ_STCLEAR      = 0x0
[30] TPMA_NV_PLATFORMCREATE    = 0x1
[29] TPMA_NV_WRITTEN           = 0x1
[28] TPMA_NV_READLOCKED        = 0x0
[27] TPMA_NV_CLEAR_STCLEAR     = 0x0
[26] TPMA_NV_ORDERLY           = 0x0
[25] TPMA_NV_NO_DA             = 0x1
```

TPM summary,
confirm:

- AUX index is defined
- Please see all other Index's below if needed



```

[24:20] Reserved          = 0x0
[19] TPMA_NV_POLICYREAD   = 0x0
[18] TPMA_NV_AUTHREAD     = 0x1
[17] TPMA_NV_OWNERREAD    = 0x0
[16] TPMA_NV_PPREAD       = 0x0
[15] TPMA_NV_GLOBALLOCK   = 0x0
[14] TPMA_NV_WRITE_STCLEAR = 0x0
[13] TPMA_NV_WRITEDEFINE   = 0x0
[12] TPMA_NV_WRITEALL      = 0x0
[11] TPMA_NV_WRITELOCKED   = 0x0
[10] TPMA_NV_POLICY_DELETE = 0x1
[9:7] Reserved            = 0x0
[6] TPMA_NV_EXTEND         = 0x0
[5] TPMA_NV_BITS           = 0x0
[4] TPMA_NV_COUNTER        = 0x0
[3] TPMA_NV_POLICYWRITE    = 0x1
[2] TPMA_NV_AUTHWRITE      = 0x0
[1] TPMA_NV_OWNERWRITE     = 0x0
[0] TPMA_NV_PPWRITE        = 0x0

AuthPolicy Size: 0x0020
AuthPolicy Digest:
C0 01 C8 00 02 10 D0 FA A4 F4 F4 F8 A7 8E F4 F8
26 4E 6F 85 55 34 0D 2F 04 18 0F 8C F1 10 FF DD

DataSize:          0x0046
Name Size:         0x0022
Name:
00 0B 40 7B A7 8D 90 B7 CF 3A A5 3C 0B 83 6D AE
A7 2A E6 B5 67 15 32 BD 4E EF E4 04 E3 7E A4 EB
B0 19

Index: 0x1C10103
Data Size: 0x46
Index Data:
00 03 0B 00 01 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 02 00 00 00 00 00 00 C8 00 08 30
00 00 08 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00

NvIndex          = 0x1C10106
NameAlg          = 0xB
Attributes       = 0x2204000A
[31] TPMA_NV_READ_STCLEAR   = 0x0
[30] TPMA_NV_PLATFORMCREATE = 0x0
[29] TPMA_NV_WRITTEN        = 0x1
[28] TPMA_NV_READLOCKED     = 0x0
[27] TPMA_NV_CLEAR_STCLEAR  = 0x0
[26] TPMA_NV_ORDERLY        = 0x0
[25] TPMA_NV_NO_DA          = 0x1
[24:20] Reserved          = 0x0
[19] TPMA_NV_POLICYREAD     = 0x0
[18] TPMA_NV_AUTHREAD       = 0x1
[17] TPMA_NV_OWNERREAD      = 0x0
[16] TPMA_NV_PPREAD         = 0x0
[15] TPMA_NV_GLOBALLOCK     = 0x0

```



```
[14] TPMA_NV_WRITE_STCLEAR = 0x0
[13] TPMA_NV_WRITEDEFINE = 0x0
[12] TPMA_NV_WRITEALL = 0x0
[11] TPMA_NV_WRITELOCKED = 0x0
[10] TPMA_NV_POLICY_DELETE = 0x0
[9:7] Reserved = 0x0
[6] TPMA_NV_EXTEND = 0x0
[5] TPMA_NV_BITS = 0x0
[4] TPMA_NV_COUNTER = 0x0
[3] TPMA_NV_POLICYWRITE = 0x1
[2] TPMA_NV_AUTHWRITE = 0x0
[1] TPMA_NV_OWNERWRITE = 0x1
[0] TPMA_NV_PPWRITE = 0x0

AuthPolicy Size: 0x0020
AuthPolicy Digest:
22 03 0B 7E 0B B1 F9 D5 06 57 57 1E E2 F7 FC E1
EB 91 99 0C 8B 8A E9 77 FC B3 F1 58 B0 3E BA 96

DataSize: 0x0046
Name Size: 0x0022
Name:
00 0B 8D D1 B6 DE A2 9D 5B 82 D7 1B 04 84 83 D6
A9 BF DE B1 A9 34 46 AA 96 09 FF D6 AF BE BC 95
7C 19

Index: 0x1C10106
Data Size: 0x46
Index Data:
01 03 0B 00 01 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 02 00 00 00 00 00 C8 00 08 30
00 00 08 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00

NvIndex = 0x1C10102
NameAlg = 0xB
Attributes = 0x62044408
[31] TPMA_NV_READ_STCLEAR = 0x0
[30] TPMA_NV_PLATFORMCREATE = 0x1
[29] TPMA_NV_WRITTEN = 0x1
[28] TPMA_NV_READLOCKED = 0x0
[27] TPMA_NV_CLEAR_STCLEAR = 0x0
[26] TPMA_NV_ORDERLY = 0x0
[25] TPMA_NV_NO_DA = 0x1
[24:20] Reserved = 0x0
[19] TPMA_NV_POLICYREAD = 0x0
[18] TPMA_NV_AUTHREAD = 0x1
[17] TPMA_NV_OWNERREAD = 0x0
[16] TPMA_NV_PPREAD = 0x0
[15] TPMA_NV_GLOBALLOCK = 0x0
[14] TPMA_NV_WRITE_STCLEAR = 0x1
[13] TPMA_NV_WRITEDEFINE = 0x0
[12] TPMA_NV_WRITEALL = 0x0
[11] TPMA_NV_WRITELOCKED = 0x0
[10] TPMA_NV_POLICY_DELETE = 0x1
[9:7] Reserved = 0x0
```



```

[6] TPMA_NV_EXTEND           = 0x0
[5] TPMA_NV_BITS             = 0x0
[4] TPMA_NV_COUNTER          = 0x0
[3] TPMA_NV_POLICYWRITE      = 0x1
[2] TPMA_NV_AUTHWRITE        = 0x0
[1] TPMA_NV_OWNERWRITE       = 0x0
[0] TPMA_NV_PPWRITE          = 0x0
AuthPolicy Size: 0x0020
AuthPolicy Digest:
EF 9A 26 FC 22 D1 AE 8C EC FF 59 E9 48 1A C1 EC
53 3D BE 22 8B EC 6D 17 93 0F 4C B2 CC 5B 97 24

DataSize: 0x0068
Name Size: 0x0022
Name:
00 0B 87 7A 0A B0 02 23 4B C3 A3 61 5C 81 9A BF
20 C3 0A 5F 2A F9 3F B6 DC 13 F3 B9 B0 59 90 F4
5A FB

Index: 0x1C10102
Data Size: 0x68
Index Data:
02 00 00 00 00 00 00 00 10 01 20 20 0C B0 00 00
00 03 00 00 00 00 00 00 00 00 00 00 01 00 01 01
F2 CB 0B 00 D7 E6 00 F9 40 08 B7 95 53 93 11 CC
8C E4 30 4F 84 AC EB C9 8D 13 B3 0C 52 AE 9B E1
80 D1 E7 2C 00 00 00 00 00 00 00 00 00 00 00 00
06 55 54 01 00 00 00 00 00 00 00 00 00 00 00 00
02 00 00 00 00 00 00 00

NvIndex = 0x1C10104
NameAlg = 0xB
Attributes = 0x62040404
[31] TPMA_NV_READ_STCLEAR = 0x0
[30] TPMA_NV_PLATFORMCREATE = 0x1
[29] TPMA_NV_WRITTEN = 0x1
[28] TPMA_NV_READLOCKED = 0x0
[27] TPMA_NV_CLEAR_STCLEAR = 0x0
[26] TPMA_NV_ORDERLY = 0x0
[25] TPMA_NV_NO_DA = 0x1
[24:20] Reserved = 0x0
[19] TPMA_NV_POLICYREAD = 0x0
[18] TPMA_NV_AUTHREAD = 0x1
[17] TPMA_NV_OWNERREAD = 0x0
[16] TPMA_NV_PPREAD = 0x0
[15] TPMA_NV_GLOBALLOCK = 0x0
[14] TPMA_NV_WRITE_STCLEAR = 0x0
[13] TPMA_NV_WRITEDEFINE = 0x0
[12] TPMA_NV_WRITEALL = 0x0
[11] TPMA_NV_WRITELOCKED = 0x0
[10] TPMA_NV_POLICY_DELETE = 0x1
[9:7] Reserved = 0x0
[6] TPMA_NV_EXTEND = 0x0
[5] TPMA_NV_BITS = 0x0
[4] TPMA_NV_COUNTER = 0x0
[3] TPMA_NV_POLICYWRITE = 0x0

```



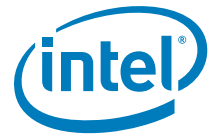
```
[2] TPMA_NV_AUTHWRITE      = 0x1
[1] TPMA_NV_OWNERWRITE     = 0x0
[0] TPMA_NV_PPWRITE        = 0x0
AuthPolicy Size: 0x0020
AuthPolicy Digest:
B7 5C E1 94 6F 78 DF 8B AA 42 69 18 DB 09 31 80
17 E6 B3 8D 04 8C 95 4E 05 C2 C4 F3 4B D4 40 60

DataSize:      0x0008
Name Size:     0x0022
Name:
00 0B 3E CE D2 44 B7 B3 E8 33 3D A2 A8 C5 5E 9A
40 22 02 E1 C4 45 E8 D3 5D EE 0F C5 EE 17 8A 05
54 53

Index: 0x1C10104
Data Size: 0x8
Index Data:
00 00 00 00 00 00 00 00 00
```

```
PCR Update Counter: 0x6E
Hash Algorithm: 0xB
Size of Select: 0x3
PCR Select[0]: 0xFF
PCR Select[1]: 0x0
PCR Select[2]: 0x0
Digest Count: 0x8
TPM2 PCR 0: 30 67 97 35 EF CE 05 EB 5C 38 FB 75 AD 2D E8 68 35 AA 99 49 5D 09 08
B0 FA 7C A0 29 88 9C C0 29
TPM2 PCR 1: 76 D2 8E 64 F5 8E CE 63 04 CA 7F D6 EE 4C 07 B5 42 D0 DE 30 97 50 AF
BA F5 18 E2 23 49 85 E9 F3
TPM2 PCR 2: 19 74 2D A9 5A 28 D3 A1 B6 3D 51 DD A9 0C 3A F0 28 C4 F1 A2 E0 B6 2D
1B 81 EB 18 5D A9 FD D5 6B
TPM2 PCR 3: 3D 45 8C FE 55 CC 03 EA 1F 44 3F 15 62 BE EC 8D F5 1C 75 E1 4A 9F CF
9A 72 34 A1 3F 19 8E 79 69
TPM2 PCR 4: CA 70 64 97 92 97 78 69 00 B4 6F 3E DF 7C B5 70 3B ED D1 69 48 FA C6
34 69 BA 25 EE 0F F6 2F C6
TPM2 PCR 5: 3D 45 8C FE 55 CC 03 EA 1F 44 3F 15 62 BE EC 8D F5 1C 75 E1 4A 9F CF
9A 72 34 A1 3F 19 8E 79 69
TPM2 PCR 6: 3D 45 8C FE 55 CC 03 EA 1F 44 3F 15 62 BE EC 8D F5 1C 75 E1 4A 9F CF
9A 72 34 A1 3F 19 8E 79 69
TPM2 PCR 7: CF 57 D9 5C CA 3D C2 B1 B6 AE EB 25 0B 52 26 39 0D AB 1D BC A1 F5 C5
69 29 60 A5 3B D2 7C 17 7D
```

```
PCR Update Counter: 0x6E
Hash Algorithm: 0xB
Size of Select: 0x3
PCR Select[0]: 0x0
PCR Select[1]: 0xFF
PCR Select[2]: 0x0
Digest Count: 0x8
TPM2 PCR 0: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00
TPM2 PCR 1: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00
TPM2 PCR 2: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00
```



```

TPM2 PCR 3: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00
TPM2 PCR 4: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00
TPM2 PCR 5: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00
TPM2 PCR 6: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00
TPM2 PCR 7: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00

```

```

PCR Update Counter: 0x6E
Hash Algorithm: 0xB
Size of Select: 0x3
PCR Select[0]: 0x0
PCR Select[1]: 0x0
PCR Select[2]: 0xFF
Digest Count: 0x8
TPM2 PCR 0: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00
TPM2 PCR 1: FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF
FF FF FF FF FF FF FF FF FF FF
TPM2 PCR 2: FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF
FF FF FF FF FF FF FF FF FF FF
TPM2 PCR 3: FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF
FF FF FF FF FF FF FF FF FF FF
TPM2 PCR 4: FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF
FF FF FF FF FF FF FF FF FF FF
TPM2 PCR 5: FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF
FF FF FF FF FF FF FF FF FF FF
TPM2 PCR 6: FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF
FF FF FF FF FF FF FF FF FF FF
TPM2 PCR 7: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00

```

Not in TXT environment

*****Heap Information*****

BIOS Data

TXT Heap BiosData

Size = 0x56

Version = 0x6

BiosSinitSize = 0x0

LcpPdBase = 0x0

LcpPdSize = 0x0

NumLogProcs = 0xC

SinitFlags = 0x0

MleFlags = 0x2

[2:1] 1 = Client, 2 = Server = 2

[0] TXT/VT-x/VT-d ACPI PPI Spec = 0

ExtDataElements:

HEAP_EXT_DATA_ELEMENT.Type = 1

HEAP_EXT_DATA_ELEMENT.Size = E

BIOS spec version element:

Major = 2

Minor = 1

Verify the LCP
Version is as
required by the
SINIT ACM

If TXTINFO is invoked
within an Intel® TXT
measured environment,
this area will display
important heap
information setup by
the Intel® TXT MLE
(additional heap info)



```
Revision                      = 0
HEAP_EXT_DATA_ELEMENT.Type    = 2
HEAP_EXT_DATA_ELEMENT.Size    = 14
BIOS ACM element:
  NumAcms                     = 0x1
  BiosAcm #0 address          = 0xFFE60000
```

*****FIT Information*****

```
Firmware Interface Table address: 0xFFFFFC0
Number of FIT entries = 14
Type 7F (Empty) entries will be omitted from output
Entry 0  FIT Header  _FIT_
Address                      0x2020205F5449465F
Size                         0x0E
Version                      0x0100
Type                         0x00
C_V                         0x01
Checksum                     0xCA

Entry 1  uCode Patch
Address                      0x60
Size                         0x00
Version                      0x0100
Type                         0x01
C_V                         0x00
Checksum                     0x00

Entry 2  uCode Patch
Address                      0x6460
Size                         0x00
Version                      0x0100
Type                         0x01
C_V                         0x00
Checksum                     0x00

Entry 3  uCode Patch
Address                      0xC860
Size                         0x00
Version                      0x0100
Type                         0x01
C_V                         0x00
Checksum                     0x00

Entry 4  uCode Patch
Address                      0x3460
Size                         0x00
Version                      0x0100
Type                         0x01
C_V                         0x00
Checksum                     0x00

Entry 5  uCode Patch
Address                      0x9C60
Size                         0x00
```




Version	0x0100
Type	0x01
C_V	0x00
Checksum	0x00
Entry 6 BIOS AC MODULE	
Address	0x00000000FFE60000
Size	0x00
Version	0x0100
Type	0x02
C_V	0x00
Checksum	0x00
Entry 7 SBIOS Region	
Address	0x0
Size	0x8000
Version	0x0100
Type	0x07
C_V	0x00
Checksum	0x00
Entry 8 SBIOS Region	
Address	0x0
Size	0xA000
Version	0x0100
Type	0x07
C_V	0x00
Checksum	0x00
Entry 9 SBIOS Region	
Address	0x0
Size	0x1B44
Version	0x0100
Type	0x07
C_V	0x00
Checksum	0x00
Entry 10 SBIOS Region	
Address	0xBF40
Size	0x40C
Version	0x0100
Type	0x07
C_V	0x00
Checksum	0x00
Entry 11 TXT TYPE A RECORD	
Address	0x0070
Data Register IO Address	0x0071
Access Width in Bytes	0x01
Bit Position	0x04
Index	0x002A
Size	0x00
Version	0x0000
Type	0x0A
C_V	0x00



Checksum	0x00
Entry 12 KEY MANIFEST	
Address	0xB440
Size	0x255
Version	0x0100
Type	0x0B
C_V	0x00
Checksum	0x00

Entry 13 BOOT POLICY MANIFEST	
Address	0xB840
Size	0x3A1
Version	0x0100
Type	0x0C
C_V	0x00
Checksum	0x00

*****BootGuard Information*****

Boot Policy Manifest

BPM Header @ 0xFFFFB840

StructureID:	__ACBP__
StructureID[8]:	5F5F414342505F5F
StructVersion:	0x21
HdrStructVersion:	0x20
HdrSize:	0x14
KeySignatureOffset:	0x190
BPMRevision:	0x01
BpmRevocation:	0x01
AcmRevocation:	0x02

Reserved:	0x0000
-----------	--------

NEMPAGES:	0x0003
-----------	--------

IBB Element @ 0xFFFFB854

StructureID:	__IBBS__
StructureID[8]:	5F5F494242535F5F
StructVersion:	0x20
Reserved0:	0x00
ElementSize:	0x114
Reserved1:	0x00
SetType:	0x00
Reserved:	0x00
PBETValue:	0x0F
Flags:	0x00000003
[31:5] Reserved	0x0
[4] TS support	0x0
[3] TPMFailureAction	0x0
[2] AuthorityMeasure	0x0
[1] InitialMeasureLoc3	0x1
[0] Enable VT-d	0x1



```

IBB_MCHBAR:          0xFED10000
VTD_BAR:             0xFED90000
DmaProtBase0:        0x100000
DmaProtLimit0:       0xF00000
DmaProtBase1:        0x00000000
DmaProtLimit1:       0x01000000
PostIBBHash:
  Hash Structure
    HashAlg:          0x0010
    Size:             0x0000
    hashBuffer:       NULL
    EntryPoint:       0xFFFFFFFF0
  HashList           (Number of Digests: 4, Total Size: 152)
    [0] HashAlg:      0x000B
        Size:        0x0020
        HashBuffer:
BD0C4B7C2595F2A527954D30761D56208B785DB1E3F24BD9ADD950666
B644E76
    [1] HashAlg:      0x0004
        Size:        0x0014
        HashBuffer:
26042CEA150CD595794A300B09F1C28F76FEF565
    [2] HashAlg:      0x000C
        Size:        0x0030
        HashBuffer:
8663C53C7D2875D120C8E2F0508C1661995510E03054F211077C65AEB
0F12823306E909FA735EBDA2245D0D2890EABE5
    [3] HashAlg:      0x0012
        Size:        0x0020
        HashBuffer:
B0397153A3C75E56A386F7A619F7EF24149A85B26E2EF4EED4FF98789
9CE7093
  OBB Hash:
    Hash Structure
      HashAlg:        0x0010
      Size:           0x0000
      hashBuffer:     NULL
      Reserved:       000 000 000
      IBB Segment Count: 0x04
      IBB Segment     0
      Reserved         0x00, 0x00
      Flags:           0x0000
      [15:1] Reserved 0x00
      [0] SegmentType 0 (0: Hashed, 1: Non-Hashed)
      Base:            0xFFEA0000
      Size:            0x00080000
      IBB Segment      1
      Reserved         0x00, 0x00
      Flags:           0x0000
      [15:1] Reserved 0x00
      [0] SegmentType 0 (0: Hashed, 1: Non-Hashed)
      Base:            0xFFFF20000
      Size:            0x000A0000
      IBB Segment      2
      Reserved         0x00, 0x00
      Flags:           0x0000

```



```
[15:1] Reserved      0x00
[0] SegmentType      0 (0: Hashed, 1: Non-Hashed)
Base:                0xFFFE0000
Size:                0x0001B440
IBB Segment         3
Reserved            0x00, 0x00
Flags:              0x0000
[15:1] Reserved      0x00
[0] SegmentType      0 (0: Hashed, 1: Non-Hashed)
Base:                0xFFFFBF40
Size:                0x000040C0
```

TXT Element @ 0xFFFFB968

```
-----
StructureID:         __TXTS__
StructureID[8]:      5F5F545854535F5F
StructVersion:       0x20
Reserved0:           0x00
ElementSize:         0x0028
Reserved:            0x0000
SetNumber:           0x0000
Reserved:            0x0000
Control Flags:       0x00000000
.....TXT Profile: - Default
.....Scrub Policy: - Trust Verified BIOS
.....Backup Policy: - Default
.....AUX Reset Control: - AUX Reset
Power Down Interval: 0x003E
PwrDown Interval:    62 (310 Seconds or f Minutes)
CMOS byte 0 offset:  0xFE
CMOS byte 1 offset:  0xFF
ACPI BASE offset:    0x0400
Reserved:            0x0000
PWRM BASE offset:    0xFE000000
Digest List:
HashList             (Number of Digests: 0, Total Size: 4)
Reserved:            000 000 000
SegmentCount:        0x00
--No Segments
```

Platform Configuration Data Element @ 0xFFFFB990

```
-----
StructureID:         __PCDS__
StructureID[8]:      5F5F504344535F5F
StructVersion:       0x20
Reserved0:           0x00
ElementSize:         0x34
Reserved1W:          0x0000
SizeofData:          0x0024
```

Power Down Request Structure @ 0xFFFFB9A0

```
-----
StructureID:         __PDRS__
StructureID[8]:      5F5F504452535F5F
StructVersion:       0x10
```



```

SizeOfData:          0x0019
Reserved:            0x00
MediaType:           0x00
NVIndex:             0x50000004
BitFieldWidth:       0x03
BitFieldPosition:    0x00
ByteOffset:          0x07
MediaType:           0x01
NVIndex:             0x01C10104
BitFieldWidth:       0x03
BitFieldPosition:    0x00
ByteOffset:          0x07
MediaType:           0x02
NVIndex:             0x01C10104
BitFieldWidth:       0x03
BitFieldPosition:    0x00
ByteOffset:          0x07

```

BPM Signature Element @ 0xFFFFB9C4

```

-----
StructureID:          __PMSG__
StructureID[8]:       5F5F504D53475F5F
StructVersion:        0x20
Key Signature Structure
  Version:            0x10
  KeyAlg:              0x0001
RSA Pub Key Structure
  Version:            0x10
  KeySizeBits:        0x0800
  Exponent:           0x00010001
  Modulus:
    13 15 84 20 E2 E2 D1 FB 84  7E 49 A7 99 4D F9 57 EF
    DF CC 97 5B 82 38 AA 21  91 E9 8C 24 62 0D B1 63
    B9 D3 4B A8 F1 E9 6B 40  8E C8 17 32 91 32 4C 25
    AD E3 8A 3F 2C 77 08 1E  4F 19 55 01 12 FB 5C 90
    55 E2 E5 76 42 EC C0 41  1F E7 EC 96 5F 1E AB 8F
    9C 24 D6 26 90 A8 4E 3A  51 E5 14 93 1C 86 04 9B
    65 74 43 8D 99 7C 79 50  31 36 E9 97 91 92 C6 6B
    A8 AA 4F 7D B7 7A 76 0F  BA 35 21 74 B6 04 8B F5
    A0 82 0C 0B 30 87 E3 2F  75 D7 2E F2 7D DC 70 E8
    B2 80 7D 39 F1 C4 91 40  EC 12 5E 7A 44 5C C7 22
    C7 80 9E 56 3F 99 09 35  CE 33 F8 E4 B2 5C 44 33
    FD D7 3D 31 EC 21 36 FD  12 06 F1 96 78 CB CE A8
    B6 4C 58 C2 B7 A8 DD EA  5D AE E5 4A 28 9B 5F 6C
    8A B8 F8 69 8D 97 7A 24  1C BF 74 C5 B1 02 EA 0E
    65 0B D0 D5 40 5F 6B DC  9B CF EC 40 D1 DD 6A F2
    C7 29 4E B8 80 A1 6B CF  8E 3B 1C 28 40 69 E0 E4

SigScheme:            0x0014
RSASSA Signature Structure
  Version:            0x10
  KeySizeBits:        0x0800
  HashAlg:            0x000B
  Signature:
    82 88 4D 6E B7 6A 7B 79  71 DA BE 2C 8D 07 B3 3D
    48 DB F8 FF 13 7A 8F 85  FF 79 94 65 F7 38 C0 35
    C9 BA E1 39 0B BE 1F CA  B0 1B 37 07 5C 05 7C 14

```



```
DA 2B 53 48 C4 9F 6C AA D9 6B 62 8F B2 0D AA 45
D5 A9 A9 1D 38 88 8F 05 EC 38 52 86 74 3B E6 A5
4C 00 DB 9F E2 68 DF 02 6F 6C 2F B7 7B 4E 1D 25
69 60 AA BA FE EE CF B5 78 FF 7B AE C8 C1 89 DD
7B EE D4 23 9A 52 F8 F9 02 6B DB F9 5C 78 FC E3
88 22 8F 7A E2 2F 80 88 94 C7 88 13 FF 41 16 70
A5 1D 39 C4 96 A1 59 69 E1 D3 21 1C 46 84 CE 4B
BB 01 A9 DC 7D 0E 94 3D 87 4F E6 FA 95 9C 52 E6
52 12 14 BB DE FF 5A D6 87 8F B2 35 AE B2 F1 7B
78 AA A7 1B 3D C4 DD 67 CD 64 4A B4 27 3E D2 0A
2D E8 AE BE 9D C9 9F FA D5 5B CB 1C E9 77 24 88
E8 30 3D DA 76 3A 47 38 A7 20 ED 3B EA 3E 02 83
11 9B 8D FC B6 25 E0 18 38 B1 20 B5 10 D0 4D E4
```

Key Manifest

```
StructureID[8]:      _KEYM_
StructureID[8]:      5F5F4B45594D5F5F
StructVersion:      0x21
Reserved:            0x00 0x00 0x00
KeySignatureOffset:  0x44
Reserved:            0x00 0x00 0x00
StructVersion:      0x21
KeyManifestRevision: 0x01
KeyManifestRevision: 0x01
KMSVN:              0x00
KeyManifestID:      0x01
KmPubKeyHashAlg:    0x000B
KeyCount:           0x0001
KeyHash:
Hash Structure
  Usage:             0x0001
  HashAlg:           0x000B
  DigestSize:        0x0020
hashBuffer:         D5 50 2F F0 61 69 9F 9E 2B 7C 64 AB 41 37 4F 56
                   AE 6F 45 DB 87 0D DB A4 73 3D DC 30 32 38 78 BB
```

Key Signature Structure

```
Version:            0x10
KeyAlg:             0x0001
RSA Pub Key Structure
  Version:          0x10
  KeySizeBits:      0x0800
  Exponent:         0x00010001
  Modulus:          FF 84 9B 32 FF 8A 95 6B 59 49 86 8D 61 91 01 65
                   1A 35 AE 51 18 2A 8F 55 05 92 A8 2F F1 4E 96 40
                   3F 35 C2 FA D4 03 C8 F9 13 10 F0 E4 AD CF 74 7C
                   62 A0 80 5D 40 D8 80 2E 47 40 24 DF FD 02 28 89
                   91 08 6A D8 18 AF B8 3A 96 7D BE E0 73 A9 4B 20
                   FA 09 57 51 E6 BE 3D 43 78 C9 94 29 F5 AF 93 B1
                   B3 03 A5 88 6B C7 D7 28 F4 51 EF F0 F2 3A 0A F9
                   81 2E B6 C5 5B 9B 12 75 FA EB D1 6A CE DB 9F 52
                   B0 8A 5C E7 80 2E 09 71 12 6F A6 91 0A CE 7A 70
                   B1 32 84 E9 A1 2E 3F 4F 95 3D E9 3E C0 B1 94 1A
                   2B 7E 6F 47 C7 14 E2 D5 CB 48 1A 42 30 C8 B8 03
                   28 15 18 3A A3 2E 5B 19 97 14 50 63 17 6D DA 64
```



```

24 85 C2 71 64 9D 6F E2  90 07 60 B5 27 C8 6F 51
6D E7 3F 5C 77 7A 29 AA  54 17 3A 2F 3B 51 D0 71
3C 4F 4C 8C EE B8 B0 BC  38 69 D5 AB A0 74 37 96
D8 F6 50 01 37 1E EA 7B  B1 A1 47 2D 67 CE 5D BF

```

```

SigScheme:          0x0014
RSASSA Signature Structure
Version:            0x10
KeySizeBits:        0x0800
HashAlg:            0x000B
Signature:          0A 26 A1 80 88 77 23 A4  02 B5 1C 80 3A DE 63 C4
DE 4A 82 5C 99 D5 CD 61  4A B1 C7 CF 32 6B D6 D8
D3 6B 26 3F 02 04 7B 45  49 57 43 CC D4 56 28 52
02 F7 C0 EB F8 5C A3 77  58 21 8F 46 5E F8 8B D2
04 C2 7B 03 C0 85 AB 9A  F3 05 C0 1C 00 2E 22 8C
62 2B FD 57 29 23 F8 42  E0 7C ED 35 8F 90 80 9A
BD E8 63 F6 06 87 48 5C  F4 C7 D0 63 3C 6A 0C 56
FF 6B 9F 68 BC FE 9E F5  57 B6 B5 99 BB 89 55 43
0B 09 82 71 5A 64 56 E4  DF 65 89 89 EC 08 31 85
A4 F6 1F C2 1A 93 E2 E7  0E 84 99 CD 26 D8 BD 0A
F1 B6 1C 73 22 3F E8 44  4F A9 B4 EF 62 A0 C1 18
1F A4 C7 7D D0 15 CD 73  41 87 56 50 0B 09 05 C6
42 CF A5 F9 78 EB CC F1  7B 1E 48 0F A1 85 08 BC
E5 DB 92 06 5C C2 8B 68  2F C3 C4 67 79 7A B3 AC
7F 98 CE 16 E5 E8 A5 5B  AF 5F BA 29 C0 24 8F 95
02 A1 2A 68 BE D9 DB 57  DE 25 5E 05 0F 57 10 94

```

*****ACM Information*****

```

START LOG BIOS AC MODULE HEADER
MODULETYPE VAL          = 0x2
HEADER LENGTH           = 0xA1
HEADER VERSION          = 0x0
CHIPSET ID              = 0xB00C
MODULE VENDOR            = 0x8086
MODULE DATE              = 0x20200110
MODULE SIZE (32-bit quants) = 26112
MODULE TxtSvn           = 3
MODULE SeSvn            = 3
MODULE FLAGS            = 0x0
END LOG BIOS AC MODULE HEADER
BIOS ACM found in flash part at address 0xFFE60000

```

ACM file info (Offsets from 0xFFE60000):

```

Module type              = 0x2
Header length            = 0xA1
Header version           = 0x0
Chipset ID               = 0xB00C
Flags                    = 0x0
    ACM is Production module.

```

```

    ACM is production chipset key signed.
    Make sure the chipset is also production
Module vendor            = 0x8086
Module date              = 0x20200110

```



Module size = 0x6600
TXT Svn = 0x3
Code control = 0x0
Error entry point = 0x0
GDT size = 0x20
GDT base pointer offset = 0x42E4
Segment selector = 0x8
Module entry point = 0xC001
Key size = 0x40
Scratch field size = 0x8F

Module public key:

C7 1A C1 E2 A4 57 E7 FC AA 58 55 72 AF E2 BA AB FC FC 17 BA
FB C5 EE D9 71 E1 28 83 A2 68 F7 EA 6E 2C 97 38 F4 93 D7 F5
97 14 4B 1A F3 F1 87 15 68 39 78 3C 50 33 92 C9 20 88 F8 9C
75 BD BC 43 0E 9B A6 3D E6 89 0C AC 5F 22 17 79 09 D7 C2 CF
CD A3 13 F0 C7 E2 99 93 25 58 B7 40 3B D1 D2 DF B4 87 4F 4F
C7 DC E3 45 24 D8 96 40 4B 64 FA 1E 88 AF 63 49 43 98 27 F1
39 24 3F 4B D6 3A E2 97 E2 35 3A 58 37 F0 ED 05 70 1F 05 7E
39 BA F3 BD 80 07 F1 A1 AD 52 BA E4 09 64 46 5E 1D 04 30 4B
63 22 1D C2 FB 5F D2 A6 2D 2A E7 DB 2F D4 7F 62 C9 93 F4 90
F5 C7 F4 3E AB C6 B4 5D B2 0E CC 69 86 35 50 D4 8B B3 90 FD
5E BF 45 AF C3 A7 AF 05 13 96 12 17 32 CA F1 32 8F 79 CB BD
0C 96 FC EE 81 9C DE B2 E0 E5 B1 E8 9A 3B 3B B7 9D 71 67 DD
EF 31 F6 63 95 95 64 90 5E DD 6A 7F A7 F7 5A EE

Module public key exponent = 0x11

Module signature:

B4 5D 65 7A CD FC BA 3C 40 B2 F0 30 C1 81 71 F2 B8 B5 8C 56
D0 FB 53 C7 A6 EB AF 32 52 42 37 59 B4 7D 4E F5 AE 88 2E 90
D3 FA 4A EC CD 5F EE BA 2E FF D8 55 DB 4C 11 E0 C4 0A C9 E1
0C C0 99 8B F4 1A 7F A5 A1 7B 34 56 02 D0 9B 3C F2 16 19 6F
3C 68 7F 0A 98 6F 12 B0 14 9D 9F C4 61 97 01 34 E8 41 50 97
56 B6 EB DF ED B1 38 2A 5E 8E D6 CB 4F 33 F0 59 36 87 59 E6
23 F9 18 7C EF 3C EF 49 3F AA 4B 02 CC E0 37 51 A6 C6 37 13
1A F5 4D E2 B6 41 A9 75 41 C4 DD 46 2D 8C 7F 46 8E A2 F9 AB
19 2C 1A 09 EF 74 D2 9D EC AA CF 97 15 3B CD 17 6E D2 6A 1E
12 E4 73 71 4A F6 CC BB A2 72 5F AE 86 3A 0A 9E 4B 0E 36 6C
07 0C F3 D8 85 B4 2A 98 E3 56 CE 4A 8F D8 38 C3 D4 DD 5D 05
4E 24 18 50 3E E5 13 0D B8 FD C6 6F D3 B2 F8 0C E8 25 F1 70
68 DC BF 0E 1B AA 5D CA 6A 95 44 F1 00 BF 7E 96

Chipset ACM Information Table (0x4C0):

UUID = 0x7FC03AAA 0x18DB46A7 0x8F69AC2E 0x5A7F418D

Chipset ACM Type = 0x0

ACM version = 0x2

ACM Revision Major = 0x1

ACM Revision Minor = 0xD

ACM Revision Build = 0x0

Table Version = 0x7

Table Length = 0x30

Chipset ID list table offset = 0x4F0

Maximum OsSinitTable version = 0x0

Minimum MLE Header version = 0x20000

TPM Information Table

TPM Capabilities = 0xF

PCR Extend Policy:



algorithms and TPM PCR Extend commands

Both Maximum Agility and Maximum Performance Policies are supported.

Measurements done using embedded fixed set of algorithms and TPM PCR Extend commands

TPM Family Support:

dTPM 1.2 Supported

dTPM 2.0 Supported

Initial TPM 2.0 TPM NV index range supported

TPM Algorithm Count = 0x4

Supported Algorithm ID = 0x4

Supported Algorithm ID = 0xB

Supported Algorithm ID = 0xC

Supported Algorithm ID = 0x14

Capabilities = 0xF76

Module supports MONITOR address RLP wakeup-method.

ACM File Memory Pointer: 0x956B9018

Chipset ID list table: 0x4F0

Count = 3

Chipset ID entry 0:

Flags = 0x1

Vendor ID = 0x8086

Device ID = 0xB008

Revision ID = 0x1

Chipset ID entry 1:

Flags = 0x1

Vendor ID = 0x8086

Device ID = 0xB006

Revision ID = 0x1

Chipset ID entry 2:

Flags = 0x1

Vendor ID = 0x8086

Device ID = 0xB00C

Revision ID = 0x1

ACM Public Key Hash:

C1 4A 4B 4B E9 B8 AA 00 1B 65 37 7F E6 89 D2 52

E6 C6 8D CD 66 D3 7B CE 1D A9 76 98 67 D1 0C FD

Publish Key Hash MSRs:

C1 4A 4B 4B E9 B8 AA 00 1B 65 37 7F E6 89 D2 52

E6 C6 8D CD 66 D3 7B CE 1D A9 76 98 67 D1 0C FD

NOTE: ACM header is not 0x19800 (CRAM size) byte aligned

Validating ACM Signature

ACM Signature Valid



13.4.2 TPM 1.2 Requirements

13.4.2.1 TPM Compatibility Matrix

For TPM 1.2 based platform, Intel® TXT requires the TPM 1.2 to be compliant to the **TPM 1.2 Rev 116 Specification** (as per TCG Conformance Suite) and must adhere to the TCG PC Client Specific TPM Interface Specification (TIS) 1.21. Details of the requirements are specified in the Trusted Platform Module - Trusted Execution Technology Requirements document. The readiness of the TPM can be determined using the TPM Compliance Matrix listed in this document. The TPM Compliance Matrix is used by TPM vendors to determine Intel® TXT compliance for their TPMs.

Check with the TPM vendor(s) for their Intel® TXT Compliance Matrix results to determine Intel® TXT readiness.

13.4.2.2 AUX and PS Indices Provisioned

In addition to checking for a compliant TPM, user must also check that the Intel® TXT TPM NV indices are properly created in the TPM NV. For this platform, Intel® TXT requires the AUX and PS indices to defined as specified in the *Intel® TXT TPM NV Requirement* for detail on the correct format. Refer to Appendix B for description of the expected TPM NV provisioning using the BIOS development reference code tools.

13.4.2.3 Checking AUX Index Accessibility

Use the **txtinfo64.efi** tool to verify this Index was created and is accessible.

Return code of zero indicates that the AUX index has been created and is accessible for Intel® TXT to use.

13.4.2.4 Checking PS Index Accessibility

Use the **txtinfo64.efi** to confirm that the PS index has been created and properly provisioned.

13.4.2.5 Checking TPM NV Locking Status

As specified in the *Intel® TXT BIOS Specification* and *TPM NV Storage Interface Usage* documents, Intel® TXT requires that the AUX and the PS indices are locked by the platform supplier after these indices are defined. Locking the TPM NV before Intel® TXT feature is used on the platform will prevent malicious software from corrupting the index area and compromising Intel® TXT integrity.

TXTINFO64.efi can be used to determine the TPM NV locking status. Production SINIT ACM will reset if the TPM NV is not locked on the platform.

13.4.3 TPM 2.0 Requirements

13.4.3.1 TPM Compatibility Matrix

For TPM 2.0 based platform, Intel® TXT requires the TPM 2.0 to be compliant to the **TPM 2.0 Rev 1.01 or latest specification** (as per TCG Conformance Suite). Details of the requirements are specified in the Trusted Platform Module - Trusted Execution



Technology Requirements document. The readiness of the TPM can be determined using the TPM Compliance Matrix listed in this document. The TPM Compliance Matrix is used by TPM vendors to determine Intel® TXT compliance for their TPMs.

Check with the TPM vendor(s) for their Intel® TXT Compliance Matrix results to determine Intel® TXT readiness.

13.4.3.2 AUX and PS Indices Provisioned

In addition to check for a compliant TPM, user must also check that the Intel® TXT TPM NV indices are properly created in the TPM NV. For this platform, Intel® TXT requires the AUX and PS indices to be defined as specified in the *Intel® TXT TPM NV Requirement* for detail on the correct format. Refer to Appendix B for description of the expected TPM NV provisioning using the BIOS development reference code tools.

13.4.3.3 Checking AUX and PS Index Accessibility

Use the **txtinfo64.efi** and the command **txtinfo64.efi -c:t** to confirm that the *INDEX_AUX* and *PS Index* has been created.

```
*****
TXTINFO64 v1.5.10
Built: 10:04:24 Oct  3 2014
Intel Corporation
Copyright (c) 2010-2014
*****
Collecting Chipset information...Done.
Collecting CPU...Done.
Collecting TXT Registers...Done.
Collecting ACM...Done.
Collecting VTd...Done.
Collecting Heap...Done.
Collecting TPM...Done.
Testing CPU...Done.
Testing TXT Reg...Done.
Testing Heap...Done.
Testing VTd...Done.
*****
*                      TPM Information                      *
*****
TPM Offsets from FED40000h:
-----
ACCESS 0h
[0] tpmEstablishment           = 0
[5] activeLocality             = 0
[7] tpmRegValidSts            = 0

VID 0F00h                      = 0x1114
DID 0F02h                      = 0x3203
RID 0F04h                      = 0xFC

AUX Index:
```



```
FF FF FF FF 09 12 14 20 06 B0 00 80 00 01 FF FF
FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF
08 F9 9B C4 EC 4A 26 5B 54 08 7D C0 59 FF E6 E6
A1 52 6B C3 84 19 00 00 FF FF FF FF FF FF FF FF
```

PS Index:

```
00 03 0B 00 01 10 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 02 00 00 00 00 09 00 0C 00
00 00 08 00 00 00 01 02 03 04 05 06 07 08 09 0A
0B 0C 0D 0E 0F 10 11 12 13 14 15 16 17 18 19 1A
1B 1C 1D 1E 1F 20
```

13.5 BIOS-BIOS AC

13.5.1 Check BIOS-BIOS AC Integration

Once the key hardware and software components are confirmed to be Intel® TXT capable, the next step is to verify that the BIOS AC module integration is done correctly. A couple items to check are:

1. SCHECK has registered the ACM in the TPM
2. Basic BIOS AC operation.

Details on BIOS requirements are out of scope for this document. For more information on BIOS AC module integration, refer to Section 2 of the "Intel Trusted Execution Technology BIOS Specification"

13.5.1.1 BIOS AC SCHECK

SCHECK verifies that the called AC module is registered in the TPM NVRAM for consumption by Intel® TXT software later in the boot sequence.

A method to check SCHECK completion is to confirm that the ACM is registered in the TPM. To do this use the *aux2_read.bat (TPM1.2)* or *TXTINFO64 (TPM2.0)* and observe the first 20 bytes to determine if the ACM has been registered. Use the same execution method described above in [Section 13.4.2.3](#).

13.5.1.2 BIOS Memory Map

Confirm that the BIOS is properly setting up the memory map according to the *Intel® TXT BIOS Specification*. Some key mappings to be evaluated are SINIT space, Intel® TXT public space, Intel® TXT private space and heap memory region. These regions can be evaluated using **txtinfo64.efi**. Observe the Intel® TXT Memory Map settings for egregious overlaps. Refer to txtinfo.efi sample output in section The method described in this document uses the following development tools provided by Intel Corporation.



13.6 Measured Launch

With the BIOS dependency met, the next validation consideration is to launch an Intel® TXT MLE (measured launch environment). By launching a MLE, user can validate that the Intel® TXT platform components: processor, chipset, TPM and AC modules are working together as expected.

Measured Launch is a key Intel® TXT feature. Thorough evaluation of the process is recommended. This section describes a two-tier approach to checkout measured launching.

The first level checkout is a fundamental check to make sure the infrastructure components (processor, chipset, TPM and ACM) can collaborate to deliver the measure launch feature. This first level checkout allows better isolation of measured launch related issues. The second level checkout is to verify that the platform is capable of supporting the targeted MLE. Intel Client Platform POR does not support launching SINIT ACM from flash. This is only POR on Server and Workstation platforms.

13.6.1 Fundamental Measured Launching with getsec64.efi

To facilitate fundamental Intel® TXT checkout, Intel Corporation makes available the **getsec64.efi** tool. To launch an MLE using **getsec.efi** perform the following steps:

1. Boot into the EFI-shell
2. Execute the following command:

```
Shell> getsec64.efi -L SENTER -a <SINIT AC-filename>
```

If the command above is failing on CNL/CFL platform, then use the following command line.

```
Shell> getsec64.efi -L SENTER -a <SINIT AC-filename> -i
```

<SINIT AC-filename> is the SINIT AC module to be released with the platform.

```
-s hashId: TPM2 hash algorithm <#> is (1 - SHA1, 2 - SHA256, 3 - Both)
-e PCR Extend Policy Control: <*> is (0 - Algorithm Agile Command set, 1
- Embedded hashing SW)
```

Measured launch failure can be diagnose using the TXT.ERRORCODE register. This register can read from the EFI shell using **txtinfo64.efi**.

Error code description is distributed with the ACM package.

Measured launch Success can be seen after the Getsec64 command is launched as seen below:

```
*****
GETSEC64 v1.2.x
Built: Sep 16 2013 11:17:11
Intel Corporation
Copyright (c) 2010-2013
```



```
*****  
GETSEC[SENTER] complete. System is now in TXT Environment.
```

13.6.2 Targeted Measured Launching

Once the fundamental checkout is completed, the next step is to validate that the BIOS has met all the requirements for targeted MLE. This verification is accomplished by configuring and installing the MLE.

At the time of this document, the publicly available MLE is Trusted Boot (tboot) is available at <http://www.bughost.org/repos/hg/tboot.hg>

MLE specific Intel® TXT checkout is dependent on architecture and capability of the targeted MLE. For the reference, Appendix B describes how Intel® TXT enabled Tboot can be used in the validation flow.

13.7 Verified Launch

Intel® TXT Verified Launch can be evaluated by installing a launch control policy (LCP) to restrict the platform to only launch the MLE that is allowed by policy. For more information on Intel® TXT LCP, refer to the “Intel® Trusted Execution Technology: MLE Developer’s Guide”.

Launch control policies are typically provided the by ISV for the corresponding MLE. If your ISV does not provide an LCP for the targeted MLE, LCP can be defined using the Intel® Trusted Execution Technology LCP Tools Reference Kit. Linux* based reference code is available from Intel. Check with the Intel engineering representative for appropriate policy for test environment.

Once the policy is defined, confirm that launch environment successfully launched or not launched per the defined policy.

Platform Supplier (PS) default policy definition (PS_ANY) is recommended to support a “boot-any” scenario.

This recommendation supports the platform owners to define the launch control policy per their business needs. This configuration is most representative of the Intel® TXT TTM configuration.

13.8 Measured Launch Environment

Once the measured environment is established and Intel® TXT has been confirmed as the launch mechanism, the last step is to validate that the MLE works as expected.

If the targeted virtual environment and applications, utilize the Intel® TXT security foundation, then those particular tools and features should be executed and validated for proper operation. Making the platform Intel® TXT ready for those ISVs is important.

In this context, the Intel® TXT measured launch environment can be validated with custom applications that make use of the trusted measurements in PCR17/18.

Here’s a sample of PCR17/18 readout from TXTINFO64 tool:

```
PCR 17: 25 1E 8F B4 84 D1 7B 96 63 C2 69 E4 CE 5C CE D3
```



D3 26 27 8A

PCR 18: FA 2D 64 7C 61 A8 29 1C 76 01 03 97 D1 82 D7 1A
62 34 2F 35

System is in TXT Environment.

Without software that utilizes the Intel® TXT launched environment, validation should evaluate proper operation for a representative set of Intel® TXT-agnostic software.

Basically, validate that the software workload works the same in the Intel® TXT measured environment as it does in the non-measured environment.

This chapter highlights some focus areas that the validation software should stress.

13.8.1 Basic Stability

Define a workload that stresses the system broadly but not deeply. Select or develop applications that stress the SMP architecture, ALU operations, system memory management, file manipulation and networking. This test suite should validate the system for general robustness.

13.8.2 Functional Comprehensive

Define a workload that utilizes the Intel® TXT trusted environment, once it has been established. Currently, there is no generally available application or software that utilizes this security foundation. However an application can be developed to simulate an application utilizing the stored measurements to extend the trust boundary of the system.

13.8.3 Platform Stability

Define a workload that stresses the system as it would be used in the targeted platform. Software categories to include are: networking, virus scan, games, photo/video editing, content management, personal finance, business applications and web browsers.

13.8.4 BIOS/ACM Update Consideration

Once Intel® TXT has been used to launch an MLE, the TPM Establishment will be set to associate the system with the AC modules that were used to launch the environment.

TPM Establishment needs to be reset as per the *Intel® TXT BIOS Specification*. Improper update will cause the ACM to be out of sync with the established environment.

This feature should be included in the validation plan. Suggested sequence to confirm that TPM Establishment is being reset by the BIOS update process:

1. Launch and exit a measured environment using one of the methods described above in [Section 13.7](#) or [Section 13.8](#).
2. Update the BIOS using the customer's method.
3. Run TXTINFO64 to confirm that TPM Establishment is cleared.



13.9 Secret Memory Protection Using SCLEAN

The last validation consideration is assuring the secret memory clean capability taking down of an Intel® TXT trusted environment is properly configured and ready for use by the application software.

Intel® TXT provides the ability to clean the memory in case of a planned or unexpected power loss using SCLEAN function. In proper operation, the measured launch environment take down is not perceptibly different from non-measured environment. For validation purpose, confirm that an MLE take down does not behave differently from a non-measured environment take down.

The special Intel® TXT validation consideration occurs when an MLE is brought down improperly (Example: Sudden power loss) and the TXT.CMD.SECRETS flag has been set to 1 by the MLE. In this scenario, at the next power up, Intel® TXT will detect a potential security risk and scrub system memory using SCLEAN before resuming operation.

This Secret Memory Protection validation should be done on all memory configurations targeted for the platform. The following two scenarios can be used to confirm that BIOS and the BIOS AC (SCLEAN) are collaborating to deliver this protection.

13.9.1 Set Secret Scenario

Set the secret bit in the trusted environment and remove power to system. To simulate this memory protection scenario perform the following steps:

1. Launch an MLE using one of the methods described in [Section 13.7](#) or [Section 13.8](#).

Note:

Tboot automatically sets the secret flag upon successful launch, so step 2 is not necessary, if *tboot* was used to establish the measured launch environment.

2. Set the secret condition using one of the following methods:

- a. With ITP/XDP with the following command:

```
Using ITP 1 'p[0]>ord4 0xfed208e0p=1' (data value not important)
Using ITP 2 '>>>itp.threads[0].mem("0xfed208e0p",4,1)' (data value not important)
```

- b. With **secrets64.efi** using:

```
EFI> secrets64.efi -s
```

3. Power-down the system.
4. Power-up the system.

13.9.2 Secret Status Unknown Scenario

Another way to trigger memory protection is by pulling down the RTESTB. This flags to Intel® TXT, the system was brought down improperly and may be at risk. To simulate this condition, do the following steps:

1. Launch an MLE using one of the methods described in [Section 13.7](#) or [Section 13.8](#).
2. Power down the system.



3. Short or Pull the RTC battery for a minute or more, to dissipate any residual charge.
4. Power up the system.

13.9.3 System Behavior with SLCEAN

Depending upon the result of SLCEAN function and state of Boot Guard technology, execution of SCLEAN may result in warm reset or a cold reset. Refer below for more details:

1. If Boot Guard technology is Disabled and SCLEAN function scrubs the system memory successfully, control is passed from BIOS ACM to BIOS, which is responsible for power down (global) reset.
2. If Boot Guard technology is Enabled (Active) and SCLEAN function scrubs the system memory successfully, control is retained by BIOS ACM and BIOS ACM performs the system reset. Control is not passed to BIOS to allow for Boot Guard protection.
3. If SCLEAN function does not scrub the system memory successfully, control is retained by BIOS ACM and BIOS ACM performs a warm reset. Warm reset ensures that TXT.Errorcode corresponding to SCLEAN failure is preserved for the next boot.

13.9.3.1 How to Verify SCLEAN Manually

1. Enter TXT Environment.
2. Run the command 'secrets64.efi -s' to set secrets bit.
3. Run the command 'secrets64.efi -m' to set seed value.
4. Run the command 'secrets64.efi -v' and will see seeded value.

```
SECRETS64 1.0.9, Copyright (c) 2010-2016 Intel Corporation
DEBUG - After First Call -- GetMemoryMap() -- Size = 0x29A0
DEBUG - After Second Call -- GetMemoryMap() -- Size = 0x27F0
Seed Value: 0xDEADBEEF
Scanning address range: 0x0 - 0x57FFF
Scanning address range: 0x59000 - 0x9DFFF
First Seed value 0xDEADBEEF found at address 0x59000
Number of Seed Values 0xDEADBEEF found: 70656
Scanning address range: 0x100000 - 0x87A80FFF
First Seed value 0xDEADBEEF found at address 0x100000
Number of Seed Values 0xDEADBEEF found: 568722432
Scanning address range: 0x87AB8000 - 0x88BDDFFF
First Seed value 0xDEADBEEF found at address 0x87AB8000
Number of Seed Values 0xDEADBEEF found: 4495360
Scanning address range: 0x88CBC000 - 0x88D9AFFF
First Seed value 0xDEADBEEF found at address 0x88CBC000
Number of Seed Values 0xDEADBEEF found: 228352
Scanning address range: 0x88F2B000 - 0x88F6EFFF
First Seed value 0xDEADBEEF found at address 0x88F2B000
Number of Seed Values 0xDEADBEEF found: 59394
Scanning address range: 0x88F84000 - 0x88F84FFF
Scanning address range: 0x100000000 - 0x16DFFFFFFF
First Seed value 0xDEADBEEF found at address 0x100000000
Number of Seed Values 0xDEADBEEF found: 461373440
-----
```



Total Number of Seed Values 0xDEADBEEF found: 1034949634

5. Enter EFI shell after SLCEAN and run 'secrets64.efi -v', then user will see that seed value is not found. This verifies that clean occurred. Please be aware that if checking for Seed value with -v multiple times there may be a single seed value found from the tool running and writing value to memory.

```
SECRETS64 1.0.9, Copyright (c) 2010-2016 Intel Corporation
Seed Value: 0xDEADBEEF
Scanning address range: 0x0 - 0x57FFF
Scanning address range: 0x59000 - 0x9DFFF
Scanning address range: 0x100000 - 0x87A80FFF
Scanning address range: 0x87AB8000 - 0x88BDDFFF
Scanning address range: 0x88CBC000 - 0x88D9AFFF
Scanning address range: 0x88F2B000 - 0x88F85FFF
Scanning address range: 0x88F8A000 - 0x88F8AFFF
Scanning address range: 0x100000000 - 0x16DFFFFFFF
```

Seed value 0xDEADBEEF was not found!

13.10 Trusted Platform Module (TPM) Establishment Management

Trusted Platform Module (TPM) Establishment, when set to "0" indicates that either currently or at some point in the past, an MLE has been established; therefore, either currently or at some point in the past, the contents of memory may have contained secrets that were protected by the MLE. Because of its key role in triggering Intel® TXT secret memory protection, proper management of this indicator is required to ensure the Intel® TXT enabled platform delivers the appropriate protection.

An Intel® TXT validation plan should include checks to make sure TPM Establishment is only set, when appropriate.

13.10.1 Checking TPM Establishment

The TPM Establishment can be checked by reading 0xFED40000[0].

Bit 0 sets to "0" means TPM Establishment is set. Bit 0 set "1" means TPM Establishment is not set. Bit 31 is the valid bit.

The TXTINFO64 tool will show user in TPM section the TPM Establishment status.



13.10.2 Recommended TPM Establishment Behavior

Scenario	TPM Establishment Status
Shipped system default	Not set
Intel® TXT is enabled in the BIOS before measured launch is ever invoked	Not set
Intel® TXT is enabled in the BIOS and measured launch completed	Set
Intel® TXT is disabled in the BIOS	Not set
BIOS updates	Not set
BIOS ACM updates	Not set
System memory configuration changes	Not set

13.10.3 Resetting Trusted Platform Module (TPM) Establishment

Once the checkout process is completed, it is recommended that the TPM Establishment be reset. If the BIOS being evaluated does not provide a mechanism to reset the TPM Establishment explicitly or when Intel® TXT is disabled, user can manually reset the TPM Establishment using the **getsec64.efi** tool.

Use the following command:

```
Shell> getsec64.efi -L ENTERACCS -a <BIOS AC-filename> -fn Est
```

13.11 Summary

Complete validation of an Intel® TXT enabled client platform can be done by focusing on the key security feature, *Intel® TXT Verified Launch*. Verified launch effectively exercises all the key Intel® TXT hardware/software components and validates that the components work correctly and are configured properly to deliver this platform feature.

This validation guide describes a strategy to validate verified launch from a bottom-up approach. This bottom-up strategy starts with validating the hardware and software components for compliance and proper operations. Then the validation consideration is brought up to the next Intel® TXT intercept, the BIOS-BIOS AC integration. Then, key SINIT-AC integration checks are considered. Then, user looked at the expected behavior of the measured launch environment. Lastly, controlled take-down of the measured launch environment was considered, with particular focus on the secret memory protection.

13.12 Intel® Trusted Execution Technology (Intel® TXT) Test Plan

This section describes sample Intel® TXT checkout plans and the tools that can be used to evaluate the platform for Intel® TXT measured launch and secret protection.



For the development environment, where a quick evaluation of implementation is desired, the test plan described in [Section 13.12.2, "Intel® TXT Baseline Coverage Summary,"](#) does a minimal check of the key Intel® TXT features. To further reduce testing time, the test iteration specified in test cases can be minimize to fit allotted time.

Note: Passing the test cases in the Intel® TXT Baseline Coverage Summary only establishes key TXT functionality/features and is not considered adequate for complete Intel® TXT checkout.

The test plan in [Section 13.12.3, "Intel® TXT Test Plan,"](#) is targeted for complete validation and compliance determination. It includes a number of test cases that evaluates platform robustness. Intel recommends that platform suppliers refer to this test plan for more thorough validation of the Intel® TXT implementation on the platforms.



13.12.1 Intel® TXT Testing Pre-requisite

Pre-requisite Checklist	Location
Intel Provided Tools	
getsec64.efi, txtinfo64.efi, secrets64.efi, pcrdump64, TxtBtgInfo.efi – “Intel® Trusted Execution Technology: Intel® TXT Client Debug Toolkit”	Distributed with ACM package
aux2_read.bat, aux2_cap.bat, ps_read, ps_cap.bat	Distributed with ACM package
TPM Provisioning tool for use with Intel® Trusted Execution Technology (TPM 1.2) - DOS based TPM Provisioning development only tool	Distributed with ACM package (in zip folder called “BIN”)
TPM Provisioning tool for use with Intel® Trusted Execution Technology (TPM 2.0) - EFI based TPM Provisioning development only tool	Distributed with ACM package (in zip folder called “TPM2ProvTool”)
TPM Provisioning tool for use with Intel® Trusted Execution Technology (TPM 2.0) with System Guard - EFI based TPM Provisioning development only tool	Distributed with ACM package (in zip folder called “System Guard PS2”)
BIOS EFI Shell or DUET	http://sourceforge.net/apps/mediawiki/tianocore/index.php?title=EDK
Tboot – Trusted boot module	http://www.bughost.org/repos.hg/tboot.hg/
Intel® TXT Trusted Boot (tboot) Usage LiveImage	Posted on VIP
BIOS Requirement	
Intel® VT, Intel® VT-d enabled	
BIOS AC integration complete	Posted to VIP
Support for TPM Establishment reset in BIOS or BIOS update	
System restore flash image to use with SCLEAN check	
TPM1.2 or TPM2.0 support	
System Requirement	
Representative sample of production memory configuration	
TPM NV indices created and locked (For TPM 1.2 Production Configuration)	
If platform is targeted to support multiple TPM	
• TPM swapping capability	
• Sample of targeted TPM	
ITP or Intel® Debug Tool hooks (desired)	
ACM	
SINIT ACM - compatible to targeted chipset	Posted on VIP

13.12.2 Intel® TXT Baseline Coverage Summary

This section describes a short test plan that can be used to verify basic Intel® TXT functionality. This test plan is a minimal set of test cases that exercise the platform’s capability to support measured launch and secret protection.



Note: Passing the test cases in the Intel® TXT Baseline Coverage Summary only establishes key TXT functionality/features and is not considered adequate for complete Intel® TXT checkout.

For a comprehensive Intel® TXT validation plan that is targeted for the validation environment, refer to [Section 13.12.3](#).

Test ID Number	Test Case Title	PETS/Manual
TXT_TC0001A	Check for Intel® TXT Components	Manual
TXT_TC0002A	Check AUX Index	Manual
TXT_TC0002B	Check PS Index	Manual
TXT_TC0002C	Verify indices are locked in TPM NV	Manual
TXT_TC0004A	SINIT, when Intel® TXT is enabled	Manual
TXT_TC0004D	Power loss after SINIT without secret	Manual
TXT_TC0004E	Power loss after SINIT with secret	Manual
TXT_TC0004G	Power loss after SINIT and RTC battery pulled	Manual
TXT_TC0004I	TPM Establishment set when the secret is undetermined	Manual
TXT_TC0004N	PCR17/18 Integrity	Manual
TXT_TC0005A	SCLEAN with targeted memory configurations	Manual
TXT_TC0006C	Tboot with Intel® TXT	Manual
TXT_TC0006D	S3 Tboot with Intel® TXT	Manual
TXT_TC0007A	Factory Default TPM Establishment Setting	Manual
TXT_TC0007B	TPM Establishment when Intel® TXT is disabled	Manual

13.12.3 Intel® TXT Test Plan

This section describes a comprehensive test plan for the validation environment and compliance determination. Extending on the Baseline test plan, listed above in [Section 13.12.2](#), “Intel® TXT Baseline Coverage Summary,” this test plan includes additional test cases to evaluate the platform’s robustness. Robustness in this context refers to:

1. How well the platform functions with various configurations, such as different memory sizes;
2. How well it handles repeated invocation. This test plan can be used as a framework and can be customized to define a Intel® TXT test plan appropriate for the validation environment and coverage objective.

Test ID Number	Test Case Title	PETS/Manual
TXT_TC0001A	Check for Intel® TXT Components	Manual
TXT_TC0002A	Check AUX Index	Manual
TXT_TC0002B	Check PS Index	Manual
TXT_TC0002C	Verify that indices are locked in the TPM NV	Manual
TXT_TC0003A	SMX Disabled	Manual
TXT_TC0003B	SINIT when Intel® TXT is disabled	Manual



Test ID Number	Test Case Title	PETS/Manual
TXT_TC0003C	SMX when Intel® TXT is enabled	Manual
TXT_TC0004A	SINIT when Intel® TXT is enabled	Manual
TXT_TC0004B	Cold boot after SINIT	Manual
TXT_TC0004C	Warm boot after SINIT	Manual
TXT_TC0004D	Power loss after SINIT without secret	Manual
TXT_TC0004E	Power loss after SINIT with secret	Manual
TXT_TC0004G	Power loss after SINIT and RTC battery pulled	Manual
TXT_TC0004H	Power loss after SINIT with secret	Manual
TXT_TC0004I	TPM Establishment set when the secret is undetermined	Manual
TXT_TC0004J	TPM Establishment not set	Manual
TXT_TC0004K	SINIT cycle testing	Manual
TXT_TC0004L	SINIT cycle testing with cold boot	Manual
TXT_TC0004M	SINIT cycle testing with warm boot	Manual
TXT_TC0004N	PCR17/18 Integrity	Manual
TXT_TC0005A	SCLEAN with targeted memory configurations	Manual
TXT_TC0006A	Windows* with Intel® TXT	Manual
TXT_TC0006B	Windows* S3 with Intel® TXT	Manual
TXT_TC0006C	Tboot with Intel® TXT	Manual
TXT_TC0006D	S3 Tboot with Intel® TXT	Manual
TXT_TC0007A	Factory Default TPM Establishment Setting	Manual
TXT_TC0007B	TPM Establishment when Intel® TXT is disabled	Manual
TXT_TC0007C	TPM Establishment after BIOS Update	Manual
TXT_TC0008A	Intel® TXT and Intel® AMT Interoperability	Manual
TXT_TC0008B	Tboot with Intel® VT-d enabled Linux* or Xen*	Manual
TXT_TC0008C	Intel® TXT when CSME is disabled	Manual
TXT_TC0008D	Intel® TXT when CSME is enabled	Manual
TXT_TC0009A	Installing SINIT ACM Driver for Windows	Manual

Test ID	TXT_TC0001A
Test Case Title	Check for Intel® TXT Components
Mandatory/Optional	Mandatory
Description	Verify that platform has Intel® TXT enabled processor, chipset and TPM required for Intel® TXT execution



Test ID	TXT_TC0001A
Objective	This test to determine that the HW and SW components are required on the targeted test platform
Procedure	Legacy ACM use TXTINFO64.efi, for Converged ACM(CBnT) use TxtBtgInfo.efi For TPM1.2/2.0: EFI: Run "TXTINFO64.efi -c:a -p" at the prompt
Test Pass/Fail Criteria	Test passes, if all the components required for TXT are present as reported by the tools NOTE: TPM Index Value Info for reference 1. AUX Index Value 0x1C10102 2. PS Index Value 0x1C10103 3. PO Index Value 0x1C10106 4. SGX Index Value 0x1C10104 5. PPI Index Value 0x1C10105

Test ID	TXT_TC0002A
Test Case Title	Check AUX Index
Mandatory/Optional	Mandatory
Description	Checks existence of the Intel® TXT Aux index
Objective	This test to determine that the TPM NV has been properly provisioned for Intel® TXT with the AUX index defined as specified
Procedure	Legacy ACM use TXTINFO64.efi, for Converged ACM(CBnT) use TxtBtgInfo.efi For TPM1.2: DOS: Run "aux2_read.bat" or "aux2_cap.bat" EFI: Run "TXTINFO64 -c:a -p" at the prompt For TPM2.0: EFI: Run "TXTINFO64 -c:a -p" at the prompt
Test Pass/Fail Criteria	The test pass, if the aux2_read.bat, TXTINFO64 shows that the AUX index is defined and accessible.

Test ID	TXT_TC0002B
Test Case Title	Check PS Index (Legacy ACM only, Not applicable for CBnT)
Mandatory/Optional	Mandatory for Legacy ACM
Description	Check the existence of the PS index as required by the platform
Objective	This test to determine that the PS has been properly provisioned for Intel® TXT execution on the targeted platform
Procedure	Legacy ACM use TXTINFO64.efi, for Converged ACM(CBnT) use TxtBtgInfo.efi For TPM1.2: DOS: Run "ps_read.bat" EFI: Run "TXTINFO64 -c:t -p" at the prompt For TPM2.0: EFI: Run "TXTINFO64 -c:t -p" at the prompt



Test ID	TXT_TC0002B
Test Pass/Fail Criteria	The test pass, if the ps_read.bat, TXTINFO64 shows that the PS is defined as specified by the Intel® TXT BIOS Spec NOTE: Use latest TPM Provisioning scripts that are included in the ACM kit that user is using. If older TPM scripts are used, then user may get system reset upon enabling TXT.

Test ID	TXT_TC0002C
Test Case Title	Verify that the indices are locked in the TPM NV
Mandatory/Optional	Mandatory only for production systems
Description	Verify that the AUX index is locked in the TPM NV
Objective	This test verifies that AUX index is locked in the TPM NV as required by the SINIT ACM
Procedure	Legacy ACM use TXTINFO64.efi, for Converged ACM(CBnT) use TxtBtgInfo.efi For TPM1.2/TPM2.0: EFI: 1. Boot to EFI-Shell 2. Run "TXTINFO64 -c:t -p" at the prompt
Test Pass/Fail Criteria	Test passes, if TXTINFO64 indicates the TPM NV indices are properly locked in the TPM NV

Test ID	TXT_TC0003A
Test Case Title	SMX Disabled
Mandatory/Optional	Mandatory
Description	With Intel® TXT and supporting options disabled in BIOS, verify SMX is properly disabled
Objective	Verify the BIOS is properly managing the SMX feature control in the processor
Procedure	Legacy ACM use TXTINFO64.efi, for Converged ACM(CBnT) use TxtBtgInfo.efi 1. Disable TXT in the BIOS. 2. Confirm using TXTINFO 64 that the platform is not ready for TXT. EFI: Run "TXTINFO64 -c:a -p" at the prompt
Test Pass/Fail Criteria	Test passes, if the <i>SENTER enable</i> and <i>control</i> bits are deasserted in the IA32_FEATURE_CONTROL MSR

Test ID	TXT_TC0003B
Test Case Title	SINIT, when Intel® TXT is disabled
Mandatory/Optional	Optional
Description	Verify SINIT does not run, when Intel® TXT is disabled in BIOS with GetSec



Test ID	TXT_TC0003B
Objective	Ensure the BIOS is properly configuring the platform to disallow Intel® TXT measured launch when Intel® TXT is disabled in the BIOS
Procedure	<ol style="list-style-type: none"> 1. Disable TXT in the BIOS. 2. Boot to EFI-Shell. 3. Run "GETSEC64 -L SENTER -a SINIT.BIN" at the prompt. 4. Run "GETSEC64 -L SEXIT" at the prompt. <p>NOTE: If this test case fails or hangs at step 3, run the test again with "GETSEC64 -L SENTER -a SINIT.BIN -i".</p> <p>NOTE: To run Getsec SENTER with DMAR enabled please use "-d" Command at the end of getsec command i.e., "GETSEC64 -L SENTER -a SINIT.BIN -d".</p>
Test Pass/Fail Criteria	Test passes, if user is not able to complete the SENTER. The following error messages will appear error message saying: "Error: SINIT base register is not programmed" leaf = 0x20 "Error: System is NOT in TXT environment."

Test ID	TXT_TC0003C
Test Case Title	SMX, when Intel® TXT is enabled
Mandatory/Optional	Mandatory
Description	With Intel® TXT option enabled in BIOS, verify SMX is properly enabled
Objective	Determine that the BIOS is properly configuring the processor for SMX execution, when Intel® TXT is enabled in the BIOS
Procedure	<ol style="list-style-type: none"> 1. Enable Intel® TXT in the BIOS. 2. Verify with either TXTINFO64. <p>EFI:</p> <ol style="list-style-type: none"> 1. Boot to EFI-Shell. 2. Run "TXTINFO64 -c:a -p" at the prompt.
Test Pass/Fail Criteria	Test passes, if the <i>SENDER enable</i> and <i>control</i> bits are asserted in the IA32_FEATURE_CONTROL MSR

Test ID	TXT_TC0004A
Test Case Title	SINIT, when Intel® TXT is enabled
Mandatory/Optional	Mandatory
Description	Verify successful SINIT with GETSEC64
Objective	Verify that the BIOS has properly configured the platform to support a basic measured launch with SINIT
Procedure	<ol style="list-style-type: none"> 1. Enable Intel® TXT in the BIOS. 2. Boot to EFI-Shell. 3. Run "GETSEC64 -L SENTER -a SINIT.BIN". 4. Run "GETSEC64 -L SEXIT". 5. Repeat steps 2-3, three times.
Test Pass/Fail Criteria	Test passes, if the platform successfully enters and exits the Intel® TXT trusted environment



Test ID	TXT_TC0004A
Note 1	<p>If you have run System Guard on this platform the PO TPM Index will be created. If you want to run this test in EFI shell you will have to delete the PO Index first then run this test. We recommend that these compliance tests are run before testing System Guard.</p> <p>This can be done with the supplied TPM Provisioning scripts.</p> <p>Command for this is Tpm2PoProv.nsh SHA256 EXAMPLE -D</p>
Note 2	<p>Please make sure that DMA Remapping (DMAR) is disabled before running GETSEC SENTER. DMA Remapping is required to be disabled for testing in EFI shell. If it is not disabled then upon GETSEC SENTER a reset will occur. More details can be found in the Measured Launch Developer's Guide referenced in the Introduction chapter. Once EFI Shell testing is complete it can be enabled. OS Bootloader will automatically disable this when launching TXT with GETSEC SENTER then enable it again once GETSEC SENTER has completed, which is why this issue is not seen in OS environment.</p> <p>This Note is relevant for any GETSEC SENTER Command that is issued in EFI Shell with DMAR Enabled.</p>

Test ID	TXT_TC0004B
Test Case Title	Cold boot after SINIT
Mandatory/Optional	Mandatory
Description	Verify system shutdown and cold boot after SENTER, GetSec Wakeup, SMCONTROL then SEXIT (three times)
Objective	Ensure that platform can be shutdown and booted after post Intel® TXT measured launch
Procedure	<ol style="list-style-type: none"> 1. Enable Intel® TXT in the BIOS. 2. Boot to EFI-Shell. 3. Run "GETSEC64 -L SENTER -a SINIT.BIN". 4. Run "GETSEC64 -L SEXIT". 5. Do a cold boot. 6. Repeat all steps three times.
Test Pass/Fail Criteria	Test passes, if the platform can shutdown and boot after the trusted environment had been established

Test ID	TXT_TC0004C
Test Case Title	Warm boot after SINIT
Mandatory/Optional	Mandatory
Description	Verify system reboot after SENTER, GetSec Wakeup, SMCONTROL then SEXIT (three times)
Objective	Ensure that platform can be shutdown and boot post Intel® TXT measured launch
Procedure	<ol style="list-style-type: none"> 1. Enable Intel® TXT in the BIOS. 2. Boot to EFI-Shell. 3. Run "GETSEC64 -L SENTER -a SINIT.BIN". 4. Run "GETSEC64 -L SEXIT". 5. Do a warm boot, for example, "reset -w". 6. Repeat all steps three times.



Test ID	TXT_TC0004C
Test Pass/Fail Criteria	Test passes, if the platform can shutdown and booted after the trusted environment had been established

Test ID	TXT_TC0004D
Test Case Title	Power loss after SINIT without secret
Mandatory/Optional	Mandatory
Description	Verify power loss without secrets after SENTER, GetSec Wakeup, SMCONTROL and verify that the system will reboot (three times)
Objective	Validate that the platform can support repetitive Intel® TXT measured launching
Procedure	<ol style="list-style-type: none">1. Enable Intel® TXT in the BIOS.2. Boot to EFI-Shell.3. Run "GETSEC64 -L SENTER -a SINIT.BIN".4. Run "GETSEC64 -L SEXIT".5. Turn off Power Supply or remove power from system.6. Repeat steps 2 – 5.
Test Pass/Fail Criteria	Test passes, if the platforms boot as normal and completes multiple measured launches

Test ID	TXT_TC0004E
Test Case Title	Power loss after SINIT with secret
Mandatory/Optional	Mandatory
Description	Verify power loss with secrets and verify it will cause SCLEAN (then reboot) and then boot (three times). NOTES: <ol style="list-style-type: none">1. In order to observe SCLEAN, watch power LED or post code read out to make sure after SCLEAN happens: system shuts down and restarts to scrub memory, shuts down again followed by a restart, returning to normal state.2. Time taken to run SCLEAN (scrub system memory) is dependent upon how much memory is populated. If the memory in the system is 16 GB or 32 GB, it will take more time than, if the system only has 1 GB or 2 GB.
Objective	Validate that the platform can support repetitive secret protection
Procedure	<ol style="list-style-type: none">1. Enable Intel® TXT in the BIOS2. Boot to EFI-Shell3. Run "GETSEC64 -L SENTER -a SINIT.BIN"4. Run "SECRETS64 -S" at the prompt.5. Turn Off Power Supply6. Watch SCLEAN occur7. Repeat steps 2–6, three times
Test Pass/Fail Criteria	The test passes, if SCLEAN is invoked on each improper shutdown with secret set. NOTE: Refer Section X.9.3.1 for SCLEAN Manual Check steps



Test ID	TXT_TC0004G
Test Case Title	Power loss after SINIT and RTC battery pulled
Mandatory/Optional	Mandatory
Description	Verify total power loss without secrets (coin cell battery failure) after SENTER, GetSec, SMCONTROL and verify it will cause SCLEAN and then boot (three times)
Objective	Validate that the platform will provide secret protection, when the secret status is undetermined
Procedure	<ol style="list-style-type: none"> 1. Enable Intel® TXT in the BIOS 2. Boot to EFI-Shell 3. Run "GETSEC64 -L SENTER -a SINIT.BIN" 4. Turn off power supply 5. Clear the CMOS by means of jumper or remove backup battery (coin) for 5 seconds 6. Put backup battery (coin) back if it was removed 7. Turn on power supply and press the power button 8. Watch SCLEAN occur 9. Repeat steps 1 - 8 two more times (totaling three times)
Test Pass/Fail Criteria	<p>The test passes, if the platform invokes an SCLEAN and boot as expected on each iteration.</p> <p>NOTE: Refer Section X.9.3.1 for SCLEAN Manual Check steps</p>

Test ID	TXT_TC0004H
Test Case Title	Power loss after SINIT with secret
Mandatory/Optional	Mandatory
Description	Verify total power loss with secrets (coin cell battery failure) after SENTER, GetSec Wakeup, SMCONTROL and verify it will cause SCLEAN and then boot (three times)
Objective	Validate that the platform will provide secret protection in spite of the powerloss
Procedure	<ol style="list-style-type: none"> 1. Enable Intel® TXT in the BIOS. 2. Boot to EFI-Shell 3. Run "GETSEC64 -L SENTER -a SINIT.BIN" 4. Run "SECRETS64 -S" at the prompt. 5. Turn off power supply 6. Clear the CMOS by means of jumper or remove backup battery (coin) for 5 seconds 7. Put backup battery (coin) back if it was removed 8. Turn on power supply and press the power button 9. Watch SCLEAN occur 10. Repeat steps 1-9, two more times (totaling three times)
Test Pass/Fail Criteria	<p>The test passes, if the platform invokes an SCLEAN and boot as expected on each iteration.</p> <p>NOTE: Refer Section X.9.3.1 for SCLEAN Manual Check steps</p>

Test ID	TXT_TC0004I
Test Case Title	TPM Establishment set, when the secret is undetermined
Mandatory/Optional	Mandatory



Test ID	TXT_TC0004I
Description	Verify total power loss with establishment bit asserted (0) in TPM (coin cell battery failure), verify it will cause SCLEAN and then boot (three times)
Objective	Confirm that the platform will provide secret protection, when the secret status on the platform is undetermined
Procedure	Establish TPM Establishment in the to enable TXT protection by: 1. Enable Intel® TXT in the BIOS 2. Boot to EFI-Shell 3. Run "GETSEC64 -L SENTER -a [SINIT.BIN]" at the prompt 4. Run "GETSEC64 -L SEXIT" at the prompt 5. Put the secret flag in an undetermined status by: 6. Turn off power supply 7. Clear CMOS by means of jumper or remove backup battery (coin) for 5 seconds 8. Put backup battery (coin) back, if removed 9. Turn on power supply and press the power button 10. Watch SCLEAN occur 11. Repeat steps 1-8, two more times (total three times)
Test Pass/Fail Criteria	Test passes, if the platform successfully boots in each iteration On successful SCLEAN, system will reset, and boot again normally. NOTE: Refer Section X.9.3.1 for SCLEAN Manual Check steps

Test ID	TXT_TC0004J
Test Case Title	TPM Establishment not set
Mandatory/Optional	Mandatory
Description	Verify total power loss with establishment bit not asserted (1) in TPM (coin cell battery failure) verify it does not cause SCLEAN and then boot
Objective	Validate that the Intel® TXT protection does not unnecessarily get invoked on platform that has opted out
Procedure	1. Disable Intel® TXT in the BIOS 2. Boot to EFI-Shell 3. Run "GETSEC64 -L-L ENTERACCS -a [BIOSAC.BIN] -fn EST" at the prompt 4. Turn off power supply 5. Clear the CMOS by means of jumper or remove backup battery (coin) for 5 seconds 6. Put backup battery (coin) back if it was removed 7. Turn on power supply and press the power button 8. Verify SCLEAN does NOT occur
Test Pass/Fail Criteria	The platform boot as expected without invoking SCLEAN

Test ID	TXT_TC0004K
Test Case Title	SINIT cycle testing
Mandatory/Optional	Mandatory
Description	Verify the platform and Intel® TXT is functional and stable by running SENTER, GetSec Wakeup, SMCONTROL then SEXIT repeatedly 1000 times
Objective	Stress test measured launching on the platform



Test ID	TXT_TC0004K
Procedure	<ol style="list-style-type: none"> 1. Enable Intel® TXT in the BIOS 2. Boot to EFI-Shell 3. Run Test to loop SENTER and SEXIT 1000 times
Test Pass/Fail Criteria	The platform successfully completes the SENTER cycle without issue

Test ID	TXT_TC0004L
Test Case Title	SINIT cycle testing with cold boot
Mandatory/Optional	Mandatory
Description	Verify the platform and Intel® TXT is functional and stable by executing cold boots after SENTER, GetSec Wakeup, SMCONTROL then SEXIT repeatedly 50 times
Objective	Stress test cold boot measured launching on the platform
Procedure	<ol style="list-style-type: none"> 1. Boot to EFI-Shell 2. Run "GETSEC64 -L SENTER -a [SINIT.BIN]" at the prompt 3. Run "GETSEC64 -L SEXIT" at the prompt. 4. Run "reset" to perform a cold boot. 5. Repeat steps 1-4, 50 times.
Test Pass/Fail Criteria	The platform successfully completes the SENTER cycle without issue

Test ID	TXT_TC0004M
Test Case Title	SINIT cycle testing with warm boot
Mandatory/Optional	Mandatory
Description	Verify the platform and Intel® TXT is functional and stable by executing warm boots after SENTER, GetSec Wakeup, SMCONTROL then SEXIT repeatedly 50 times
Objective	Stress test warm boot measured launching on the platform
Procedure	<ol style="list-style-type: none"> 1. Boot to EFI-Shell 2. Run "GETSEC64 -L SENTER -a [SINIT.BIN]" at the prompt 3. Run "GETSEC64 -L SEXIT" at the prompt. 4. Run "reset -w" to perform a warm boot. 5. Repeat steps 1-4, 50 times.
Test Pass/Fail Criteria	The platform successfully completes the SENTER cycle without issue

Test ID	TXT_TC0004N
Test Case Title	PCR17/18 Integrity
Mandatory/Optional	Mandatory
Description	PCR17/18 measured value correctness
Objective	Ensure that the measured value of the launch environment is correctly recorded in PCR17



Test ID	TXT_TC0004N
Procedure	<ol style="list-style-type: none">1. Boot to EFI-Shell2. Run "GETSEC64 -L SENTER -a [SINIT.BIN]" at the prompt3. Run "TXTINFO64 -c:a -p" at the prompt4. Check that the PCR17/18 value matches the expected value5. Run "GETSEC64 -L SEXIT" at the prompt.6. Do a cold boot7. Repeat steps 1-6, 10 times.
Test Pass/Fail Criteria	TXTINFO reports that PCR17/18 contains the expected measured value

Test ID	TXT_TC0005A
Test Case Title	SCLEAN with targeted memory configurations
Mandatory/Optional	Mandatory
Description	Verify SCLEAN functions with on all platform supported memory configurations
Objective	Validate that secret protection will work on all targeted
Procedure	<ol style="list-style-type: none">1. Setup the platform to the desired memory configurations: test with all supported memory speeds (1333 MHz, 1600 MHz), slot combinations, sizes (4 GB, 8 GB, 16 GB, 32 GB), and max memory supported - 16/32/64 GB (using up to 8 Gb DRAM in dual channel, 2 DIMMs/channel)2. Boot to EFI-Shell3. Run "GETSEC64 -L SENTER -a [SINIT.BIN]" at the prompt4. Run "SECRETS64 -S" at the prompt.5. Turn off power supply6. Turn on power supply and press the power button7. Watch SCLEAN occur8. Reset all BIOS settings (save and reset)9. Repeat steps 1-8 two more times with different memory configurations, as suggested in Step 1.
Test Pass/Fail Criteria	SCLEAN completes and the platform boots as expected in a secret protection scenario. NOTE: Refer Section X.3.9.1 for SCLEAN Manual Check steps

Test ID	TXT_TC0006A
Test Case Title	Microsoft Windows* with Intel® TXT
Mandatory/Optional	Optional
Description	Verify Windows* loads without issue with Intel® TXT options enabled in BIOS
Objective	Validate that the Intel® TXT implementation does not affect standard OS
Procedure	<ol style="list-style-type: none">1. Preload Windows*2. Enable Intel® TXT in the BIOS3. Boot Windows*
Test Pass/Fail Criteria	Test passes, if the Windows* boot is not affected by TXT being enabled in the BIOS. The platform boots Windows* as normal.



Test ID	TXT_TC0006B
Test Case Title	Microsoft Windows* S3 with Intel® TXT
Mandatory/Optional	Optional
Description	Verify Windows* S3 works without issue, when Intel® TXT options enabled in BIOS
Objective	Validate that the Intel® TXT implementation does not affect standard OS
Procedure	<ol style="list-style-type: none"> 1. Preload Windows* 2. Enable Intel® TXT in the BIOS 3. Boot Windows* 4. Put the platform into S3 5. Bring the platform out of S3 6. Shutdown the platform 7. Repeat steps 1–6, two more times (totaling three times)
Test Pass/Fail Criteria	The platform performs Windows* S3 as normal

Test ID:	TXT_TC0006C
Test Case Title	Tboot with Intel® TXT
Mandatory/Optional	Mandatory
Description	Verify Tboot is capable of loading Linux*/Xen* without issue with Intel® TXT enabled in BIOS
Objective	Validates that the platform can support launching a TXT measured environment
Procedure	<ol style="list-style-type: none"> 1. Enable Intel® TXT in the BIOS 2. Preload a Intel® TXT enabled Linux* (Fedora Tboot LiveImage) or Xen* environment 3. Boot Linux* or Xen* using tboot
Test Pass/Fail Criteria	Test passes, if Tboot log/serial/screen shows that Intel® TXT launch was successful.

Test ID	TXT_TC0006D
Test Case Title	S3 Tboot with Intel® TXT
Mandatory/Optional	Mandatory
Description	Verify the platform can successful go into S3 and restore to a TXT measured
Objective	Validate that the platform can successful go into S3 and restore back into a TXT measured environment.
Procedure	<ol style="list-style-type: none"> 1. Enable Intel® TXT in the BIOS 2. Preload a TXT enabled Linux* or Xen* environment 3. Boot Tboot-Linux*/Xen* 4. Put the platform into S3 5. Bring the platform out of S3 6. Shutdown the platform 7. Repeat steps 1–6, two more times (totaling three times)
Test Pass/Fail Criteria	The test passes, if the platform restores from S3 and puts the system back into the measured environment

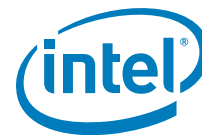


Test ID	TXT_TC0007A
Test Case Title	Factory Default TPM Establishment Setting
Mandatory/Optional	Mandatory
Description	TPM Establishment is not set in the default shipping configuration
Objective	Verify that the TPM establishment is not set in the manufacturing process
Procedure	1. Make sure the system in factory default state 2. Read memory location 0xFED40000[0] 3. The Establishment Bit can be found using TXTINFO64
Test Pass/Fail Criteria	0xFED40000[0] = 1

Test ID	TXT_TC0007B
Test Case Title	TPM Establishment when Intel® TXT is disabled
Mandatory/Optional	Mandatory
Description	TPM Establishment is not set, when Intel® TXT is disabled in BIOS
Objective	TPM Establishment is not set, when Intel® TXT disabled in the BIOS
Procedure	1. Disable Intel® TXT in the BIOS 2. Read memory location 0xFED40000[0] 3. The Establishment Bit can be found using TXTINFO64
Test Pass/Fail Criteria	0xFED40000[0] = 1

Test ID	TXT_TC0007C
Test Case Title	TPM Establishment after BIOS update
Mandatory/Optional	Mandatory
Description	TPM Establishment is not set, when the BIOS is updated
Objective	TPM Establishment is not set, when Intel® TXT when the BIOS is being updated
Procedure	1. Updated BIOS using the normal process 2. Read memory location 0xFED40000[0] 3. The Establishment Bit can be found using TXTINFO64
Test Pass/Fail Criteria	0xFED40000[0] = 1

Test ID	TXT_TC0008A
Test Case Title	Intel® TXT and Intel® AMT Interoperability
Mandatory/Optional	Optional
Description	Run measured launch on a platform that running Intel® AMT



Test ID	TXT_TC0008A
Objective	Validate that the platform will support Intel® TXT and Intel® AMT concurrency
Procedure	<ol style="list-style-type: none"> 1. Enable CSME as instructed in the CSME section 2. Enable Network Activation in Intel® MEBX AMT menu 3. Boot to EFI-Shell 4. Run "GETSEC64 -L SENTER -a [SINIT.BIN]" at the prompt 5. Run "SECRETS64 -S" at the prompt. 6. Turn off power supply 7. Turn on power supply and press the power button 8. Watch SCLEAN occur
Test Pass/Fail Criteria	Success, if SCLEAN completes as expected

Test ID	TXT_TC0008B
Test Case Title	Tboot with Intel VT-d enabled Linux* (Tboot LiveImage)
Mandatory/Optional	Optional User can skip this, if donot have Intel® VT-d capable Xen* MLE. Alternatively, user may use the TXT Tboot LiveImage that also uses VT-d.
Description	Verify Intel® VT-d is functional within a Intel® TXT measured environment.
Objective	Validate that the Intel® TXT implementation does not affect standard VMM
Procedure	<ol style="list-style-type: none"> 1. Preload tboot to launch a Intel® VT-d Enabled Linux* or Xen* (that is, Xen* with VT-d patches and grub command line switch "iommu=1"). 2. Enable Intel® TXT and Intel® VT-d in the BIOS. 3. Tboot Intel® VT-d enabled Linux* or Xen*. 4. Assign a bus-device-fn of a device to guest. (Refer to the Intel® VT-d section and the Tboot usage kit for additional detail).
Test Pass/Fail Criteria	Success criteria is the guest can access the device after assignment

Test ID	TXT_TC0008C(REMOVE)
Test Case Title	Intel® TXT, when CSME is Disabled
Mandatory/Optional	Optional - If this option is provided by the BIOS
Description	Invoke measured launch and SCLEAN, when the platform has CSME disabled
Objective	Validate that the platform will support Intel® TXT independent of ME
Procedure	<ol style="list-style-type: none"> 1. Disable CSME as instructed in the CSME section 2. Boot to EFI-Shell 3. Run "GETSEC64 -L SENTER -a [SINIT.BIN]" at the prompt 4. Run "SECRETS64 -S" at the prompt. 5. Turn off power supply 6. Turn on power supply and press the power button 7. Watch SCLEAN occur



Test ID	TXT_TC0008C(REMOVE)
Test Pass/Fail Criteria	Success, if SCLEAN completes as expected. NOTE: Refer Section X.9.3.1 for SCLEAN Manual Check steps

Test ID	TXT_TC0008D
Test Case Title	Intel® TXT when CSME is Enabled
Mandatory/Optional	Optional
Description	Invoke measured launch and SCLEAN, when the platform has CSME enabled
Objective	Validate that the platform will support Intel® TXT independent of ME
Procedure	<ol style="list-style-type: none"> 1. Enable CSME as instructed in the CSME section 2. Boot to EFI-Shell 3. Run "GETSEC64 -L SENTER -a [SINIT.BIN]" at the prompt 4. Run "SECRETS64 -S" at the prompt. 5. Turn off power supply 6. Turn on power supply and press the power button 7. Watch SCLEAN occur
Test Pass/Fail Criteria	Success, if SCLEAN completes as expected. NOTE: Refer Section X.9.3.1 for SCLEAN Manual Check steps

Test ID	TXT_TC0009A
Test Case Title	Install SINIT ACM Driver for Windows
Mandatory/Optional	Optional
Description	Install SINIT ACM Driver for Windows for use for with Windows Update
Objective	Validate that the platform will successfully Install SINIT ACM Driver
Procedure	<ol style="list-style-type: none"> 1. Find ACM ACPI Device in Device Manager 2. Install SINIT ACM Driver 3. Verify driver was successfully installed in Device Manager
Test Pass/Fail Criteria	<p>Success, if SINIT ACM Driver Successfully installs and "Intel® Authenticated Code Module" appears in Device Manager and SINIT ACM is copied into Windows/System32 folder as "acm.bin".</p> <p>Please refer to the readme file in the SINIT Driver kit for more information.</p>

§ §



(This page intentionally left blank.)



14 Intel® Integrated Clock Control Compliance

This chapter covers details of ICC test cases supported by all CML platforms across different segments.

ICC feature support:

ICC feature support is based on a PCH used on the platform. Refer below table for more details.

PCH Supported	ICC Feature/Configuration Supported
CML-LP SKUs	<ul style="list-style-type: none">• Standard• Adaptive
CML-H SKUs	<ul style="list-style-type: none">• Standard• Adaptive

ICC Profile and parameters configuration recommendation

- Review Intel® Bringup Guide to get familiar with supported frequency and SSC configurations for above features.
- OEMs are recommended to configure ICC Boot profile and parameters for the profile via Intel® FIT -> ICC tab. Make sure to choose appropriate profile and configure parameters to meet platform and HW requirements.

CCT Tool usage

- for manual testing CCT tool located under ./System_Tools/ICC Tools/ is required.

ICC PETS test package details

The test cases supported by platforms using Intel® Platform Enablement Test Suite (Intel® PETS) are defined as a part of Compliance_ICC_*.xml. Select respective ICC package since this version of PETS supports different PCHs.

- For CML-LP SKUs, select xml file from: ./CML/./**Compliance_ICC_CML-LP**
- For CML-H SKUs, select xml file from: ./CML/./**Compliance_ICC_CML_H**

NOTE: pets automation will available in future releases



14.1 Test Coverage Summary for CML-LP and CML-H

Test ID	Test Case Title	Mandatory	PETS/ Manual	Applicable to PCH SKU	Network Factor
ICC_TST_01	Test default settings for Standard configuration	Yes (Only mandatory when SUT's boot profile is selected based on standard profile under FIT or by means of BIOS)	PETS /Manual using ICC SDK embedded	<ul style="list-style-type: none"> CML- LP CML-H 	LAN+WLAN; WLAN only
ICC_TST_02	Test default settings for Adaptive configuration	Yes (Only mandatory when SUT's boot profile is selected based on adaptive profile under FIT or by means of BIOS)	PETS/Manual using ICC SDK embedded	<ul style="list-style-type: none"> CML-LP CML-H 	LAN+WLAN; WLAN only
ICC_TST_04	Test Get and Set of MPHY setting	Yes	PETS/Manual using ICC SDK embedded	<ul style="list-style-type: none"> CML-LP CML-H 	LAN+WLAN; WLAN only

14.2 Test cases

14.2.1 Test Default Settings for Standard Configuration

Test ID:	ICC_TST_01
Test Case Title:	Test default settings for Standard configuration
Mandatory/Optional:	<p>Mandatory.</p> <p>Note: Only for SUTs with boot profile that to "standard" profile under FIT ->ICC -> Boot Profile or by means of BIOS</p> <p>Note: For FIT Tool, Check parameter under FIT Integrated Clock Controller Boot Profile selection. if Boot profile selection is based on Standard profile, then this test is mandatory otherwise it can be skipped.</p> <p>Note: For BIOS, Check parameter using the request to HECI: ICC_GET_PROFILE_REQ if Boot profile selection is based on Standard profile, then this test is mandatory otherwise it can be skipped.</p>
Description:	Verify if the current ICC registers setting in the SUT are set correctly based on standard configuration



Test ID:	ICC_TST_01
Objective:	Ensure that critical ICC register values are configured correctly for standard configuration.
Procedure:	<p>Get BCLK PLL Settings:</p> <ul style="list-style-type: none">• API: <code>ICC_GET_CLOCK_SETTINGSEX</code>• library method: <code>EXTERNAL_API UINT32IccLibGetCurrentClockSettingsWrapper(const ICC_HECI_CLOCK_ID clockId, ICC_GET_CLOCK_SETTINGSEX * const clockSettings);</code> <p>An error should be returned in case the test has failed</p>
Test Pass/Fail Criteria:	<p>Pass if the critical ICC registers values read are set correctly based on the standard configuration. Frequency= 400 MHZ SSC = 0.5</p> <p>Note: For FIT, Check parameter under Flash Image Tool Integrated Clock Controller Boot profile selection. If Boot profile is not based on standard profile then this test is expected to fail.</p> <p>Note: For BIOS, check parameter using the request to HECI: ICC_GET_PROFILE_REQ if Boot profile is not based on standard profile then this test is expected to fail.</p>

14.2.2 Test Default Settings for Adaptive Configuration

Test ID:	ICC_TST_02
Test Case Title:	Test default settings for Adaptive configuration
Mandatory/Optional:	<p>Mandatory</p> <p>Note: Only for SUTs with boot profile set to "Adaptive" profile under FIT ->ICC -> Boot Profile or by means of BIOS.</p> <p>Note: For FIT Tool, Check parameter under FIT Integrated Clock Controller Boot profile selection. if boot profile selection is based on Adaptive profile, This test is mandatory else the user can skip to execute it.</p> <p>Note: For BIOS check parameter using the request to HECI: ICC_GET_PROFILE_REQ if Boot profile selection is based on Adaptive profile, then this test is mandatory otherwise it can be skipped.</p>
Description:	Verify if the current ICC registers setting in the SUT are set correctly based on Adaptive configuration



Test ID:	ICC_TST_02
Objective:	Ensure that critical ICC register values match defaults for Adaptive configuration
Procedure:	<p>Get BCLK PLL Settings:</p> <ul style="list-style-type: none"> API: <code>_ICC_SET_CLOCK_SETTINGSEX</code> Library method: <code>EXTERNAL_API UINT32IccLibGetCurrentClockSettingsWrapper(const ICC_HECI_CLOCK_ID clockId, ICC_GET_CLOCK_SETTINGSEX * const clockSettings);</code> <p>An error should be returned in case the test has failed</p> <p>Set the BCLK PLL settings:</p> <ul style="list-style-type: none"> API: <code>_ICC_SET_CLOCK_SETTINGSEX</code> Library method: <code>EXTERNAL_API UINT32 IccLibSetCurrentClockSettingsWrapper(const ICC_HECI_CLOCK_ID clockId, ICC_SET_CLOCK_SETTINGSEX * clockSettings);</code> <p>An error should be returned in case the test has failed</p>
Test Pass/Fail Criteria:	<p>Pass if the critical ICC registers values read are set correctly based on the Adaptive configuration.</p> <p>Note: For FIT, Check parameter under Flash Image Tool Integrated Clock Controller Boot profile selection. If Boot profile is not based on Adaptive profile then this test is expected to fail.</p> <p>Note: For BIOS check parameter using the request to HECI: ICC_GET_PROFILE_REQ if Boot profile selection is based on Adaptive profile, then this test is mandatory otherwise it can be skipped.</p> <p>Note: Default frequency and SSC supported for Adaptive is 97.5MHz with 0.50%. Supported Min.-Max. frequency range is [97.5- 100 MHz]. This test checks default configuration for Adaptive clocking. Test may fail if customer change SSC or frequency from default value; however make sure to check if settings are within the expected range supported for Adaptive clocking.</p>



14.2.3 GET and SET MPHY Settings

Test ID:	ICC_TST_04
Test Case Title:	Get and Set of MPHY setting
Mandatory/Optional:	Mandatory, This is informative test.
Description:	<p>This test output high level detail like CRC count into a bin file, Version and product detail of chipset initialization settings.</p> <p>this test apply a new version of chipset User to manually verify data is correct or not.</p>
Objective:	<p>Verify if correct version of chipset initialization settings are applied or not. In case issue is seen, detail like CRC count, Version and product detail can be used for debug purpose.</p> <p>Apply a new version of chipset initialization settings</p>
Procedure:	<p>GET MPHY Version: API: _GET_MPHY_VERSION library method: EXTERNAL_API UINT32 IccLibGetMphyVersion(GET_MPHY_VERSION *survTable);</p> <p>GET MPHY table: library method: EXTERNAL_API UINT32 IccLibGetMphySettingsWrapper(UINT32 length, UINT32 offset, UINT8 *buffer,UINT32 *bytesRead);</p> <p>Set MPHY table: library method: EXTERNAL_API UINT32 IccLibSetMphySettingsWrapper(char *mphyFileName);</p> <p>Note: Retrieving Chipset Initialization file and information can be blocked by some restrictions enforced with End-of-Post being issued. Tester may require to disable End-of-Post message from BIOS menu for the test to successfully pass.</p> <p>Note: This test currently displays the command result only.</p>
Test Pass/Fail Criteria:	This is informative test and displays details like CRC count, Version and product detail. User to manually confirm if data looks correct or not.





15 Media Playback

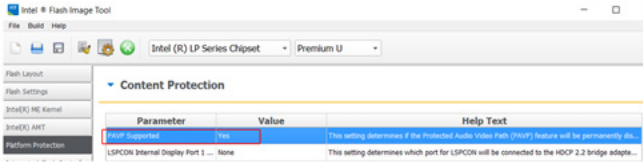
Protected Media Playback is supported by Intel® CSME firmware. The table below documents compliancy tests to verify Protected Content is working on the platform.

15.1 Test Coverage—Summary and Details

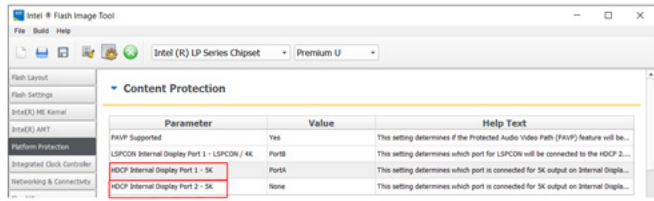
Test ID	Test Case Title	PETS/Manual	Form Factor
Media_001	Verify default configuration settings for Protected Audio Video Path [PAVP] in Firmware Image Tool [FIT]	Manual	DT, MB, WS/Server
Media_003	Verify Internal Port configuration in Firmware Image Tool [FIT]	Manual	DT, MB, WS/Server
Media_004	Verify PAVP Enabled in BIOS (<i>Only if the SUT BIOS menu displays PAVP Mode</i>)	Manual	DT, MB, WS/Server
Media_005	Protected Content Playback (Mandatory)	Manual	DT, MB, WS/Server
Media_006	Interaction of Protected Content Playback with Power Management features (Mandatory)	Manual	DT, MB, WS/Server


Note: DT = Desktop, MB = Mobile, WS/Server = Workstation/Server

Test ID:	Media_001
Test Case Title:	Verify default configuration settings for Protected Audio Video Path [PAVP] in Firmware Image Tool [FIT]
Platform	CML
Mandatory/Optional:	Mandatory
Mobile Only:	No
Firmware SKU:	Consumer/Corporate
Description:	Intel® CSME initiates PAVP secure session in firmware for key exchange and encryption for Content from Media player or cloud. PAVP can be enabled or disabled using FIT Tool. In this test we verify the PAVP is enabled in the SUT SPI image using FIT.
Objective:	Verify if the PAVP control in Intel® FIT are set correctly

Test ID:	Media_001
Procedure:	<ol style="list-style-type: none"> 1. Open customer image in FIT tool 2. Got to Platform Protection tab 3. Verify and ensure if the 'PAVP Supported Parameter' is set to 'Yes' 
Test Pass/Fail Criteria:	Test passes is FIT PAVP parameter is set to 'Yes' when we open SPI image in FIT.

Test ID:	Media_003
Test Case Title:	Verify Internal Port configuration in Firmware Image Tool [FIT]
Platform	CML
Mandatory/Optional:	Mandatory
Mobile Only:	No
Firmware SKU:	Consumer/Corporate
Description:	<p>For configuring ports that are connected to internal SUT panel or eDP panel Intel® CSME provides configuration parameter in FIT to assign port to internal.</p> <p>In this test we verifies what are the Internal port assignment set in SUT SPI image and confirm if they are intended ports to configured as internal.</p> <p>Note: Only ports that are planed to be connected to internal panels /eDP should be assigned as internal Port A is set as the default Internal port by Intel® ME. If you set the FIT parameter for internal port to 'None' Intel® CSME assigns Port A to internal. When a port is set to internal HDCP encryption is by-passed by Intel® CSME even if the content license requires it. Do not assign ports that are planned to be connected to HDMI,DVI,DP to internal.</p>
Objective:	Verify if the internal port configuration parameter in FIT assigns the right port.

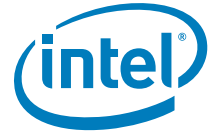
Test ID:	Media_003
Procedure:	<ol style="list-style-type: none"> 1. Open customer image in FIT tool 2. Got to Platform Protection tab 3. Verify the right ports are assigned in the Internal Port parameters 
Test Pass/Fail Criteria:	Test pass criteria: The FIT Internal Port parameters have the right ports assigned intended to be connected to internal panel/eDP

Test ID:	Media_004
Test Case Title:	Verify PAVP Enabled in BIOS
Platform	CML
Mandatory/Optional:	Mandatory (Only if the SUT BIOS menu displays PAVP Mode)
Mobile Only:	No
Firmware SKU:	Consumer/Corporate
Description:	PAVP can be configured in the BIOS. In this test we verifies what the PAVP mode is enabled in SUT BIOS.
Objective:	Verify PAVP configuration in BIOS
Procedure:	<ol style="list-style-type: none"> 1. Boot system to BIOS menu 2. Navigate in BIOS menu where you have PAVP Option [example: in Intel BIOS goto - Intel Advance Menu->System Agent (SA) Configuration->Graphics Configuration-> PAVP Enable 3. Verify the PAVP mode setup 
Test Pass/Fail Criteria:	Test passes if we PAVP is enabled in SUT BIOS.



Test ID:	Media_005
Test Case Title:	Protected Content Playback
Mandatory/Optional:	Mandatory
Platform:	CML
Mobile Only	No
Firmware SKU:	Consumer/Corporate
Description:	<p>This is an end to end test of Blu-ray Disc* Playback using an HDCP 2.0 compliant ISV media player.</p> <p>Content under test include MPEG2, VC1 and H.264 (AVC) decode formats. These tests utilizes ISV players to play protected content on the local display as well as Wireless Display for all supported decode formats with hardware acceleration enabled. Visual verification is used to confirm any corruption during playback. Third party screen scraper applications are applied to attempt capture of the premium content.</p>
Objective:	To demonstrate Blu-ray Disc* playback by means of the successful key exchange between Intel® ME, Chipset and Graphics/Audio driver and Wireless Display.
Procedure:	<ol style="list-style-type: none">1. Install Intel® ME Firmware/Software on system under test2. Install GFX driver on system under test3. Install Intel a supported Wi-Fi module4. Install Intel Wi-Fi Driver5. Install Intel Wireless Display 3.0 software6. Install an ISV player on the system under test7. Attempt to play a Blu-ray Disc* (MPEG2, H.264, VC-1). Playback should be clear and smooth8. Attempt to copy or capture of the displayed content by means of a screen scraper application Using only the local display9. Attempt to copy or capture of the displayed content by means of a screen scraper application Using Intel Wireless Display 3.0 repeat procedure 8. <p>Note: HDCP 2.0 requires a v2 Intel® WiDi Adapter.</p>
Test Pass/Fail Criteria:	Test passes if Blu-ray Disc* content is played successfully on the local screen and the Wireless Display screen with audio and without visual corruption. Also no premium content should be captured by the screen scraper application.

Test ID:	Media_006
Test Case Title:	Interaction of Protected Content Playback with Power Management features
Mandatory/Optional:	Mandatory
Platform:	CML
Mobile Only	No
Firmware SKU:	Consumer/Corporate
Description:	<p>This is an end to end test of Blu-ray Disc* Playback using an HDCP 2.0 compliant ISV media player.</p> <p>Content under test include MPEG2, VC1 and H.264 (AVC) decode formats. These tests utilizes ISV players to play protected content on the local display as well as Wireless Display for all supported decode formats with hardware acceleration enabled. Visual verification is used to confirm any corruption during playback. Third party screen scraper applications are applied to attempt capture of the premium content.</p>



Test ID:	Media_006
Objective:	To demonstrate Blu-ray Disc* playback by means of the successful key exchange between Intel® ME, Chipset, and Graphics/Audio driver and Wireless Display.
Procedure:	<ol style="list-style-type: none"> 1. Install Intel® ME Firmware/Software on system under test. 2. Install GFX driver on system under test 3. Install Intel a supported Wi-Fi module 4. Install Intel Wi-Fi Driver 5. Install Intel Wireless Display 3.0 software 6. Install an ISV player on the system under test 7. Put system into either S3 or S4 and then resume 8. Attempt to play a Blu-ray Disc* (MPEG2, H.264, VC-1). Playback should be clear and smooth 9. Attempt to copy or capture of the displayed content by means of a screen scraper application Using only the local display 10. Attempt to copy or capture of the displayed content by means of a screen scraper application Using Intel Wireless Display 3.0 repeat procedure 8. <p>Note: HDCP 2.0 requires a v2 Intel® WiDi Adapter.</p>
Test Pass/Fail Criteria:	Test passes if Blu-ray Disc* content is played successfully on the local screen and the Wireless Display screen with audio and without visual corruption. Also no premium content should be captured by the screen scraper application

Note: If respective graphics validation team has covered local display and Wireless Display Blu-ray Disc* playback with ISV software, for ME PAVP/HDCP2 validation testing then PAVP media playback tests outlined in test 001 and 002 are not mandatory.

§ §



16 Intel® Dynamic Application Loader (Intel® DAL)

16.1 Introduction

Intel® Dynamic Application Loader (Intel® DAL) is an Intel® CSME infrastructure for applications such as Intel® Identity Protection Technology (Intel® IPT), Intel® Authenticate, Intel® SGX and others.

The following table documents compliance tests to verify Intel® Dynamic Application Loader (Intel® DAL) is working on the platform.

This Test plan is targeted at all OEMs.

Note: application testing is out of this compliance guide scope.

16.2 Test Environment

Note: No OEM implementation is required on the board/BIOS or EC level. Intel® CSME should be set to Enabled in FIT when creating the firmware image.

The Management console could be a laptop or a desktop a version of Windows* supported by Intel® Platform Enablement Test Suite. The network to use is a hub/switch and network cables.

The Intel® DAL tests should not be conducted in Windows* Server 2008 as Intel® DAL currently does not supports this OS.

16.2.1 Tools for Testing

Intel® Platform Enablement Test Suite—Latest version of the tool from the Intel® CSME Compliance kit release. Refer the Intel® Platform Enablement Test Suite (Intel® PETS) user guide available in the Intel® Compliance kit for exact instructions on how to load and setup the Intel® Platform Enablement Test Suite software.

Package DAL.xml should be loaded to Intel® PETS in order to compete the tests in this section

16.2.2 Prerequisites

The following software components need to be available in the platform OS:

Intel® MEI Driver:

This is the interface used for communication between the host OS components and the Intel® CSME components (included in the general Intel® CSME installer kit).

Intel® Dynamic Application Loader (Intel® DAL) host software components:

Exposes an API that allows communication between the host client and the application (included in the general Intel® CSME installer kit)



16.3 Test Coverage Summary and Details

Test ID	Test Case Title	PETS/Manual	Form Factor
DAL_001	Intel® DAL applications cleanup	PETS	DT/MB/AIO/WS-Server
DAL_002	Intel® DAL test application installation and load	PETS	DT/MB/AIO/WS-Server
DAL_003	Intel® DAL communication channel exercise	PETS	DT/MB/AIO/WS-Server

Note: DT = Desktop, MB = Mobile, AIO = All In One, WS-Server = WS-Server

Note: OS test runs on Microsoft* Windows* 7/8.x/10.

Test ID:	DAL_001
Test Case Title:	Intel® DAL applications cleanup
Mandatory/Optional:	Mandatory for those who implement Intel® IPT
Firmware SKU:	All Consumer and Corporate SKUs (Desktop, Mobile, and Workstation)
Description:	Intel® DAL applications cleanup mechanism test
Objective:	To test that the Intel® Dynamic Application Loader (Intel® DAL) clean-up mechanism works properly, and no application is currently running in Intel® DAL
Procedure:	<p>Start test DAL_001 in the Intel® Platform Enablement Test Suite from management console.</p> <p>Intel® Platform Enablement Test Suite performs the following steps:</p> <ol style="list-style-type: none"> 1. Confirm the Intel® Dynamic Application Loader (Intel® DAL) is enabled in firmware. 2. Confirm needed Host software components are available (Intel® MEI driver and Intel® Dynamic Application Loader (Intel® DAL) host software). 3. Perform cleanup of all Intel® DAL applications.
Test Pass/Fail Criteria:	All steps return the value "Passed"

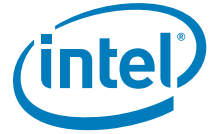
Test ID:	DAL_002
Test Case Title:	Intel® DAL test application installation and load
Mandatory/Optional:	Mandatory for those who implement Intel® IPT
Firmware SKU:	All Consumer and Corporate SKUs (Desktop, Mobile, and Workstation)
Description:	Intel® DAL test application is installed and loaded, verifying basic functionality of Intel® DAL applications execution capability.



Test ID:	DAL_002
Objective:	To test that the Intel® Dynamic Application Loader (Intel® DAL) basic functionality works properly.
Procedure:	<p>Start test DAL_002 in the Intel® Platform Enablement Test Suite from management console.</p> <p>Intel® Platform Enablement Test Suite performs the following steps:</p> <ol style="list-style-type: none">1. Confirm the Intel® Dynamic Application Loader (Intel® DAL) is enabled in firmware.2. Confirm that the needed Host software components are available (Intel® MEI driver and Intel® Dynamic Application Loader (Intel® DAL) host software).3. Confirm test application can be installed and loaded to Intel® Dynamic Application Loader.4. Unload the test application.
Test Pass/Fail Criteria:	All steps return the value "Passed"

Test ID:	DAL_003
Test Case Title:	Intel® DAL communication channel exercise
Mandatory/Optional:	Mandatory for those who implement Intel® IPT
Firmware SKU:	All Consumer and Corporate SKUs (Desktop, Mobile, and Workstation)
Description:	Intel® DAL test application is installed and loaded, followed by a communication channel exercise between application and host side application.
Objective:	To test that the Intel® Dynamic Application Loader (Intel® DAL) application can communicate successfully with a host application.
Procedure:	<p>Start test DAL_003 in the Intel® Platform Enablement Test Suite from management console.</p> <p>Intel® Platform Enablement Test Suite performs the following steps:</p> <ol style="list-style-type: none">1. Confirm the Intel® Dynamic Application Loader (Intel® DAL) is enabled in firmware.2. Confirm needed Host software components are available (Intel® MEI driver and Intel® Dynamic Application Loader (Intel® DAL) host software).3. Exercise basic communication channel between test application and host to verify connectivity flow4. Unload the test application.
Test Pass/Fail Criteria:	All steps return the value "Passed".





17 Intel® Platform Trust Technology (Intel® PTT) Compliance

Intel® Platform Trust Technology (Intel® PTT) is the Intel implementation of TCG TPM 2.0 standard in firmware. For more information about Intel® PTT integration with BIOS refer BIOS Writers Guide and Intel® PTT Overview documentation.

The purpose of this section is to describe the tests required to verify PTT is functional, main PTT end to end use cases are working and platform meets Windows* 10 requirements for TPM 2.0 support.

The scope of this section is end to end testing and is not intended to provide TPM command level testing.

Note: Intel Boot Guard testing with Intel® PTT is out of scope of this chapter and should be done as part of Intel Boot Guard testing.

Test Environment for PTT Compliance Section:

- Canon Lake Platform with Intel® PTT enabled
- Windows* 10 Professional or Enterprise installed in UEFI mode
- Intel® CSME firmware and Intel® PTT enabled

Tools for Testing:

- Intel® Platform Enablement Test Suite (Intel® PETS)—Latest version of the tool from the Intel® CSME Compliance kit release. Refer the Intel® Platform Enablement Test Suite (Intel® PETS) user guide available in the Intel Compliance kit for exact instructions on how to load and setup the Intel® Platform Enablement Test Suite (Intel® PETS) software.
- Windows* 10 HLK Testing Environment
- manage-bde.exe (Windows* command line tool for BitLocker Driver Configuration)
- bdehdcfg.exe (Windows* command line tool for BitLocker Drive Encryption)
- makecert.exe (command line tool, part of Windows* 10 SDK)
- pvk2pfx.exe (command line tool, part Windows* 10 SDK)
- CertUtil.exe (Windows* 10 Command line tool)



17.1 Test Coverage Summary

The table below describes the test methodology, where:

- How?: A = Fully Automated using Intel® PETS, I = Interactive using Intel® PETS and M = Manual.

Test ID	Test Case Title	How?
PTT_001	CRB Interface Communication Test	A
PTT_002	Intel® PTT Windows* 10 Basic Functionality	A
PTT_003	TPM Clear and Physical Presence	A
PTT_004	Windows* 10 BitLocker Integration	A
PTT_005	Windows* 10 BitLocker TPM Protection	A
PTT_006	Windows* 10 Virtual Smart Card (VSC) Tests	A
PTT_007 ¹	Microsoft* Windows* HLK TPM Tests	M
PTT_008	Intel® PTT Enable/Disable from BIOS	M
PTT_009	Power Transition Testing with Intel® PTT Enabled	A
PTT_010	Dictionary Attack Lockout After Coin Battery Removal with EOM Commit	M

Notes:

1. This test is not required for Intel® CSME compliance but may be required for Microsoft* logo certification. For any questions or support issues when running this test, refer Microsoft* support.



17.2 Verification of BIOS and Intel® PTT Communication Over CRB Interface

Test ID:	PTT_001
Test Case Title:	CRB Interface Communication Test
Mandatory/Optional:	Mandatory Note: This test uses CRB access and therefore needs to run with disabled driver to ensure elimination of false failures.
Description:	The test confirms that BIOS correctly implements the CRB protocol for communication with Intel® PTT
Objective:	Verify BIOS is able to successfully send commands to Intel® PTT
Procedure:	<ol style="list-style-type: none"> 1. Confirm Intel® PTT is enabled in the SPI image. 2. Relinquish locality 0: Write 1 to TPM_LOC_CTRL_0.Relinquish (0xfed40008, bit 1). 3. Request locality 0: Write 1 to TPM_LOC_CTRL_0.RequestAccess (0xfed40008, bit 0). 4. Verify TPM_LOC_STATE_x.locAssigned field (0xfed40000, bit 1) is set to 1 and that TPM_LOC_STATE_x.activeLocality field (0xfed40000, bits 2-4) is set to 000. 5. Write 1 to TPM_CRB_CTRL_REQ_0.cmdReady (0xfed40040, bit 0). 6. Poll TPM_CRB_CTRL_REQ_0.cmdReady every 5 ms for 500 ms until it is 0. 7. Verify TPM_CRB_CTRL_STS_0.tpmIdle (0xfed40044, bit 1) is 0. 8. Write a TPM command such as TPM2_SelfTest to TPM_CRB_DATA_BUFFER register (0xfed4_0080). 9. Write "1" to the TPM_CRB_CTRL_START register (0xFED4_004C). 10. Poll the TPM_CRB_CTRL_START register (0xfed4_004C) until its value becomes "0". 11. Write 1 to TPM_CRB_CTRL_REQ_0.goIdle (0xfed40040, bit 1). 12. Poll TPM_CRB_CTRL_REQ_0.goIdle for 500ms until it is 0. 13. Relinquish locality 0: Write 1 to TPM_LOC_CTRL_0.Relinquish (0xfed40008, bit 1). 14. Verify TPM_LOC_STATE_x.locAssigned field (0xfed40000, bit 1) is set to 0 and TPM_LOC_STATE_x.activeLocality field (0xfed40000, bits 2-4) is set to 000. 15. Request locality 0: Write 1 to TPM_LOC_CTRL_0.RequestAccess (0xfed40008, bit 0). <p>Note: For detailed information on how to send a TPM command, refer the PC client specific platform TPM profile for TPM 2.0.</p>
Test Pass/Fail Criteria:	<p>If TPM_CRB_CTRL_START register returns 0x00 after the duration listed in Table 15 of the TCG specification for the test command sent and before the listed timeout, the TPM command is received by PTT through HCI, the test passes, else fails. Test fails also if a timeout occurs at any other stage.</p> <p>Note: HCI reference code provides serial output status of whether or not TPM command is received by PTT. Check PttHciReceive function for more details.</p>



17.3 Intel® PTT Basic Functionality Under Windows* 10

Test ID:	PTT_002
Test Case Title:	Intel® PTT Basic Functionality Under Windows* 10
Mandatory/Optional:	Mandatory
Description:	Verify Intel® PTT has been enabled on the platform and Intel® PTT is functional on Windows* 10
Objective:	Windows* can successfully communicate with Intel® PTT
Procedure:	<ol style="list-style-type: none">1. Boot to Windows* 10 UEFI installation2. Open Device Manager (devmgmt.msc) and verify a "Trusted Platform Module 2.0" device exists in "Security Devices"3. Open Trusted Platform Module (TPM) Management Page (tpm.msc)4. Verify Status is "The TPM is ready for use."5. Open an elevated command prompt with admin privileges and enter powershell (type powershell at prompt)6. Prepare the WMI object for querying Intel® PTT information by typing: <code>\$ptt = get-wmiobject -namespace "root/cimv2/security/microsofttpm" win32_tpm</code>7. Check different Intel® PTT parameters by typing the following at the PS prompt:<ol style="list-style-type: none">d. <code>\$ptt.IsEnabled()</code>e. <code>\$ptt.IsActivated()</code>f. <code>\$ptt.IsAutoProvisioningEnabled()</code>g. <code>\$ptt.IsOwned()</code>h. <code>\$ptt.IsReadyInformation()</code>
Test Pass/Fail Criteria:	No "yellow bang" in device manager, Intel® PTT is the TPM device and all TPM queries return "true"



17.4 Trusted Platform Module (TPM) Clear and Physical Presence

Test ID:	PTT_003
Test Case Title:	TPM Clear and Physical Presence
Mandatory/Optional:	Mandatory
Description:	TPM Clear command erases user data on the TPM. TPM Clear requires BIOS to check for physical presence to authorize the TPM Clear operation. User save the SrkPublicKey and verify that new/old SRK keys differ after TPM Clear.
Objective:	Verify TPM clear and take ownership flows work correctly under Windows* 10 OS and physical presence asserted.
Procedure:	<ol style="list-style-type: none"> Save the current SrkPublicKey by performing the following actions: <ol style="list-style-type: none"> Open elevated command prompt and enter PowerShell by typing "powershell" at the prompt and type: \$ptt = get-wmiobject -namespace "root/cimv2/security/microsofttpm" win32_tpm \$ret = \$ptt.GetSrkPublicKeyModulus() \$ret.SrkPublicKeyModulus > SrkPubModOld.txt Run "tpm.msc" to open TPM Management Console Click 'Clear TPM...' in the Actions pane on right. In the pop-up window click 'Restart' to invoke TPM Clear flow. Upon reboot, a physical presence authorization message may be displayed (BIOS setting dependent) requiring the user to press a key to authorize the TPM clear or abort. In CRB, F12 authorizes, ESC rejects the operation. Upon booting to Windows*, pop-up window shows up indicating OS is taking ownership of the TPM After ownership operation completes, press OK. Save the new SrkPublicKey by performing the following actions: <ol style="list-style-type: none"> Open elevated command prompt and enter PowerShell by typing "powershell" at the prompt and type: \$ptt = get-wmiobject -namespace "root/cimv2/security/microsofttpm" win32_tpm \$ret = \$ptt.GetSrkPublicKeyModulus() \$ret.SrkPublicKeyModulus > SrkPubModNew.txt Compare the old and new keys
Test Pass/Fail Criteria:	OS takes ownership of TPM, new/old keys differ.



17.5 Windows* 10 BitLocker Integration

Test ID:	PTT_004
Test Case Title:	Windows* 10 BitLocker Integration
Mandatory/Optional:	Mandatory
Description:	BitLocker uses Intel® PTT to store and retrieve keys securely, in addition Windows* BitLocker confirms system components did not change by checking system load measurements saved to TPM. The test verifies BitLocker can be activated, BitLocker can encrypt, decrypt, and restart encryption after reboot.
Objective:	Test BitLocker integration with Intel® PTT
Procedure:	<ol style="list-style-type: none">1. In elevated permissions command line run: "bdehdcfg.exe -driveinfo" and check system drive is configured to support BitLocker2. Set BitLocker to use TPM for measuring boot devices in Windows* Group Policy by:<ol style="list-style-type: none">a. Run "gpedit.msc" to open Group Policy Editorb. Open "Local Computer Policy" > "Computer Configuration" > "Administrative Templates" > "Windows Components" > "BitLocker Drive Encryption" > "Operating System Drives"c. On the right pane double click "Configure TPM platform profile for native UEFI firmware configuration"d. Check the enabled radio button. Verify PCR 0, PCR2, PCR4 and PCR11 are checked in the "Options" pane.e. Click apply and OK.f. Commit the group policy change by typing "gpupdate /force" in an elevated command prompt <p>Note: This action is required once per OS installation</p> <ol style="list-style-type: none">3. Set up tpm as a bitlocker protector with recovery password and turn-on BitLocker by typing the following at the command prompt<ol style="list-style-type: none">a. manage-bde -protectors -add c: -tpmb. manage-bde -protectors -add c: -rp 000000-000000-000000-000000-000000-000000-000000-000000c. manage-bde -on c:d. shutdown -r -t 04. After OS completes reboot, verify no error messages displayed. Wait for "Encryption in Progress" notification or type "manage-bde -status" to check on encryption status5. After encryption reaches 10%, restart system, and verify encryption continues without error message after reboot completes.6. Turn off BitLocker by typing "manage-bde -off c:" at the command line, decryption process should start7. After decryption process ends, reboot and verify system boots into OS without error message. BitLocker should be off
Test Pass/Fail Criteria:	All system boots complete successfully and OS loads.



17.6 BitLocker TPM Protection

Test ID:	PTT_005
Test Case Title:	BitLocker TPM Protection
Mandatory/Optional:	Optional
Description:	When BitLocker is set to use TPM protection, BitLocker enters recovery mode if any protected component changed during boot. By disabling Intel® PTT, user checks BitLocker is indeed using TPM as key protector.
Objective:	Verify BitLocker is using Intel® PTT as a key protector
Procedure:	<ol style="list-style-type: none"> 1. Encrypt the OS drive using BitLocker with TPM protection (follow instructions in PTT_004 steps 1 through 5, and wait till drive encryption reaches 10%) 2. Run manage-bde -status and verify drive is "protected" 3. Create a measured boot failure in order to trigger Bitlocker Recovery <ol style="list-style-type: none"> a. In BIOS, choose disable Intel® PTT or send a TPM_Clear command. Note: Clearing TPM by means of the OS disables Bitlocker and would not prompt the user for his recovery password. The TPM must be cleared by the BIOS. b. System should boot into BitLocker recovery screen. Provide the recovery password to continue boot. c. Verify boot completes successfully 4. Disable BitLocker by typing "manage-bde -off c:" at the command line, decryption process should start 5. After decryption process ends, reboot and verify system boots into OS without error message. BitLocker should be off
Test Pass/Fail Criteria:	BitLocker completes drive encryption successfully and reboots. System displays BitLocker recovery screen after choosing Disable Intel® PTT or Clear TPM in BIOS setup.



17.7 Virtual Smart Card Tests

Test ID:	PTT_006
Test Case Title:	Virtual Smart Card (VSC) Tests
Mandatory/Optional:	Optional
Description:	Virtual Smart Card is a new Microsoft* use case for TPMs. More information on VSC can be found on Microsoft* web site. This test verifies a VSC can be created and certificate installed so VSC is accessible
Objective:	Intel® PTT can be used to support VSC use case
Procedure:	<ol style="list-style-type: none">1. Create a VSC running the following command on an elevated command line: <code>tpmvscmgr.exe create /name TPM2VSC /adminkey random /PUK default /pin default /generate</code>2. Verify that TPM2VSC smart card reader was created in "Smart card readers" in device manager3. Restart Windows*, and check the device is not yellow banded in device manager4. Create and import a self-signed certificate into the VSC<ol style="list-style-type: none">a. Ensure the following registry keys exist under [HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Cryptography\Defaults\Provider\Microsoft Base Smart Card Crypto Provider]:<ul style="list-style-type: none">• "AllowPrivateSignatureKeyImport"=DWord:00000001• "AllowPrivateExchangeKeyImport"=DWord:00000001b. Open an elevated command promptc. Type: <code>MakeCert.exe -sky exchange -r -n "CN=TPM2VSCCert" -pe -a sha1 -len 2048 -ss My -m 36 -sv "TPM2VSCCert.pvk" "TPM2VSCCert.cer"</code>d. When requested, create a password. When asked for the password, provide the password created (for this example, using "123" as the password)e. Convert certificate to PFX format using the following command: <code>pvk2pfx.exe -pvk "TPM2VSCCert.pvk" -pi 123 -spc "TPM2VSCCert.cer" -pfx "TPM2VSCCert.pfx" -f</code>f. Import the certificate into the smart card using the following command: <code>CertUtil.exe -p 123 -csp "Microsoft* Base Smart Card Crypto Provider" -pin 12345678 -importpfx TPM2VSCCert.pfx AT_KEYEXCHANGE</code>5. Verify import was successful by examining the certificate in the VSC using the following command: <code>CertUtil.exe -scinfo -pin "12345678"</code>. Window allowing to view the certificate pops up, click OK to close6. Restart the platform, and run step 5 again, to verify certificate persists after reboot7. Remove the key from the VSC using the following commands<ol style="list-style-type: none">a. Retrieve the name of the container to use by typing: <code>CertUtil.exe -key -csp "Microsoft* Base Smart Card Crypto Provider" -pin "12345678" -v -privatekey -user</code>b. Use the container name returned in the previous command prefixed to the "[Default Container]" and replace the text in bold: <code>CertUtil.exe -delkey -csp "Microsoft* Base Smart Card Crypto Provider" -pin "12345678" -v -privatekey "TPM2VSCCert-0d6e6c94-9bd6-4640-aa-63900"</code>8. Destroy the VSC by running: <code>TpmVscMgr.exe destroy /instance ROOT\SMARTCARDREADER\0000</code>, making sure to use the correct index of the smartcard created
Test Pass/Fail Criteria:	VSC created successfully, certificate can be loaded and is persistent across reboot. VSC can be removed after key is deleted.



17.8 Microsoft* Windows* Hardware Lab Kit (HLK) TPM Testing

Test ID:	PTT_007
Test Case Title:	Microsoft* Windows* Hardware Lab Kit (HLK) TPM Testing
Mandatory/Optional:	Optional
Description:	Windows* 10 Logo requires TPM device to pass all TPM related tests in the HLK
Objective:	Ensure Intel® PTT passes all required platform HLK test for TPM device. Note: This test is not required for Intel® CSME compliance but may be required for Microsoft* logo certification. For any questions or support issues when running this test, refer Microsoft support.
Test Pass/Fail Criteria:	All HLK tests must pass. Ensure that all latest Errata filters are downloaded from the Microsoft* HLK web site. Refer the Windows* Hardware Lab Kit Step-by-Step Guide found at the link below for detailed instructions: https://msdn.microsoft.com/en-us/library/windows/hardware/dn915002(v=vs.85).aspx

17.9 Intel® PTT Disable/Enable from BIOS

Test ID:	PTT_008
Test Case Title:	Intel® PTT Disable/Enable from BIOS
Mandatory/Optional:	Optional
Description:	BIOS may implement option to disable/enable Intel® PTT, or switch between Intel® PTT and a discrete TPM 1.2
Objective:	Ensure BIOS can enable and disable Intel® PTT successfully and that BIOS clears the TPM during disable.
Procedure:	Can be run on Windows* 10 or Windows* 8.1. <ol style="list-style-type: none">1. Boot to Windows*, verify PTT_002 passing.2. Reboot, enter BIOS and disable Intel® PTT through BIOS3. Boot to Windows*, enter TPM Management Console (tpm.msc) and verify that either TPM is not available, or if TPM is available it is not Intel® PTT4. Reboot, enter BIOS and enable Intel® PTT through BIOS5. Boot to Windows*, verify PTT_002 passing Note: Intel® PTT enable/disable interface in BIOS is dependent on implementation and therefore not described
Test Pass/Fail Criteria:	When Intel® PTT is disabled; Intel® PTT does not show up in TPM management console. (It is possible for dTPM to show up pending on platform design).

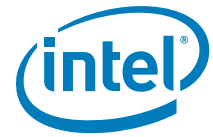


17.10 Intel® PTT and Power Flows

Test ID:	PTT_009
Test Case Title:	Power Flow Testing
Mandatory/Optional:	Mandatory
Description:	System with Intel® PTT enabled must pass all platform power flow testing. Intel® PTT must also be able to support all power flows when BitLocker is enabled and using Intel® PTT as a protector.
Objective:	Verify Intel® PTT does not interfere with system power operations.
Procedure:	<ol style="list-style-type: none">1. Perform all platform power flow tests with Intel® PTT enabled2. Encrypt the OS drive using BitLocker with TPM protection (follow instructions in PTT_004 steps 1 through 5, and wait till drive encryption reaches 10%)3. Perform the following power transitions during encryption phase and after encryption has reached 10%:<ol style="list-style-type: none">a. OS Restartb. OS Shutdown/Power upc. Hibernation/Resumed. Cold Reset (boot to internal EDK shell and type mm cf9 e -io)e. G3 (complete power off)f. Connected Standby (Windows* 8 CS)
Test Pass/Fail Criteria:	All power flow tests pass, BitLocker does not enter into recovery mode.

17.11 Dictionary Attack Lockout After Coin Battery Removal with EOM Commit

Test ID:	PTT_010
Test Case Title:	Dictionary Attack Lockout Mechanism with coin battery removal
Mandatory/Optional:	Optional for systems that do not have RPMC enabled in the image. Note: This test is not relevant to platforms that do not include a coin battery.
Description:	<p>Intel® PTT keeps monotonic counters for Dictionary Attack (DA) under RTC power well. When RTC power is lost, Intel® PTT enters lockout period to avoid Dictionary Attack for 2 hours. This is only after the coin battery has been removed 10 times and after EOM. Before that, Intel® PTT would not enter the lockout period of 2 hours.</p> <p>Note: During the 2 hour lockout period, no other Intel® PTT tests can be executed; even if correct credentials are provided. Execution of this test does not impact other non-Intel® PTT related testing.</p> <p>Note: This test can be run only once on a specific part. After this test is run, all FPF bits related to the feature is blown. With such parts, test consistently enters dictionary attack scenario after every RTC clear operation.</p>



Test ID:	PTT_010
Objective:	Allows OEM to validate the dictionary attack scenario after first coin battery removal, causing the counters to be reset.
Procedure:	<ol style="list-style-type: none"> 1. System must be after the EOM procedure, as DA lockout would not occur during manufacturing mode. 2. Set up a VSC with certificate (Instructions can be found in test PTT_006 steps 1 through 6). 3. Shutdown system, and perform RTC clear operation by removing all power and RTC battery from the board. Repeat this procedure 11 times. 4. Return RTC battery and power, boot system to Windows* 10. 5. Try to view the certificate in VSC by running: CertUtil.exe -scinfo -pin "12345678". 6. The command should fail due to Dictionary Attack lockout. 7. Wait 2 hours for lockout to pass, and try again, it should be possible to access the certificate. 8. Remove the certificate and VSC (Instruction can be found in test PTT_006 steps 8 and 9). <p>Note: At step#3, the Intel® PTT is expected to enter a lockout period to avoid Dictionary Attack for 2 hours. This period cannot be adjusted.</p>
Test Pass/Fail Criteria:	<p>Intel® PTT would not allow access to user data (VSC) during lockout period post coin battery removal</p> <p>Note: In this test Field Programmable Fuses (FPF) is blown on every battery removal and there is no recovery for it. Select few processors to be used for this test and track them.</p>

§ §



18 Intel® Virtualization Technology (Intel® VT)

Throughout this document references to Intel® VT cover both Intel® VT-x and Intel® VT-d, unless otherwise specified.

Note: Intel® VT-x refers to Intel® Virtualization Technology (Intel® VT) for IA-32, Intel® 64, and Intel® Architecture (Intel® VT-x).

Note: Intel® VT-d refers to Intel® Virtualization Technology (Intel® VT) for Directed I/O.

18.1 Introduction

18.1.1 Purpose and Scope

The purpose of this document is to provide OEMs guidance on the steps necessary to successfully validate the Intel® Virtualization Technology (Intel® VT) with Virtualization and Intel® VT-d enabled BIOS on Intel client (desktop and mobile) platforms. This document defines the purpose and value of each validation aspect in the validation process.

The intent of this document is to outline the ideal validation sequence for Intel® VT in this platform and provide an overview of the collateral that is available to provide OEMs the framework to define their own validation strategy for Intel® VT.

This document is not a technology overview and does not supplant the existing Intel® VT collateral (refer [Section 1.6: "Reference Documents"](#)). The readers are expected to be familiar with Intel® VT-x and Intel® VT-d and to use this document as a validation supplement to develop their own Intel® VT validation plan.

18.1.2 Platforms Applicable

This validation guide is applicable to the following Client platforms and their corresponding chipsets:

Table 18-1. Applicable Platforms

Platform Name
6th Generation Intel® Core™ and Intel® Core™ M Processors Platforms
Kaby lake Platform

18.1.3 Terminology

Term	Description
DMA	Direct Memory Access
GPA	Guest Physical Address



Term	Description
HPA	Host Physical Address
HVM	Hardware Virtual Machine (Virtual Machine using Intel® VT)
MMIO	Memory Mapped I/O Address Space
OS	Operating System
TXT	Trusted Execution Technology
VM	Virtual Machine
VMM	Virtual Machine Monitor

18.1.4 Prerequisites

Table 18-2. Virtualization Testing Prerequisites

Prerequisite Checklist	Document Number/Location
Client VT Info Tool	551893
Fedora Live USB Creator (Optional)	Open Source
OpenSUSE	Open Source

18.2 Test Plan and Details

Table 18-3. Intel® Virtualization Technology (Intel® VT) Test Overview

ID	Test Case Description	Tool/ Manual	Mandatory / Optional	Result
EFI Shell Environment Tests				
VT_TC01	Intel® VT Capable and Enabled as measured by Passing ALL Test Assertions	Client VT Info Tool	Mandatory	Pass
Windows* Environment Tests				
VT_TC02A	Verify Intel® VT-x with Microsoft* Client Hyper-V* Manager Boots on Windows* 8/8.1	Manual	Mandatory	Pass
VT_TC02B	Verify that the Virtual Machine Boots in Microsoft* Client Hyper-V* Manager	Manual	Mandatory	Pass
VT_TC02C	Verify that the Virtual Machine Correctly Resumes during Sleep and Hibernate Cycles on Host OS	Manual	Mandatory	Pass
Xen*/Linux* Environment Tests				
VT_TC03A	Xen* Hypervisor Boots (Xen* Environment)	Manual	Optional	Pass
VT_TC03B	Intel® VT-x and VT-d Enabled (Xen* Environment)	Manual	Optional	Pass
VT_TC03C	Intel® VT-d Functionality—Virtual Machine (VM) Boots (Xen* Environment)	Manual	Optional	Pass
VT_TC03D	Intel® VT-d Functionality—Pass Through with No VT-d Error (Xen* Environment)	Manual	Optional	Pass
VT_TC04	Intel® VT-d Functionality—IOMMU Exercise (Xen* Environment)	Manual	Optional	Pass



18.2.1 Tests in EFI Shell

18.2.1.1 Test Environment

A system under test is needed which has an Intel® VT-x and Intel® VT-d capable Processor and stable BIOS with support for VT-x and VT-d technologies. Prior to tests **enable Virtualization (or VT-x) and Intel® VT-d** in BIOS and make sure **TXT is Disabled**

Note: Disabling TXT is just for test purposes.

Tools for Testing:

- Client VT Info Tool - Get the latest version of the tool from PC Design Center VT Technology page or using Document #551893.

18.2.1.2 Verify Processor is Intel® VT Capable and Enabled

Test ID:	VT_TC01
Test Case Title:	Intel® VT Capable and Enabled as measured by Passing ALL Test Assertions
Mandatory/Optional:	Mandatory
Description:	This test checks that the Processor has VT-x/VT-d capability, that VT-x/VT-d are enabled correctly in BIOS.
Objective:	Verify Processor and BIOS is Intel® VT-x/VT-d Capable and Enabled
Procedure:	<ol style="list-style-type: none">1. Enable Intel® Virtualization Technology (VT-x) and Intel® VT-d in BIOSNote: Make Sure TXT is disabled (for test purposes only).2. Download Client VT Info Tool #551893 and save to a EFI bootable USB drive.3. Unzip the Client VT Info Tool in the USB drive.4. Boot to EFI Shell (Called Internal EDK Shell for Intel Reference BIOS).5. Move to Folder with unzipped Client VT Info tool using cd [folder_name]6. Run ALL Test Assertions using Client VT Info tool by entering vtinfo -t or vtinfo_vxx.xx.xx -t where xx.xx.xx is the version number7. Record score. (Make a note of how many tests PASS and how many FAIL.) Refer example outputs below in section Section 18.2.1.2.1: "Sample Output for Client VT Info Tool Results—Passing All Tests", Section 18.2.1.2.2: "Sample Output for Client VT Info Tool Results—Failing Some Tests", and Section 18.2.1.2.3: "Sample Output for Client VT Info Tool Results—Obtaining Test Result Details". <p>Note: For additional information on VT Status, use vtinfo -h to display other command line options.</p>
Test Pass/Fail Criteria:	Test passes when: <ol style="list-style-type: none">1. Tool returns VT Test Status: PASS.2. No Errors are reported in test results.

18.2.1.2.1 Sample Output for Client VT Info Tool Results—Passing All Tests

This example was generated using the -t option with Client VT Info Tool:

```
*****
VtInfo vXX.XX.XX
Built: XXX X 2014 XX:XX:XX
Intel Corporation
Copyright (c) 2014
*****
```

```
-----
VT Test Status: PASS
-----
```




```
-----
Pass | 52
Fail | 00
Warn | 00
NA   | 05
Total | 57
-----
```

Note: Tests which do not apply to the system under test would not be shown in results.

18.2.1.2.2 Sample Output for Client VT Info Tool Results—Failing Some Tests

This example was generated using the -t option with Client VT Info Tool:

```
*****
VtInfo vXX.XX.XX
Built: XXX X 2014 XX:XX:XX
Intel Corporation
Copyright (c) 2014
*****
```

VT Test Status: FAIL

```
-----
Pass | 50
Fail | 02
Warn | 00
NA   | 05
Total | 57
-----
```

Errors:

40) Verify 4k granularity of RMRR regions.
-- RMRR Base Address(0xAD800000) Limit Address(0xFFFFFFFF) is not marked as reserved in system memory map.

62) VTd Support for Large Pages (2MB and 1GB) on DEFAULT and GFX VTd Unit.
-- Remapping Engine 0xFED91000 Capability Register BIT56 must be set.

Note: Tests which do not apply to the system under test would not be shown in results.

18.2.1.2.3 Sample Output for Client VT Info Tool Results—Obtaining Test Result Details

This example was generated using the -v -t options with Client VT Info Tool:

```
...
-----
Platform Information
-----
CPUID1.EAX      0x000306D3
CPUID1.EBX      0x00100800
CPUID1.ECX      0x77FAFBFF
[6] SMX        1
[5] VMX        1
CPUID1.EDX      0xBFEBFBFF
IA32_FEATURE_CONTROL 0x000000000000FF07
[2] En VMX outside SMX 1
[1] En VMX inside SMX 1
[0] Lock bit    1
...
-----
```

Test Assertions

01) Check DMAR table presence.
Result: PASS
...

61) Each ACPI device number in ANDD structure must have a corresponding enumeration ID in Device Scope.
Result: PASS

62) VTd Support for Large Pages (2MB and 1GB) on DEFAULT and GFX VTd Unit.
Result: FAIL
: Remapping Engine 0xFED91000 Capability Register BIT56 must be set.

63) Graphics VTd Unit Support for SVM (Shared Virtual Memory).
Result: PASS
...

**VT Test Status: FAIL**

Pass | 50
Fail | 02
Warn | 00
NA | 05
Total | 57

Errors:

40) Verify 4k granularity of RMRR regions.
-- RMRR Base Address(0xAD800000) Limit Address(0xAFFFFFFF) is not marked as reserved in system memory map.

62) VTd Support for Large Pages (2MB and 1GB) on DEFAULT and GFX VTd Unit.
-- Remapping Engine 0xFED91000 Capability Register BIT56 must be set.

Note: Tests which do not apply to the system under test would not be shown in results.

18.2.2 Intel® VT-x Tests with Microsoft* Client Hyper-V* on Windows* 8/8.1

18.2.2.1 Test Environment

A system under test is needed which has an Intel® VT-x and Intel® VT-d capable Processor and stable BIOS with support for VT-x and VT-d technologies. Prior to tests **enable Virtualization (or VT-x)** and **Intel® VT-d** in BIOS and make sure **TXT is Disabled**.

Note: Disabling TXT is just for test purposes.

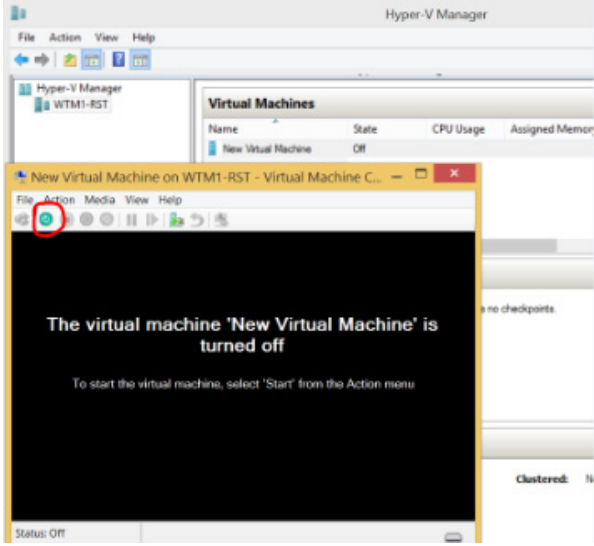
Tools for Testing:

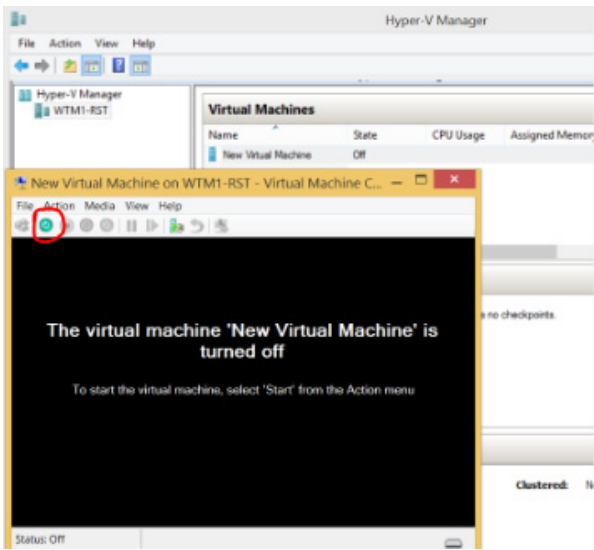
— **Microsoft* Windows* 8/8.1 or higher**

Test ID:	VT_TC02A
Test Case Title:	Verify Microsoft* Client Hyper-V* Manager Boots
Mandatory/Optional:	Mandatory
Description:	Microsoft* Client Hyper-V* uses Intel® VT to create a Hypervisor based on Windows* 8/8.1.
Objective:	Verify Intel® VT-x implementation at platform level
Procedure:	1. Enable Intel® Virtualization Technology (VT-x) in BIOS. 2. Boot to Windows* 8/8.1 and open Client Hyper-V* Manager. Note: Refer Section : "Microsoft* Client Hyper-V* and Virtual Machine Enabling and Installation Instructions" for instructions on how to enable Client Hyper-V*.
Test Pass/Fail Criteria:	Test passes when: Microsoft* Client Hyper-V* Manager Boots

Test ID:	VT_TC02B
Test Case Title:	Verify Virtual Machine Boots in Microsoft* Client Hyper-V* Manager
Mandatory/Optional:	Mandatory
Description:	Microsoft* Client Hyper-V* uses Intel® VT to launch a virtual guest OS in Windows* 8/8.1 host OS.



Test ID:	VT_TC02B
Objective:	Verify Intel® VT-x implementation at platform level
Procedure:	<ol style="list-style-type: none"> 1. Enable Intel® Virtualization Technology (VT-x) in BIOS. 2. Boot to Windows* 8/8.1 and open Client Hyper-V* Manager. 3. Open virtual machine by double clicking on it. If it is not running, user can click on the start button.  <p>Note: Refer Section 18.2.2.1.2: "How to Create a New Virtual Machine in Client Hyper-V" for instructions on how to enable Microsoft* Client Hyper-V*.</p>
Test Pass/Fail Criteria:	Test passes when: Virtual Machine Guest boots within Client Hyper-V* (when Intel® VT is enabled in BIOS).

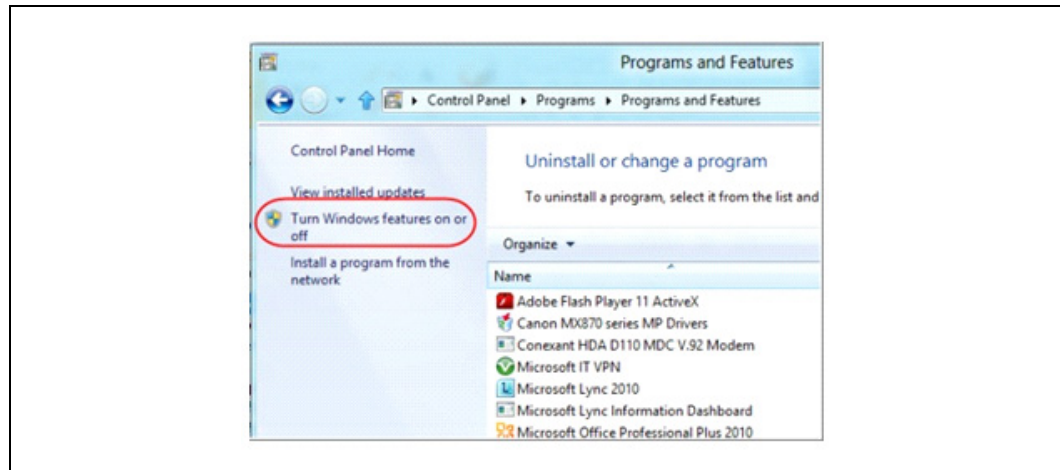
Test ID:	VT_TC02C
Test Case Title:	Verify Virtual Machine Correctly Resumes during Sleep and Hibernate Cycles on Host OS.
Mandatory/Optional:	Mandatory
Description:	While performing Sleep and Hibernate cycles on the Host Machine, the Virtual Machine should correctly resume and remain stable.
Objective:	Verify Intel® VT-x implementation at platform level.
Procedure:	<ol style="list-style-type: none"> 1. Enable Intel® Virtualization Technology (VT-x) in BIOS. 2. Boot to Windows* 8/8.1 and open Client Hyper-V* Manager. 3. Open virtual machine by double clicking on it. If it is not running, you can click on the start button.  <p>Note: If user are running Client Hyper-V* on a laptop and close the lid, the VMs that are running is put into a saved state, and can be resumed when the machine wakes, as long as lid close action is set to sleep or hibernate.</p> <ol style="list-style-type: none"> 4. While Virtual Machine is running, put the system (from Windows* 8/8.1 Host OS) to Sleep mode and then bring it back out of sleep. Check that Virtual machine is still alive and working. Repeat 3-5 cycles. 5. While Virtual Machine is running, put the system (from Windows* 8/8.1 Host OS) to Hibernate and then bring it back out of hibernate. Check that Virtual machine is still alive and working. Repeat 3-5 cycles.
Test Pass/Fail Criteria:	Test passes when: A. Virtual machine is alive and working <i>after system Sleep cycle</i> . B. Virtual machine is alive and working <i>after Hibernate cycle</i> .

Microsoft* Client Hyper-V* and Virtual Machine Enabling and Installation Instructions

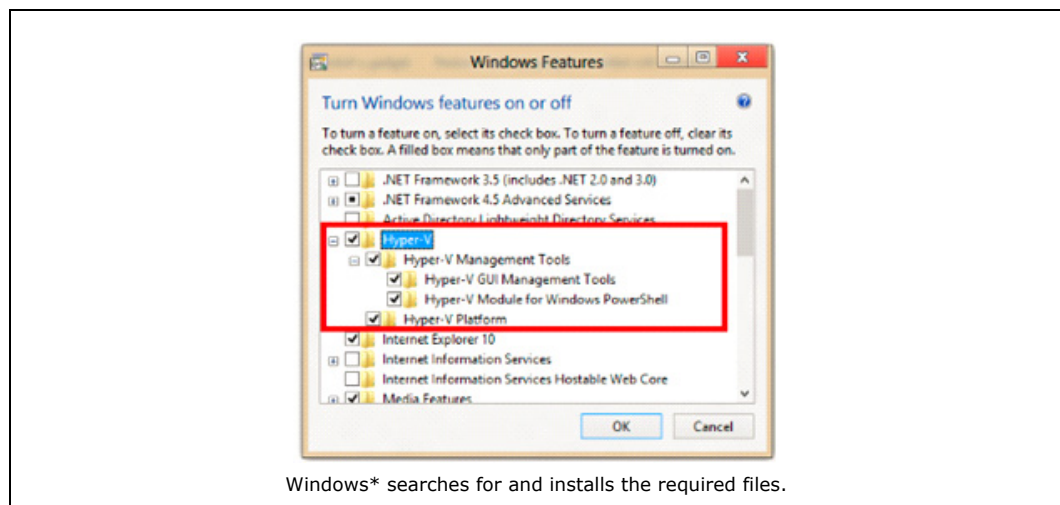
18.2.2.1.1 How to Enable Microsoft* Client Hyper-V*

1. In the Windows* 8/8.1 Control Panel, tap or click Programs, and then tap or click **Programs and Features**.

2. Tap or click **Turn Windows* features on or off**.



3. In the **Windows* Features** dialog box, select the check-boxes for **Hyper-V*** options and then click **OK**.



4. Restart after Enabling or Disabling Microsoft* Client Hyper-V*.

Note:

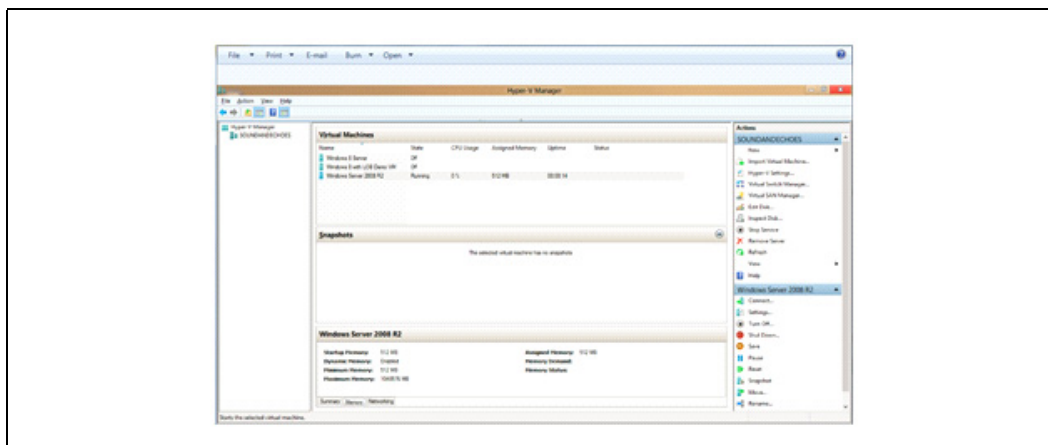
Enabling Client Hyper-V* installs Hyper-V* Manager. User uses Hyper-V* Manager to create and manage virtual machines.

For more information on the Hyper-V* Manager user interface, go to <http://technet.microsoft.com/library/cc770494.aspx>.

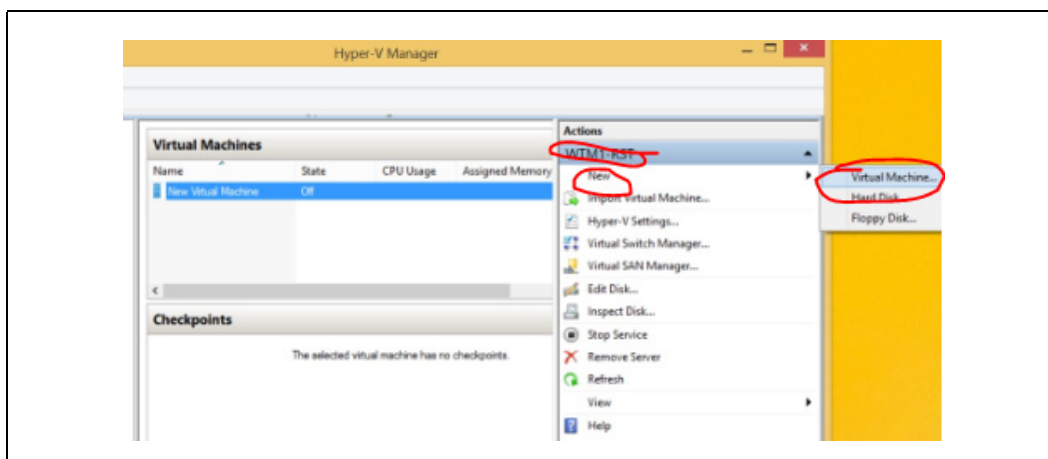
18.2.2.1.2 How to Create a New Virtual Machine in Client Hyper-V*

Skip this page if you already have a Virtual Machine in Client Hyper-V* Manager.

1. Open Hyper-V* Manager from Windows* Start screen (In Windows* 8.1 you may need to go to Start screen > Click arrow at bottom left > Hyper-V Management tools > Hyper-V Manager.)

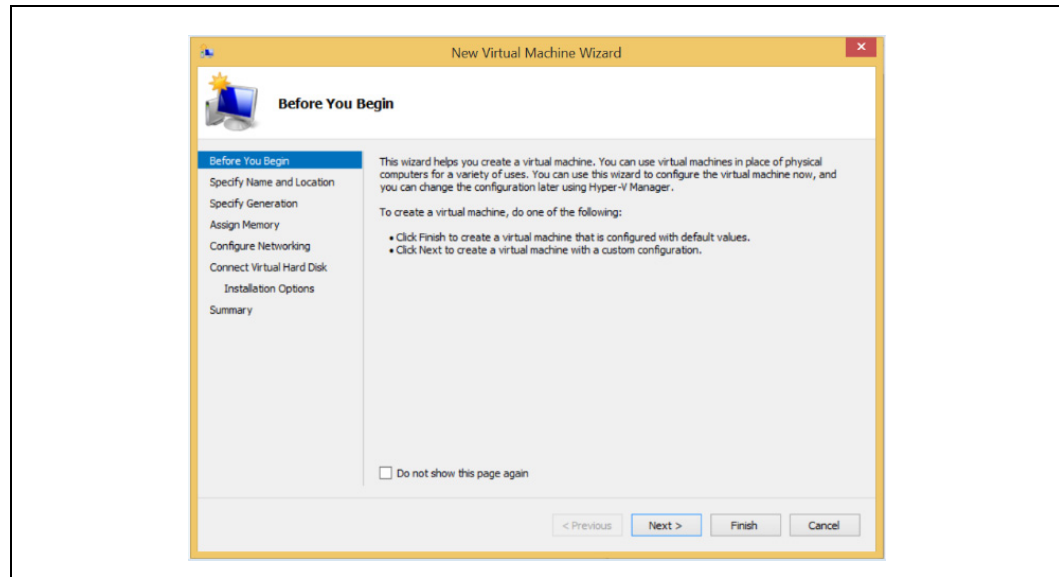


2. From the navigation pane of Hyper-V* Manager, select the computer name.
3. From the **Action** pane on the right side, click **New**, and then click **Virtual Machine**.The New Virtual.

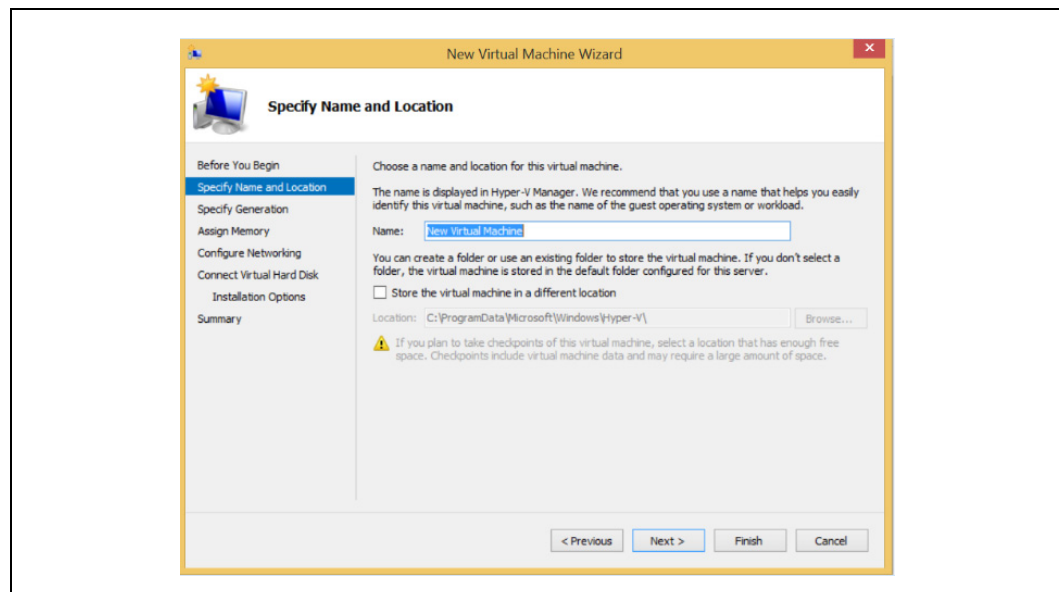




4. Machine wizard opens. Click **Next**.

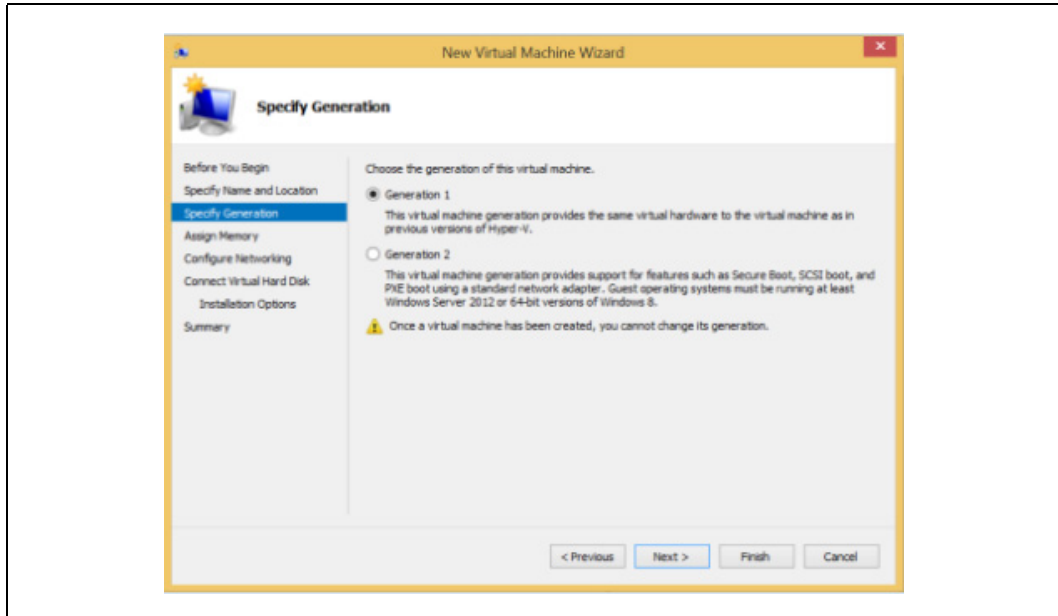


5. On the **Specify Name and Location** page, type any name.

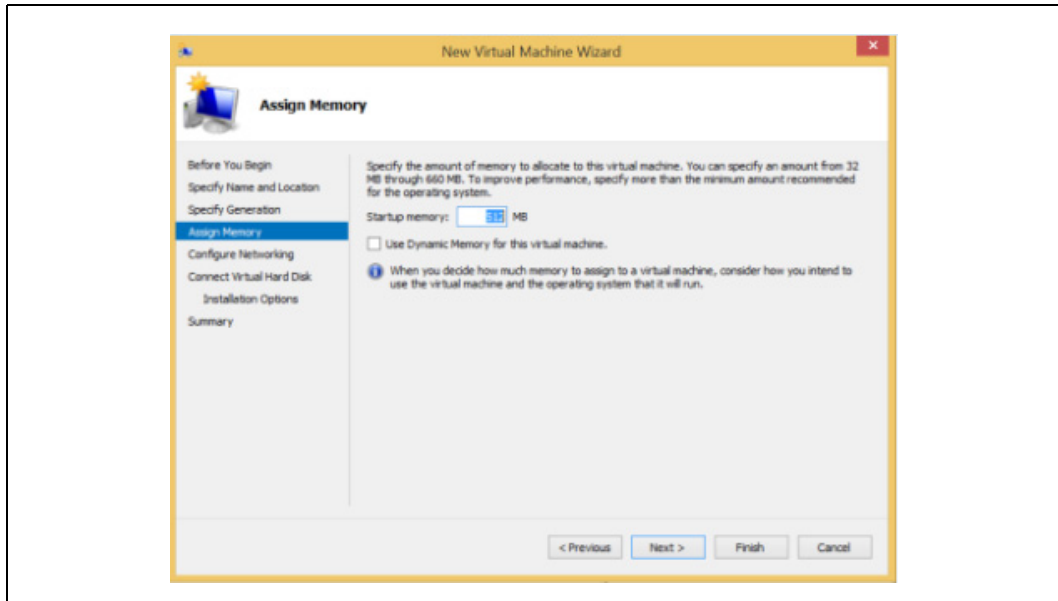


6. On the **Specify Generation** page, leave the default, Generation 1.

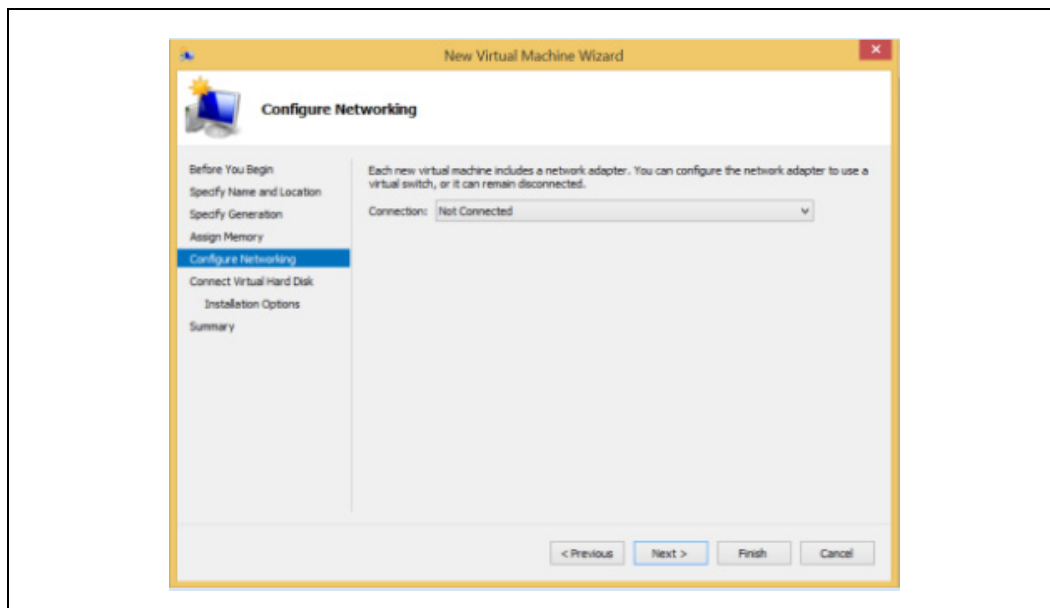
Note: Earlier versions of Client Hyper-V* may not have this step.



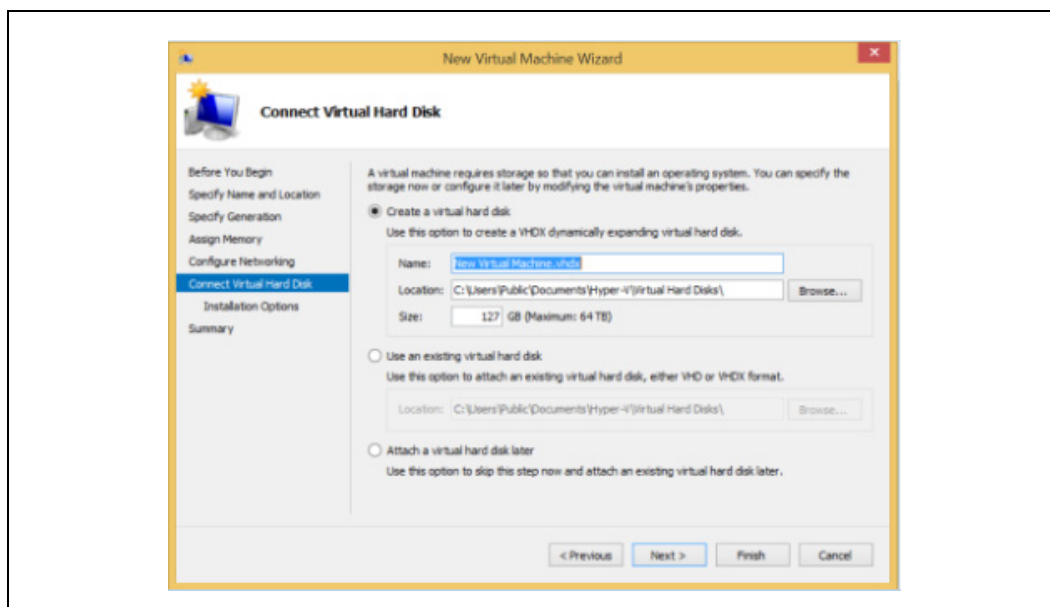
7. On the **Assign Memory** page, specify enough memory to start the guest operating system.

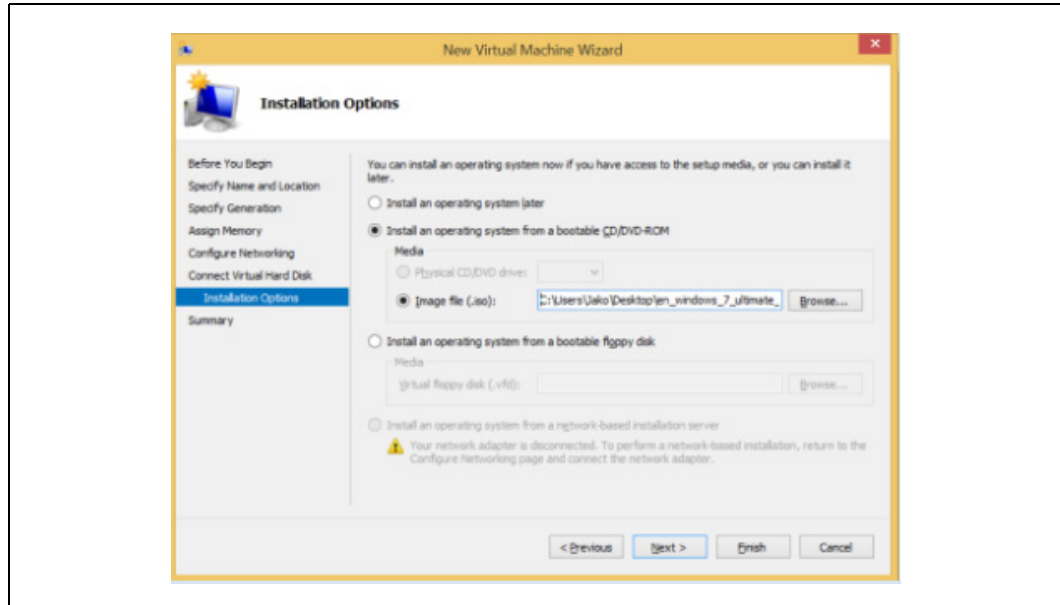


8. On the **Configure Networking** page, leave the default settings.



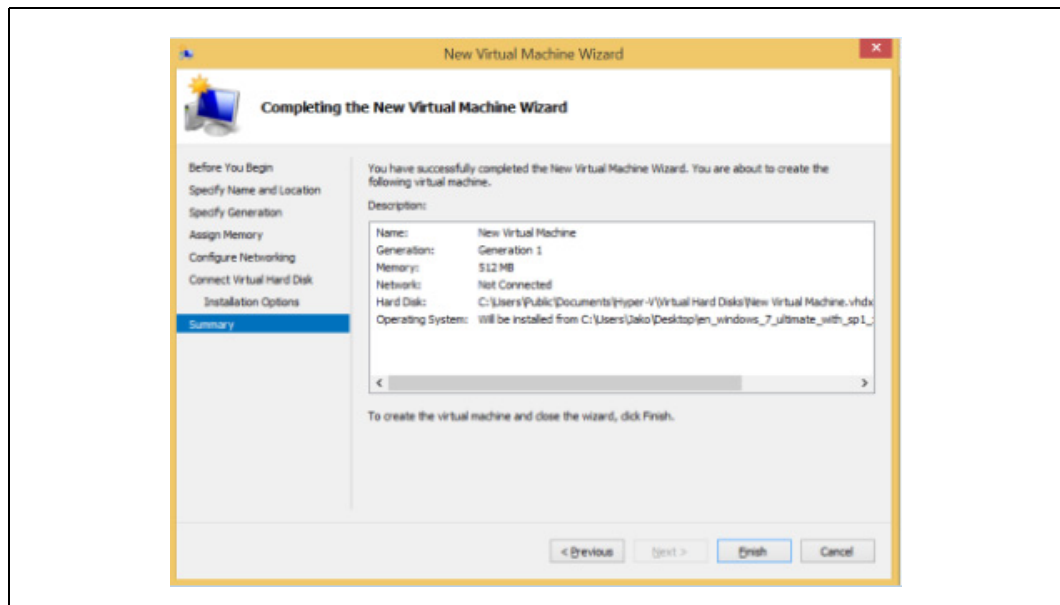
On the **Connect Virtual Hard Disk** and **Installation Options** pages, choose the option that is appropriate for how you plan to install the guest operating system: If user installs the guest operating system from a DVD or an image file (an.ISO file), choose **Create a virtual hard disk**. Click **Next**, and then click the option that describes the type of media which user use. For example, to use an.iso file, click **Install an operating system from a boot CD/DVD** and then specify the path to the.iso file. **(This is recommended)**.



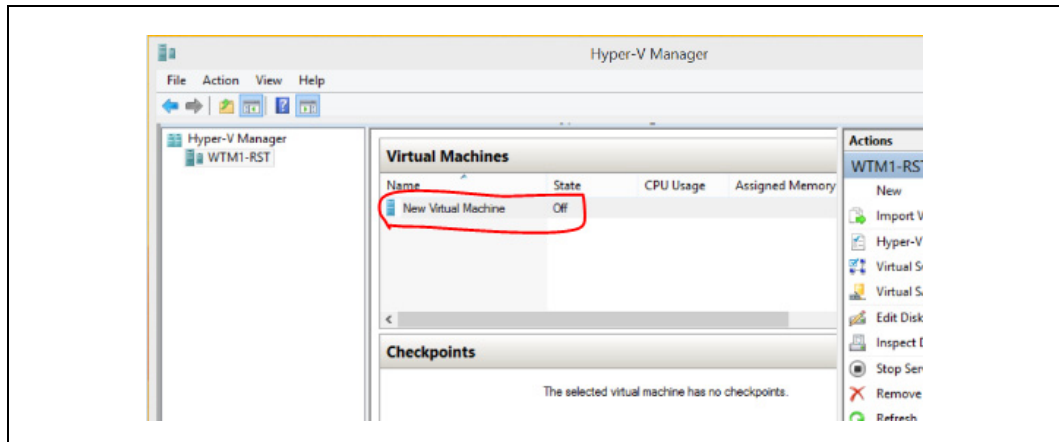


- g. If the guest operating system is already installed in a virtual hard disk, choose **Use an existing virtual hard disk** and click **Next**. (Refer figure at top of page). Then, choose **Install an operating system later**.

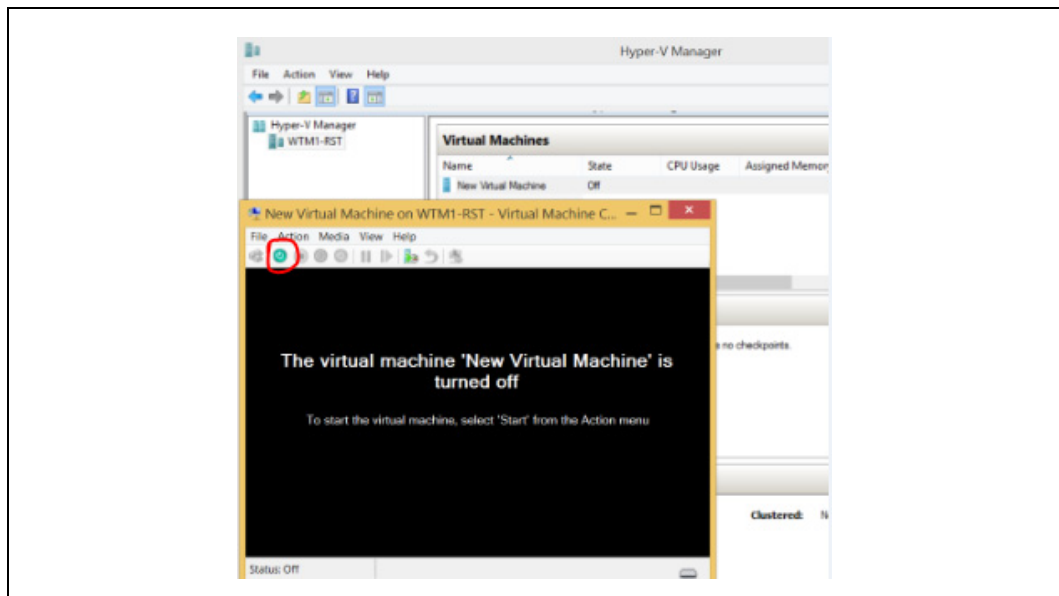
9. On the **Summary** page, verify selections and then click **Finish**.



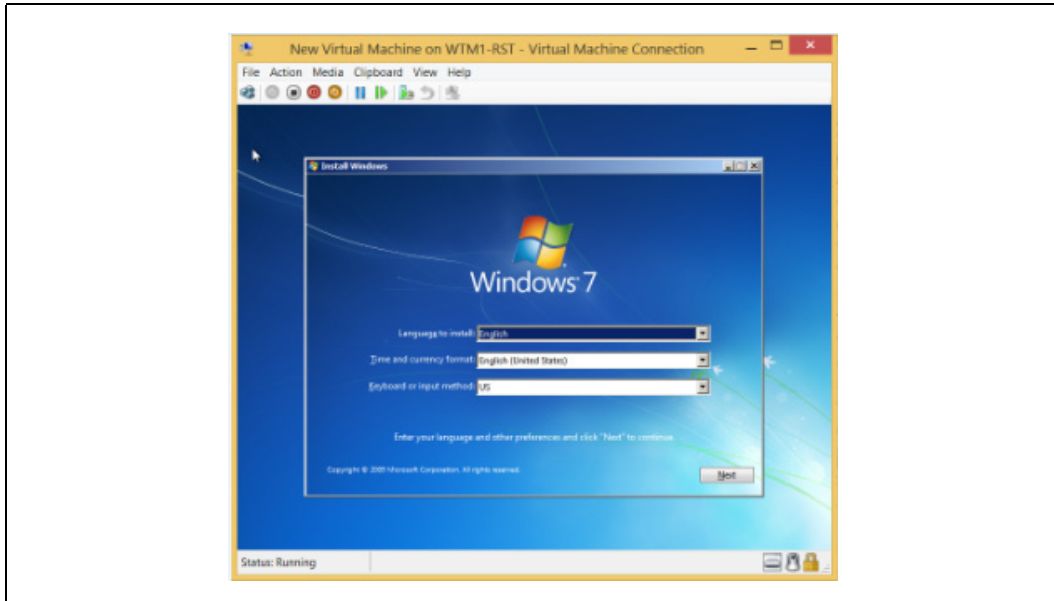
10. **Double Click** on the **Virtual Machine** to Open it.



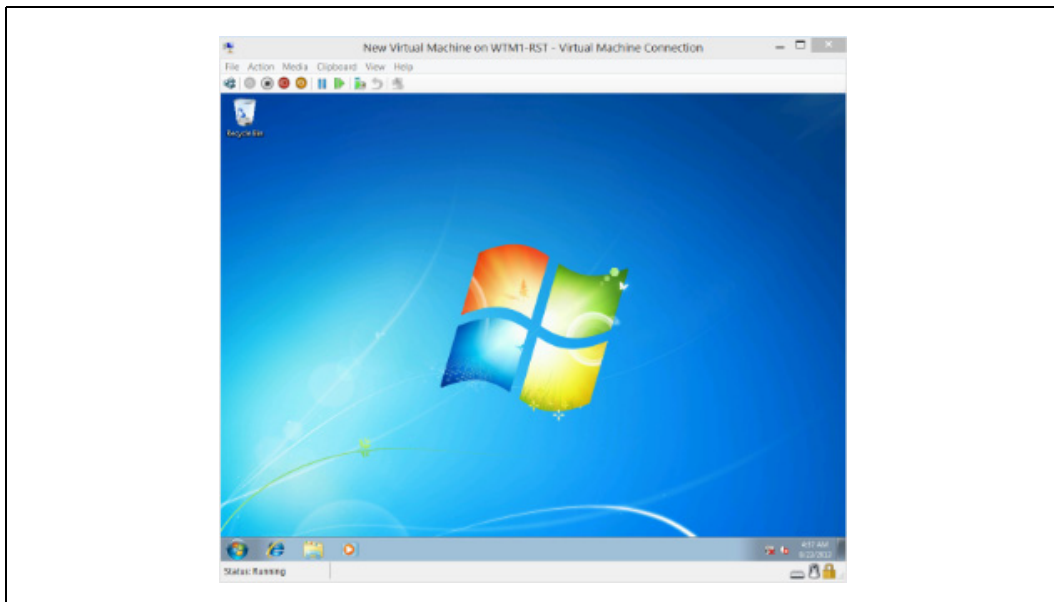
11. Click on the green **Start** button to run Virtual Machine



12. **Follow** normal OS Installation Instructions, this depends on OS you have chosen.



13. Once this is complete the Virtual Machine looks like a normal System inside the Virtual Machine Window.





18.2.3 Intel® VT Tests in Xen*/Linux* Environment

Test Environment:

A system under test is needed which has an Intel® VT-x and Intel® VT-d capable Processor, a stable BIOS with support for VT-x and VT-d technologies. Prior to tests **enable Virtualization (or VT-x)** and **VT-d** in BIOS and make sure **TXT is Disabled**.

Tools for Testing:

- Open source openSUSE* 12.2 or Open source Fedora* 17
- Xen* open source VMM

18.2.3.1 Verify System Under Test (SUT) Boots Xen* Mode/VMM

Test ID:	VT_TC03A
Test Case Title:	Xen* Hypervisor Boots (Xen* Environment)
Mandatory/Optional:	Optional
Description:	Ensures that Test cases VT_TC13, VT_TC14 and VT_TC15 can be executed.
Objective:	Verify platform can boot to Xen* Hypervisor/VMM
Preparation:	<ol style="list-style-type: none"> 1. Install Xen* OS (for example openSUSE* 12.2 or Fedora* 17 or equivalent). 2. Enable Intel® Virtualization Technology (VT-x) and VT-d in BIOS. 3. Build/Install Xen* VMM. <p>Installation steps are explained in Section .</p>
Procedure:	<ol style="list-style-type: none"> 1. Boot to Xen* drive. 2. Choose Xen* Hypervisor option. 3. When system boots, login as root. 4. To login as root: Change user to root and use password: linux123 5. Enter "xl info" into terminal. Result should give Xen version number and no error message.
Test Pass/Fail Criteria:	Test passes when the following occurs: System successfully boots to Xen* Hypervisor with no error messages.



18.2.3.2 Verify Intel® VT-x and VT-d Enabled (Xen* Mode)

Test ID:	VT_TC03B
Test Case Title:	Intel® VT-x and VT-d Enabled (Xen* Environment)
Mandatory/ Optional:	Optional
Description:	Ensures that VT-d is enabled and supported. This test is in Xen* Hypervisor.
Objective:	Verify Intel® VT Functionality is enabled on the SUT.
Preparation:	Install Xen* OS (for example openSUSE* 12.2 of Fedora* 17) Download and build/Install Xen*. Installation steps are explained in Section .
Procedure:	<ol style="list-style-type: none">1. Boot to Xen* Mode.2. Open terminal.3. Enter xl dmesg grep -i Virt <i>This should yield:</i> <i>(XEN) I/O virtualisation enabled</i>4. Enter xl dmesg grep -i VT <i>This should yield:</i> <i>(XEN) Intel VT-d iommu 0 supported page sizes: 4kB, 2MB, 1GB.</i> <i>(XEN) Intel VT-d iommu 1 supported page sizes: 4kB, 2MB, 1GB.</i> <i>(XEN) Intel VT-d Snoop Control not enabled.</i> <i>(XEN) Intel VT-d Dom0 DMA Passthrough not enabled.</i> <i>(XEN) Intel VT-d Queued Invalidation enabled.</i> <i>(XEN) Intel VT-d Interrupt Remapping enabled.</i> <i>(XEN) Intel VT-d Shared EPT tables enabled.</i> <p>Note: "dmesg" is Xen* command, run from a terminal. Depending on the version of Xen kernel, "xl" might be replaced with "xl -f" or "xm"</p>
Test Pass/Fail Criteria:	<p>Test passes when all the following occur:</p> <ol style="list-style-type: none">1. "xl dmesg grep -i virtual" results in: <i>(XEN) I/O virtualisation</i>2. "xl dmesg grep -i VT" results in: <i>(XEN) Intel VT-d iommu 0 supported page sizes: 4kB, 2MB, 1GB.</i> <i>(XEN) Intel VT-d iommu 1 supported page sizes: 4kB, 2MB, 1GB.</i> <i>(XEN) Intel VT-d Snoop Control not enabled.</i> <i>(XEN) Intel VT-d Dom0 DMA Passthrough not enabled.</i> <i>(XEN) Intel VT-d Queued Invalidation enabled.</i> <i>(XEN) Intel VT-d Interrupt Remapping enabled.</i> <i>(XEN) Intel VT-d Shared EPT tables enabled.</i> <p>Note: There may be additional results too; if above results are shown on test system, this test is passing.</p>



18.2.3.3 Verify Intel® VT-d Functionality VM Boots (Xen* Mode)

Test ID:	VT_TC03C
Test Case Title:	Intel® VT-d Functionality - Virtual Machine (VM) Boots (Xen* Environment)
Mandatory/Optional	Optional
Description:	Verifies VT_TC14 can be executed.
Objective:	Verify Intel® VT implementation at platform level.
Preparation:	<p>Enable Intel® Virtualization Technology (VT-x) and VT-d in BIOS:</p> <ol style="list-style-type: none"> 1. Install Xen* OS (for example openSUSE* 12.2 or Fedora* 17). 2. Install/Build Xen* VMM onto Xen* OS. <p>Instructions are explained in Section .</p>
Procedure:	<ol style="list-style-type: none"> 1. Boot to Xen* Hypervisor Mode. 2. Open Virtual Machine Manager. 3. Create a Virtual Machine. Instructions are explained in Section 18.2.5.3: "Creating Virtual Machine on OpenSUSE* 12.2". 4. Launch Hardware Virtual Machine (HVM) for example Windows* XP, Windows* 7 or other OS as a Virtual Machine. 5. Verify that no VT faults are reported using dmesg grep -i VT
Test Pass/Fail Criteria:	<p>Test passes when all the following occur:</p> <ol style="list-style-type: none"> 1. A Virtual Machine (VM) is open and working. 2. Verify that no VT faults are reported in serial log messages and "dmesg" log. <p>Note: "dmesg" is Xen* command, run from a terminal. You may need to use xm dmesg (prior to Xen* 4.1.0) or xl dmesg (if you are using Xen* 4.1.0 and later).</p>



18.2.3.4 Verify Intel® VT-d Functionality Pass Through (Xen* Mode)

Test ID:	VT_TC03D
Test Case Title:	Intel® VT-d Functionality—Pass through with No VT-d Error (Xen* Environment)
Mandatory/Optional:	Optional
Description:	<p>Verifies Intel® VT-d Functionality by Assigning Devices to Guest OS and checking for errors by output log messages.</p> <ul style="list-style-type: none">Validates Intel® VT BIOS implementation by using Intel® VT hardware as exposed by BIOS through ACPI table.Creates Address translation tables as per Intel® VT Specification.Exercises Intel® VT-d functionality by assigning devices to guest OS – outputs log messages.Outputs debug messages on serial port. (Intel® VT messages have a keyword "Intel VT" or "Intel VT-d" on the lines).
Objective:	Verify Intel® VT implementation at platform level.
Preparation:	Required to test VT_TC13.
Procedure:	<p>If you already have an open Virtual Machine, you can skip to step 3.</p> <ol style="list-style-type: none">Boot to Xen* Hypervisor (with Intel® VT and Intel® VT-d enabled in BIOS setup options).Launch Hardware Virtual Machine (HVM) for example Windows* XP or Windows* 7.Directly assign one or more I/O devices to guest HVM, for example Ethernet Controller, Integrated Network device, Audio, Firewire, USB controller and so forth. Refer Section 18.2.5.4: "Testing Intel® VT Using Xen* VMM in openSUSE* 12.2" for instructions.Verify that no VT faults are reported in serial log messages.Verify that no VT faults are reported using dmesg grep -i VT
Test Pass/Fail Criteria:	<p>Test passes when all the following occur:</p> <ol style="list-style-type: none">Directly assign one or more I/O devices to guest HVM, for example Integrated Network device, Audio, Firewire, USB controller and so forth.Verify that directly assigned I/O device is visible only in HVMVerify that no VT faults are reported in serial log messages and "dmesg" log <p>Note: "dmesg" is Xen* command, run from a terminal. You may need to use xm dmesg (prior to Xen* 4.1.0) or xl dmesg (if you are using Xen* 4.1.0 and later).</p>



18.2.3.5 Verify Intel® VT-d Functionality Through IOMMU Exercise

Test ID:	VT_TC04
Test Case Title:	Intel® VT-d Functionality - IOMMU Exercise (Xen* Environment)
Mandatory/Optional:	Optional
Description:	Runs in Xen* Environment. Enable Intel® Virtualization Technology (VT-x) and VT-d in BIOS. Dynamically creates Intel® VT-d address translation tables by running concurrent workloads on integrated I/O devices like graphics, network device, HD audio, FireWire or USB device. Since Xen* IOMMU does page invalidation on each I/O transaction, it stresses the Intel® VT-d at system level in a unique way.
Objective:	Verify Intel® VT-d functionality through the IOMMU driver.
Preparation:	Install openSUSE* 12.2. The latest stable Xen* includes Intel® VT-d IOMMU driver. Xen* installation steps are explained in Section .
Procedure:	<ol style="list-style-type: none"> 1. Boot openSUSE* Xen* with Intel® Virtualization Technology (VT-x) and VT-d enabled in BIOS. 2. Run concurrent workloads like TTCP or disk copy, while playing audio to stress these I/O devices, and/or playing video clips from internet (for example YouTube* and so forth) at same time. 3. Check for error messages. IOMMU driver forwards faults in the DMESG log or the RS232 port.
Test Pass/Fail Criteria:	Test passes when IOMMU messages appear in DMESG log or on RS232 port, and no VT-d faults are reported in DMESG log or serial port log. Note: "dmesg" is Xen* command, run from a terminal. You may need to use xm dmesg (prior to Xen* 4.1.0) or xl dmesg (if you are using Xen* 4.1.0 and later).

Installing and Using Linux* (openSUSE* 12.2, Fedora* 17) and Xen* VMM for Intel® VT Testing

18.2.4 Platform Setup Requirements

The system/platform on which the Linux*/Xen* is to be installed is System Under Test (SUT). The following are the SUT setup requirements:

System needs to be stable and booting to DOS/Windows* OS

- Add Intel® PRO100 Network PCI card. This is needed as Linux*/Xen* installation requires a working network connection. If the system is based on Intel® 5 Series Express Chipsets or previous generation chipsets, the onboard wired network is sufficient.
- Add DVD ROM drive for booting Linux* from CD or DVD.
- BIOS setup options:
 - **Optional: Disable** "Intel Virtualization Technology" and "Intel® VT-d" in BIOS setup options (prior to OS installation, then **Enable after installation** is complete).
 - Set SATA disk drive mode to **AHCI mode**.

18.2.5 Using openSUSE* 12.2 (64-Bit)

For a video on [openSUSE* 11.3 Xen Hypervisor Installation](#), refer the Videos Section on Broadwell Platform PCDC VT page.



Note: openSUSE* 11.3 installation is very similar to openSUSE* 12.2 installation.

18.2.5.1 Standard Linux* Installation for openSUSE* 12.2

View instructions below or refer [openSUSE* Installation Instructions](#). Be sure to also follow **step 8** below:

1. Download openSUSE* 12.2 (64-bit) and burn it on a DVD. Examples and references used in this procedure are based on installing openSUSE* 12.2 on an Intel CRB.
2. After booting the openSUSE* DVD, choose Installation.
3. Select Language and Keyboard Layout. Click Next.
4. Choose New Installation. Click Next.
5. Choose region and Time Zone. Click Next.
6. Select preferred desktop environment. Click Next.
7. Choose Partition based or LVM based. Click Next.
8. Enter Username and Password. Click Next. **(Un-check the option to automatically sign in, during installation).**
9. Review settings, modify any if necessary, and Click Install.
10. After Installation the configuration automatically be created.

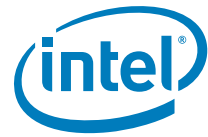
18.2.5.2 Xen* Hypervisor Installation on openSUSE* 12.2

1. Choose the default option on boot options menu, and log in using root as the username.
2. Ensure openSUSE* 12.2 installation disk is loaded.
3. In the Applications Menu go to System > Install Hypervisor and Tools (Or search for YaST2).
4. Choose Xen* and Accept.
5. When asked to configure a default network bridge, choose Yes.
6. Reboot Machine.
7. To verify if Xen* Hypervisor is installed:
 - a. Boot up machine.
 - b. Choose Xen* – openSUSE* 12.2.
 - c. Log in as root user.
 - d. Open terminal and type **uname -r**
 - e. You should refer “xen” along with the kernel version number.

18.2.5.2.1 What to do if Xen Hypervisor Option Does Not Show Up

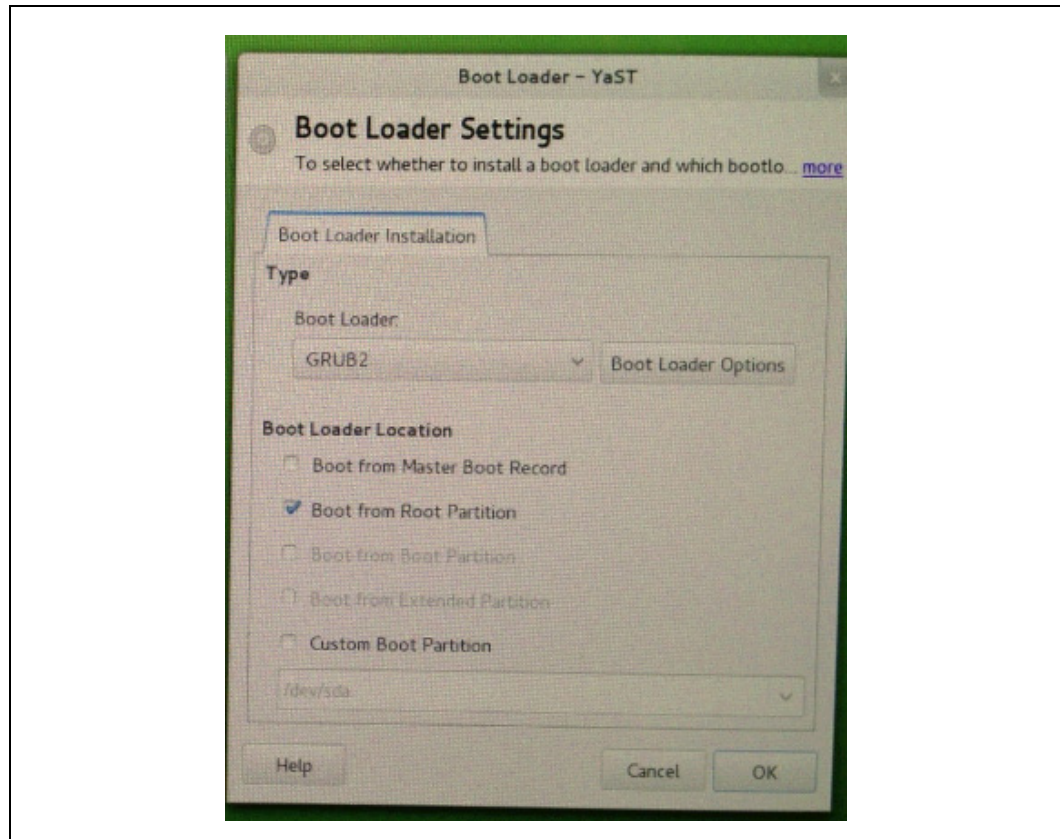
After Xen Installation, if Xen Hypervisor does not show up in the boot loader menu, you may need to change its boot loader configuration file after Xen Installation:

1. Reboot the system after installation.
2. Use Desktop boot option (the first option).
3. Find the Yast Boot Loader Settings: **Computer > Yast > System > Boot Loader** or **Administrator Settings > Boot Loader**



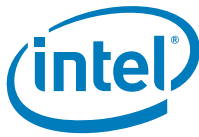
4. Enter Boot loader type: **GRUB2**. Choose **Boot from Root Partition**. Click Ok.
5. After a reboot, user able to refer the hypervisor in the boot loader menu.

Figure 18-1. Boot Loader Settings



18.2.5.3 Creating Virtual Machine on OpenSUSE* 12.2

1. Choose Xen* Hypervisor boot option and log in using root as username.
2. In Applications Menu go to System > Virtualization > Create Virtual Machines.
3. Click Forward.
4. Insert Guest OS Installation disk.
5. Choose I need to install an operating system. Click Forward.
6. Choose Guest OS user would like to use and click Forward.
7. Review Summary of Virtual Machine.
 - a. You may want to change the Name of Virtual Machine. Click Apply.
 - b. Also in Hardware section, ensure that you have at least 1024MB of Initial Memory and Maximum Memory. Click Apply.
 - c. In Disks option, add CD-ROM by clicking on CD-ROM and Move CD-ROM to the top option using the arrows. Click Apply.



- d. In Network Adapters delete any default adapters. Click Apply.
- e. Then click OK.
- f. Follow the on screen instructions for installing the Guest OS in the Virtual Machine.

18.2.5.4 Testing Intel® VT Using Xen* VMM in openSUSE* 12.2

The Intel® VT can be tested by assigning PCIe* I/O device(s) to the guest OS. When Intel® VT-d is used to directly assign an I/O device to a guest, the guest OS has direct access to I/O device hardware and guest VM owns the physical driver for that I/O device.

The test is considered to be passing when all of the following occur:

1. An I/O device can be successfully assigned to guest VM ([Section 18.2.5.4.1](#)).
2. Xen* VMM does not report any VT faults. Xen* VMM reports no VT faults in “dmesg” log. User need to search for VT faults by executing the following and search for VT messages:

```
dmesg | grep -i fault
--OR--
xm dmesg | grep -i fault (if using Xen earlier than 4.1)
--OR--
xl dmesg | grep -i fault (if using Xen 4.1.0 or later)
```

3. Guest VM detects the presence of new hardware. (In a Windows* OS, this can be determined through the VM device manager).
4. If the physical driver for the newly assigned I/O device is present in the guest OS, check that the device is functional.

18.2.5.4.1 Assigning an I/O Device Using PCISTUB Method

1. First obtain the Bus, Device, Function (BDF) ID of the device using:

```
lspci --OR-- lspci | grep -i Ethernet
```

Example result:

```
...
00:19.0 Ethernet controller: Intel Corporation 82566DM Giga-
bit Net...
...
BDF = "00:19.0"
```

2. Enter the following, in order to unbind and attach the device:

- a. `echo -n 0000:00:19.0 > /sys/bus/pci/devices/0000:00:19.0/driver/unbind`
- b. `echo 0000:00:19.0 > /sys/bus/pci/devices/0000:00:19.0/driver/unbind`
- c. `echo 0000:00:19.0 > /sys/bus/pci/drivers/pciback/new_slot`
- d. `echo 0000:00:19.0 > /sys/bus/pci/drivers/pciback/bind`
- e. **`ls -l /sys/bus/pci/devices/0000:00:19.0/driver`**
this verifies the binding
- f. `xl pci-attach Guest 0:0:19.0`
where *Guest* is the name of virtual machine

Note: In Xen* 4.1 or earlier, use “xm” instead of “xl”



To find version of Xen* you are using, use **xl info** or **xm info** command.

18.2.5.5 Special Instructions to Obtain Serial Log on openSUSE* 12.2

User needs to modify the serial device parameters in the grub file, in order to receive kernel information on a serial port.

1. Open /boot/grub/menu.lst
2. Add the changes highlighted in red below:

Original

```
title Desktop -- openSUSE 12.2 - 2.6.37.1-1.2.Original
    root (hd0,0)
    kernel /vmlinuz-2.6.37.1-1.2-desktop root=/dev/system/root
    resume=/dev/system/swap splash=silent showopts vga=0x31a
    initrd /initrd-2.6.37.1-1.2-desktop
```

New

```
title Desktop -- openSUSE 12.2 - 2.6.37.1-1.2
    root (hd0,0)
    kernel /vmlinuz-2.6.37.1-1.2-desktop com6=115200,8n1 con-
    sole=com6L root=/dev/system/root resume=/dev/system/swap
    splash=silent console=tty0 console=ttyS0,115200 showopts
    vga=0x31a
    initrd /initrd-2.6.37.1-1.2-desktop
```

Note: In this example, com6/com6L is used, however COMM ports may vary.

18.2.6 Using Fedora* 17 (64-Bit)

For a video on Installing Fedora* and Xen*, refer [VT Training Series Videos](#) on PC Design Center.

18.2.6.1 Standard Linux* Installation for Fedora* 17 (64-Bit)

Prior to OS Installation, refer [Section 18.2.4 "Platform Setup Requirements"](#). Download Fedora* 17 (64-bit) and burn it on a DVD. Examples and references used in this procedure are based on installing Fedora* 17 on this platform (using Intel CRB). After booting the Fedora* DVD, follow the installation instructions below, (also, refer Fedora* installation guide on web).

1. Select Language and Keyboard Layout. Click Next after each page is complete.
2. Choose "Basic Storage Devices" in Installation Options. Click Next.
3. Choose system name, desired time zone, and password. Click Next after each.
4. Choose what type of Installation to use (It is recommended to Use All Space."), also check Use LVM. Click Next and Write Changes to Disk.
5. When prompted, choose "Software Development" and "Customize Now" option (at bottom of page) to install additional packages. Click Next. The recommended packages to install are:
 - a. Applications > Office and Productivity
 - b. Development > Development Tools
 - c. Development > Development Libraries



- d. Base System > System Tools
 - e. Base System > Virtualization Client
 - f. Base System > Virtualization Hypervisor
 - g. Servers > Network Server
6. Click Next and continue the installation.
 7. The system prompts for reboot after installing Fedora* so that the changes can be made.
 8. After the reboot follow the instructions to create an account when prompted. Click Forward.
 9. Alter login settings from user account:
 - a. Log on with the personal account you created.
 - b. Move to root permissions (using Linux* command "su").
 - c. When prompted for a password, make sure to use the root password.
 - d. Edit files for root login:
 - i. Change to root directory using **cd /**
 - ii. Edit "gdm-password" file in: `/etc/pam.d/gdm-password`
 - iii. Comment out the following line:
`Auth required pam_succeed_if.so user!=root quiet`
 - iv. Save the file and log out of system
 10. Log back in as root user.
 11. **Optional:** If user need to enable Ethernet access on boot:
 - a. Edit the following file: `/etc/sysconfig/network-scripts/ifcfg-eth0`
 - b. change **ONBOOT=no** to **ONBOOT=yes**
 - c. Reboot system
 - d. Log in as root after system reboot.

18.2.6.1.1 Installing Additional Packages for use with Fedora* 17

1. Open a web browser or terminal window and check again that you have a good internet connection (using "ifconfig", look for an assigned IP address in terminal).
2. Optional: If environment uses a proxy to connect to the internet, open a terminal window and type the command (as an example).
export http_proxy=http://proxy.yourcompany.com:port#
3. Install the following packages using yum:
 - a. `yum -y update yum`
 - b. `yum -y install bridge-utils`
 - c. `yum -y install mkinitrd`
 - d. `yum -y install iasl`
 - e. `yum -y install dev86`
 - f. `yum -y install unifdef`
 - g. `yum -y install mercurial`
 - h. `yum -y install xfig`



- i. yum -y install tigervnc-server
- j. yum -y install git
- k. yum -y install mesa-demos (this is for glxgears)

Note: If user receive the following error: **"Error: Cannot retrieve metalink for repository: Fedora*. Verify its path and try again"** Do the following to fix it:

1. CD to /etc/yum.repos.d
2. open fedora.repo in a text editor
3. Mask each instance of "#mirrorlist=" and unmask each instance of "baseurl="
4. Save file and do the same (steps 2 and 3) for fedora-updates.repo

Note: If you have difficulty installing from CD-ROM, try using an ISO file. Be sure to first copy the ISO file over to the local system (Using right click > Copy To > Home) and then use the local file.

18.2.6.2 Xen* Hypervisor Installation on Fedora* 17

First log into system as root user and ensure that the system is connected to the internet. To install and configure Xen* Hypervisor:

1. Enter **yum install xen and/or yum install xen kernel-xen**, or Download from **http://xen.org/products/xen_source** (This downloads latest Xen* Hypervisor available on the xen.org website).

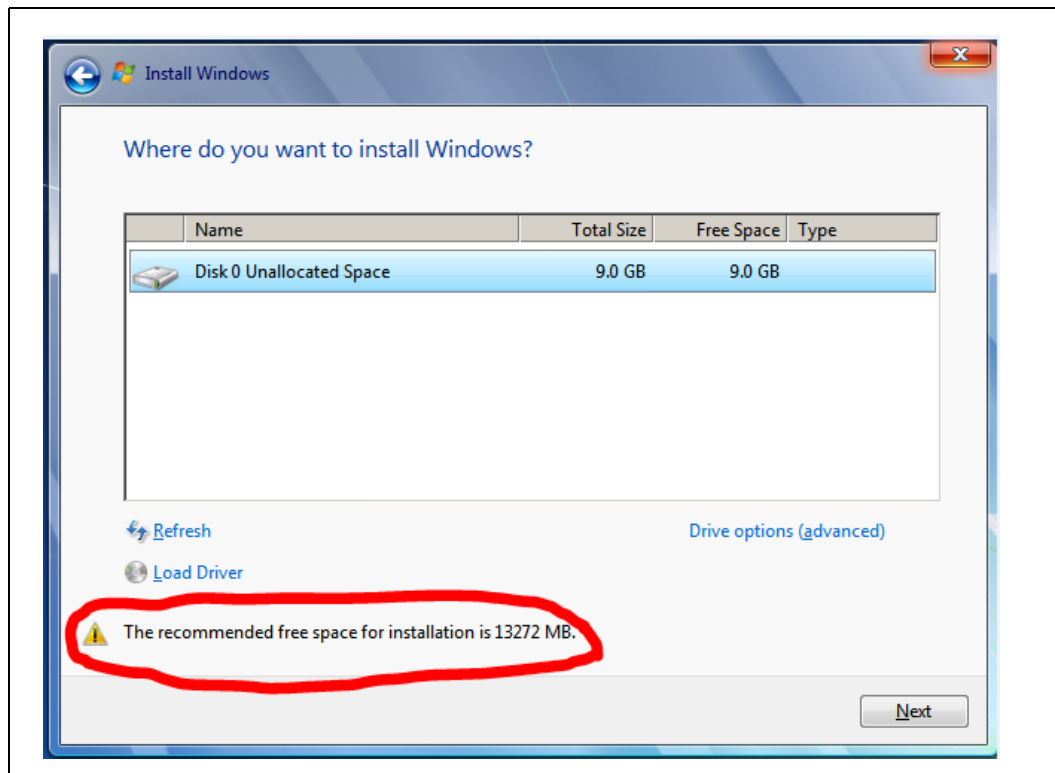
18.2.6.3 Creating a Virtual Machine on Fedora* 17

For a video on [Creating a virtual machine on Fedora* 14](#), refer the Videos Section on Broadwell Platform PCDC VT page.

Note: This process in Fedora* 14 is very similar to Fedora* 17.

1. Go to Applications > System Tools > Virtual Machine Manager. (if you are not logged in as root user, user need to provide root password to continue.)
2. Go to File > Add Connection > Choose Xen and Click Connect.
3. Click on localhost (xen).
4. Click on Create a new virtual machine icon and enter Name. Choose Xen* as connection type. Select Local installation media (ISO image or CD-ROM).
5. Select the Installation Source (If using an ISO file, it is best to copy the file directly to the system), Choose OS type and version. Click Forward.
6. Choose 2048MB RAM or more, and 1 Processor. Click Forward.
7. Choose Enable storage for this virtual machine, allocate at least 14GB (This number may vary. If you do not have enough space allocated, user may get an error that tells you how much to allocate. Refer [Figure 18-2](#)), and check allocate entire disk now.
8. Optional: In Final step, open Advanced options, use default Virtual network, change Virtual Type to xen, set architecture as x86_64 and Click Finish.
9. Follow the installation instructions for the OS.

Figure 18-2. Example Warning Allocating Space for Windows* 7/Virtual Machine



18.2.6.4 Testing Intel® VT Using Xen* VMM in Fedora* 17

The Intel® VT can be tested by assigning PCIe* I/O device(s) to the guest OS. When Intel® VT is used to directly assign an I/O device to a guest, the guest OS has direct access to I/O device hardware and guest VM owns the physical driver for that I/O device.

The test is considered to be passing when all of the following occur:

1. An I/O device can be successfully assigned to guest VM (Section 18.2.6.4.1).
2. Xen* VMM does not report any VT faults. Xen* VMM reports no VT faults in "dmesg" log. User need to search for VT faults by executing the following and search for VT messages:

```
dmesg | grep -i fault
--OR--
xm dmesg | grep -i fault (if using Xen earlier than 4.1)
--OR--
xl dmesg | grep -i fault (if using Xen 4.1.0 or later)
```

3. Guest VM detects the presence of new hardware. (In a Windows* OS, this can be determined through the VM device manager).



4. If the physical driver for the newly assigned I/O device is present in the guest OS, check that the device is functional.

18.2.6.4.1 Assigning an I/O Device Using PCISTUB Method

1. First obtain the Bus, Device, Function (BDF) ID of the device using:

```
lspci --OR-- lspci | grep -i "Ethernet"
```

Example result:

...

```
00:19.0 Ethernet controller: Intel Corporation 82566DM Giga-bit Net...
```

...

```
BDF = "00:19.0"
```

2. Now obtain device ID.

```
lspci -n
```

Example Result:

...

```
00:19.0 0200: 8086:153a (rev 01)
```

```
00:16.0 0200: 8086:8c3a (rev 01)
```

...

Use the BDF to find Device ID

```
Device ID = "8086 153a"
```

3. Enter the following, in order to unbind and attach the device

```
echo -n 0000:00:19.0 > /sys/bus/pci/devices/0000:00:19.0/driver/unbind
```

```
echo "8086 153a" > /sys/bus/pci/drivers/pci-stub/new_id
```

```
echo -n 0000:00:19.0 > /sys/bus/pci/drivers/pci-stub/bind
```

```
ls -l /sys/bus/pci/devices/0000:00:19.0/driver
```

this verifies the binding

```
xm pci-attach Guest 0:0:19.0
```

where *Guest* is the name of virtual machine

xl pci-assignable-add/remove

18.2.6.5 Special Instructions to Obtain Serial Log on Fedora* 17

To be added in a future revision.

§ §



19 Intel® Device Protection Technology with Boot Guard

19.1 Overview

Boot Guard (BtG) formerly Anchor Cove (AnC) is an Intel platform boot integrity protection technology. Boot Guard can protect the platform boot integrity by preventing execution of unauthorized boot block. With Boot Guard, the OEM can create a platform boot policies, such that invocation of an unauthorized (or compromised) boot block triggers the platform protection per the OEM policies. Based in the hardware, Boot Guard also extends the trusted boundary of the platform boot process down to the hardware. A benefit of this protection is that Boot Guard can help OEM maintains platform integrity by preventing reuse of the OEM hardware to run unauthorized software stack.

Note: The terms *Boot Guard* and *Anchor Cove* may be used interchangeably in this section.

19.2 Scope

This chapter describes a validation strategy for Boot Guard. This chapter is intended for validation purposes. The objective is to provide validation professionals with additional insight into Boot Guard by highlighting validation considerations. This chapter is not a technology overview and does not replace the existing Boot Guard collateral. The reader is expected to be familiar with Boot Guard and to use this document as a validation supplement to develop his own validation plan.

19.3 Prerequisites

This Boot Guard evaluation plan documented in this chapter requires the following components and tools for execution.

Table 19-1. Boot Guard Tools for Testing (Sheet 1 of 2)

Tool/Component	Revision	Comments
FIT	ME firmware kit with Boot Guard support	FIT is required to define the Boot Guard Boot Policies (persistent policies). Available on VIP
MEInfo	ME firmware kit with Boot Guard support	MEInfo is required to confirm Boot Guard Policies. Available on VIP Note: Non-Windows OS: Use the EFI version of the CSME tools (MEinfo.efi) to confirm Boot Guard Policies

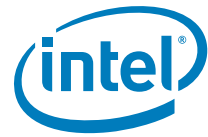


Table 19-1. Boot Guard Tools for Testing (Sheet 2 of 2)

Tool/Component	Revision	Comments
TXtBtgInfo.efi	0.7.10 or higher	<p>TXtBtgInfo.efi can be used to confirm Boot Guard status in the test cases below. Available on IBL. Training videos for BootGuardInfo are available on PCDC under Ingredients->Technologies->Boot Guard->Latest Videos</p> <p>Boot Guard status can be determined using various platform status registers:</p> <ol style="list-style-type: none"> 1. Refer BIOS Writers Guide for status registers (for example, ERRORCODE, BOOTSTATUS, ANC_SACM_INFO) usage 2. Refer ME BIOS Writer's Guide for Boot Guard related FWSTS registers verification.

19.4 Boot Guard Test Coverage Summary

Note: Profile 1 and profile 2 support has been deprecated. Only Profile 0: NO_FVME, Profile 3: VM, Profile 4: FVE and Profile 5: FVME are supported.

Note: Successful Boot Guard on S3 Resume has been removed as BootGuardInfo.exe tool runs only from EFI shell.

How?: A = Fully Automated using Intel® PETS, I = Interactive using Intel® PETS and M = Manual.

Test ID	Test Case Title
BtG_001	Successful VM (Verified Measured) Boot to OS ¹
BtG_002	Unsecure Boot to OS ¹
BtG_003	Failed VM (Verified Measured) Boot fail to Fallback
BtG_004	Platform Public Signing Key Provisioned
BtG_005	Successful VM (Verified Measured) Boot to OS ¹ using FPF
BtG_006	BIOS Update Procedure includes Signature Verification
BtG_007	Service Center's Recovery process for Boot Guard failed platform
BtG_008	BIOS Continues the Chain of Trust

Notes:

1. Refer Chapter 1- Introduction, Section 1.1 for supported Operating Systems (OS).

Test ID	BtG_001
Test Case Title	Successful Verified-Measured (VM) Boot to OS
Mandatory/Optional	Mandatory
Firmware SKU	Consumer / Corporate
Description	In this test case, Boot Guard performs a successful verification and measuring of the SUT Initial Boot Block (IBB.) Upon successful verification Boot Guard pass execution to the IBB to continue the boot process.
Objective	This test verifies that the SUT has all the required components: hardware, firmware, ACM and BIOS. Additionally, the SUT has been correctly provisioned in manufacturing for the platform to boot with the Boot Guard for IBB verification and measurement.



Test ID	BtG_001
Procedure	<p>Prepare the SUT Persistent Policy (FPF)</p> <ol style="list-style-type: none">Provision the SUT Persistent Policies (NVAR, if this is development system) to either the VM or FVE or FVME profile. Per the testing objective<ul style="list-style-type: none">The FVME profile usage is not advised for the development or testing environment. In this strictest protection mode, test failure requires BIOS flashing to restore the system.Refer the ME Firmware Bring Up Guide for information on the Boot Guard related FIT options and settingsInstall the Intel® ME firmware and BIOS image that are Boot Guard enabled and has been authorized by the key in the Persistent Policy (FPF or NVAR).Install the targeted OS (OS), if not already installed on the SUT.Run the MEinfo tool and check for the fields under "FPF" column for FPF contents and "ME" for NVAR contents. Ensure that these matches with what was provisioned during the image creation process. <p>Verify the Boot</p> <ol style="list-style-type: none">Power-off the SUT.Power-on the SUT.Boot to EFI shell and execute TXTBtgInfo.efiVerify the TXTBtgInfo.efi output to confirm that Boot Guard has booted as configured to verify and measure the IBB.Boot to OS.Execute PETS package for Boot Guard from Remote ConsoleVerify PETS results should Pass
Test Pass/Fail Criteria	<p>Test passes, if the SUT:</p> <ul style="list-style-type: none">Boots fully functional to OS.The TPM/PTT device reports the correct measurement in PCR.PETS tests BootGuard_001 and BootGuard_002 should Pass.TXTBtgInfo.efi reports that Boot Guard was successful.

Test ID	BtG_002
Test Case Title	Un-secure Boot to OS
Mandatory/Optional	Mandatory
Firmware SKU	Consumer / Corporate
Description	In this test case, Boot Guard performs a successful un secure boot of SUT Initial Boot Block (IBB.) Upon successful completion Boot Guard passes execution to the IBB to continue the boot process with IBB verification.
Objective	This test verifies that the SUT has all the required components: hardware, firmware, ACM and BIOS. Additionally, the SUT has been correctly provisioned in manufacturing for the platform to boot without Boot Guard verification and measuring of the IBB.
Procedure	<p>Prepare the SUT Persistent Policy (FPF)</p> <ol style="list-style-type: none">Verify <i>Persistent Policies</i> on the SUT set to default (that is, all '0') or set the <i>No_FVME</i> profile.<ul style="list-style-type: none">Refer the ME Firmware Bring Up Guide for information on the Boot Guard related FIT options and setting.Install the Intel® CSME firmware and BIOS image that are Boot Guard enabled and has been authorized by the key in the Persistent Policy (FPF or NVAR).Install the targeted OS (OS, OS), if not already installed on the SUT.Run MEinfo tool and check for the fields under "FPF" column for FPF contents and "ME" for NVAR contents. Ensure that these matches with what was provisioned during the image creation process. <p>Verify the Boot</p> <ol style="list-style-type: none">Power-off the SUT.Power-on the SUT.Boot to EFI shell and execute TXTBtgInfo.efiVerify the TXTBtgInfo.efi output to confirm that Boot Guard has booted as configured to verify and measure the IBB.Boot to OS.Execute PETS package for Boot Guard from Remote ConsoleVerify PETS results should Pass



Test ID	BtG_002
Test Pass/Fail Criteria	<p>Test passes, if the SUT:</p> <ul style="list-style-type: none"> Boots fully functional to OS. PETS tests BootGuard_001 and BootGuard_002 should Pass. TXTBtgInfo.efi reports that Boot Guard boot was successful.

Test ID	BtG_003
Test Case Title	Failed VM Boot fail to Fallback
Mandatory/Optional	Mandatory
Firmware SKU	Consumer / Corporate
Description	In this test case, Boot Guard performs an unsuccessful verification and measuring of the SUT Initial Boot Block (IBB.) Upon verification failure Boot Guard performs the fallback behavior per the persistent policy.
Objective	This test verifies that the SUT has all the required components: hardware, firmware, ACM, and BIOS. Additionally, the SUT has been correctly provisioned in manufacturing for the platform to handle failure condition per the SUT targeted security objective.
Procedure	<p>Prepare the SUT Persistent Policy (FPF)</p> <ol style="list-style-type: none"> Provision the SUT <i>Persistent Policies</i> (NVAR if this is development system) to either the <i>VM</i> or <i>FVE</i> or <i>FVME</i> profile. Per testing objective. <ul style="list-style-type: none"> The FVME profile usage is not advised for the development or testing environment. In this strictest protection mode, test failure requires BIOS flashing to restore the system. Refer the ME Firmware Bring Up Guide for information on the Boot Guard related FIT options and settings. Install the Intel® ME firmware and BIOS image that are Boot Guard enabled and has been authorized by the key in the Persistent Policy (FPF or NVAR). Install the targeted OS (OS) if not already installed on the SUT. Run MEinfo tool and check for the fields under "FPF" column for FPF contents and "ME" for NVAR contents. Ensure that these matches with what was provisioned during the image creation process. <p>Prepare the SUT BIOS</p> <ol style="list-style-type: none"> Corrupt the BIOS image by modifying either KM, BPM or IBB to create a BPM signing key mismatch, KM key mismatch or a invalid KM key index. <p>Verify the Boot</p> <ol style="list-style-type: none"> Power-off the SUT. Power-on the SUT. Execute PETS package for Boot Guard from Remote Console. Verify PETS results should Fail. Verify that the platform has failed per the persistent policy. <ul style="list-style-type: none"> Refer the Boot Guard for HSW-ULT to details on expected failure handling behavior for the SUT.
Test Pass/Fail Criteria	<p>Test passes, if the SUT exhibit the failure condition as expected per the configured profile:</p> <ul style="list-style-type: none"> FVE - The platform halts upon verification failure. FVME - The platform halts upon verification failure. VM - The platform would not halt upon verification failure.

Test ID	BtG_004
Test Case Title	Platform Public Signing Key Provisioned
Mandatory/Optional	Mandatory
Firmware SKU	Consumer / Corporate
Description	In this test case, the platform public signing key is verified to be provisioned for the platform.



Test ID	BtG_004
Objective	This is intended to be a check of the OEM signing capability and persistent policy provisioning process.
Procedure	<p>Prepare the SUT Persistent Policy</p> <ol style="list-style-type: none"> 1. Provision the SUT <i>Persistent Policies</i> (NVAR if this is development system) to either the <i>VM</i> or <i>FVE</i> or <i>FVME</i> profile. Per testing objective <ul style="list-style-type: none"> — The FVE profile usage is not advised for the development or testing environment. In this strictest protection mode, test failure requires BIOS flashing to restore the system. <p>Verify the signing key in the Persistent Policy</p> <ol style="list-style-type: none"> 2. Boot the SUT to OS. 3. Run MEInfo.exe. 4. Evaluate the Boot Guard related fields: <ul style="list-style-type: none"> • "FPF" for committed Persistent policies. • "ME" for NVAR stored Persistent policies.
Test Pass/Fail Criteria	<p>Test passes, if the SUT:</p> <ul style="list-style-type: none"> • Hash of the OEM platform public signing key was correctly provisioned in the Persistent Policy (NVAR or FPF) that is, matches with what was provisioned during the image creation process.

Test ID	BtG_005
Test Case Title	Boot Guard feature testing using Field programmable Fuse (FPF) values
Mandatory/Optional	Mandatory
Firmware SKU	Consumer / Corporate
Description	<p>In this test case, Boot Guard performs Boot Guard feature testing using the values from the FPFs that is, accessing the Boot Guard profile values from the FPFs instead of the Flash variables that is, NVARs).</p> <p>Note: This test can be skipped if test BtG_001 or BtG_004 were completed using FPF Persistent Policies.</p>
Objective	This test performs and validates all the components used in the Boot Guard feature that is, hardware, firmware, ACM and BIOS. It also tests that the platform is properly provisioned for Boot Guard IBB verification and measurement from the Field Programmable Fuses (FPFs).
Procedure	<p>Pre-requisite: Perform this test ONLY, when all the tests (BtG_001 to BtG_006) have passed by testing Boot Guard using the profile values from the NVARs (flash variables).</p> <p>Important: The profile selected to be committed into FPFs becomes the final profile, which cannot be altered later. It is not possible to return the system to a pre-test configuration state, once FPF has been committed. As such, care must be taken to ensure that the proper test pre-requisites have been completed before proceeding.</p> <ol style="list-style-type: none"> 1. Perform the step to commit the Boot Guard profile values to the FPFs. <p>This is done automatically after CSME Manufacturing mode is disabled (during the global reset from FPT -closemnf or first boot for Pre-Lock image), if firmware and MCP combination is Production.</p> <p>Or</p> <p>Done by means of a specific FPF MEI command (if combination of firmware and MCP is Pre-production).</p> <p>Below commands can be used for FPF commit on pre-production platforms. (Also refer the CSME Tools guide for the tools usage).</p> <ul style="list-style-type: none"> • "FPT -FPFs" - To retrieve the FPF names. • "FPT -COMMITFPFS <FPFname>" - To commit values to FPFs one at a time. • or "FPT -COMMITFPF All" - To commit values to FPFs all at once. <ol style="list-style-type: none"> 2. Run MEInfo tool to view the values set in the FPFs and the NVAR-FPF mismatch field. If there is a mismatch, tool indicates it with a FPF mismatch message. 3. Execute the tests (Test ID BtG_001 or BtG_004) based on the profile that has been committed on the FPFs.



Test ID	BtG_005
Test Pass/Fail Criteria	<p>Test passes, if the SUT:</p> <ul style="list-style-type: none"> The FPF commit command is successfully executed and MEinfo tool O/P shows the correct Boot Guard profile settings and values under the "FPF" column for each Boot Guard variable. Further Fail/Pass criteria is the same as criteria mentioned for each of the tests above (test id #BtG_001 or BtG_004).

Test ID	BtG_006
Test Case Title	BIOS Update Procedure includes Signature Verification
Mandatory/Optional	Optional
Firmware SKU	Consumer / Corporate
Description	This is a manual assessment of the platform BIOS update process to ensure that signature verification is applied to maintain BIOS integrity.
Objective	Confirm the signature authorization structure defined by the Persistent Policy (FPF)->KM->BPM->IBB are maintained in BIOS update process.
Procedure	1. Confirm with the BIOS Development team that BIOS update process is using proper authorization process to maintain the Boot Guard authorization structure from FPF->KM->BPM->IBB.
Test Pass/Fail Criteria	<p>Test passes, if the SUT:</p> <ul style="list-style-type: none"> If the BIOS update process contains the proper checks to maintain the Boot Guard signature authorization structure.

Test ID	BtG_007
Test Case Title	Service Center's Recovery process for Boot Guard failed platform
Mandatory/Optional	Optional
Firmware SKU	Consumer / Corporate
Description	This is a manual assessment of the platform service process to ensure that platforms that has failed Boot Guard verification can be recovered to fully functional state.
Objective	Confirm that a service process is established to handle Boot Guard failure per configured persistent policy.
Procedure	1. Evaluate the platform service process for the failed Boot Guard scenario. <ul style="list-style-type: none"> Does the service process meet the platform business objective?
Test Pass/Fail Criteria	<p>Test passes, if the SUT:</p> <ul style="list-style-type: none"> If the platform recovery process meets the business objective.

Test ID	BtG_008
Test Case Title	BIOS Continues the Chain of Trust
Mandatory/Optional	Optional
Firmware SKU	Consumer / Corporate
Description	This is a manual test to confirm that the BIOS has taken the required steps to protect and continue the chain of trust from Boot Guard.
Objective	Ensure that the SUT maintains the secure boot value proposition from when Boot Guard completes to when the UEFI Secure Boot protection are implemented in the BIOS.



Test ID	BtG_008
Procedure	1. Confirm with the BIOS Development team that IBB and the next boot phase is protecting the integrity of the secure boot on the platform, as recommended in the Boot Guard BIOS Writer's Guide, when it receives platform controls from the Boot Guard ACM.
Test Pass/Fail Criteria	Test passes, if the SUT: <ul style="list-style-type: none">• If the BIOS team confirms that the proper protection are implemented for the SUT

§ §



20 Manufacturing Flow Simulation Test

20.1 Manufacturing Flow Simulation Test

Test ID	Test Case Title	PETS/Manual	Form Factor	Network Factor
MFG_001	Intel® CSME Manufacturing Flow Simulation Test	Manual	MB, DT and WS	LAN+WLAN; WLAN only

Test ID	MFG_001
Test Case Title	Intel® CSME Manufacturing Flow Simulation Test
Mandatory/Optional	Mandatory
Firmware SKU	Corporate
Description	For platform with Intel® ME, it is necessary to perform steps in the manufacturing line to ensure the Intel® CSME is functional and the system is secure, and ready for shipment. The minimum requirements can be met by following the Intel® CSME Manufacturing Reference Flow.
Objective	This test is to run Intel manufacturing tools in manufacturing simulation during the development phase to capture configuration, settings, and other potential issues that customers might encounter later in manufacturing, which is costly.



Test ID	MFG_001
Procedure:	<p>Test Environment:</p> <ul style="list-style-type: none">• System configuration should be as close as possible to what it is during production/manufacturing phase. Example: WLAN module installed, and so forth.• Use the same OS environment as planning to use in the manufacturing line (with all the necessary driver/software installed. Example: Intel® MEI driver for Windows* OS, and so forth.) <p>Test Preparation:</p> <ul style="list-style-type: none">• Configure the desired secure boot setting (OEM public key hash, policy, and so forth) for Boot Guard and Intel® PTT Supported [FPF] for PTT and all the variables in MEManuf.xml under EOL VAR TEST session.• If this test is conducted on platform with production configuration and ready to run EOM flow, also configure the desired secure boot setting (OEM public key hash, policy, and so forth) for Boot Guard and Intel® PTT Supported [FPF] for PTT in MEManuf.xml under EOL CONFIG Test session. <p>Test Procedure:</p> <ol style="list-style-type: none">1. Use the version of FPT and, MEManuf executable suitable for the chosen OS environment (located in the latest Intel® CSME kit) to simulate at least the Intel® CSME Manufacturing reference flow (Below steps).2. If using pre-lock (the descriptor Master Access permission set to Intel recommended production value during image preparation), do only steps 5, 6, 7, 8 and 11.3. Reprogram the image currently on board (Example: Image.bin). Example: FPTW64.exe -f image.bin4. Reset Intel® CSME and Host after program successfully. Example: FPTW64.exe -greset5. For platform supporting AMT (if platform does not supporting AMT, skip this step), firstly ensure supported Intel WLAN module is installed. Then perform WLAN µcode update using the Intel® CSME binary (Example: ME.bin) from Firmware kit. Example: FWUpdLcl64.exe -f ME.bin -partid wcod6. Verify Intel® CSME (for non-AMT capable only w/ Auto BIST disabled). Example: MEManufWin64.exe Example (option): MEManufWin64.exe -f MEManuf.xml (use the MEManuf.xml configuration file configured during preparation).7. Verify Intel® CSME (for AMT capable w/ Auto BIST enabled) If Automatic Build In Self Test is enabled in FIT during preparation, run MEManuf once to get full verification result. Example: MEManufWin64.exe. Example (option): MEManufWin64.exe -f MEManuf.xml (use the MEManuf.xml configuration file configured during preparation).8. Verify Intel® CSME (for AMT capable w/Auto BIST disabled). If Automatic Build In Self Test is disabled in FIT during preparation, run MEManuf twice to get full verification result. After first running 1st time MEManuf, user observes a power cycle, which is because system entering CSME BIST under M3 mode and save the result in SPI. After running 2nd MEManuf, it get the full validation result. Example: MEManufWin64.exe. Example (option): MEManufWin64.exe -f MEManuf.xml (use the MEManuf.xml configuration file configured during preparation).9. Check Boot Guard, PTT, and all the variables match with setting configured in FIT. Example: MEManufWin64.exe -EOL var -f MEManuf.xml (use the MEManuf configuration file configured during preparation).



Test ID	MFG_001
	<p>10. Set Intel® CSME manufacturing done bit and descriptor Master Access permission to Intel recommended production value, then perform global reset to make sure Intel® CSME manufacturing mode is disabled. Example: FPTW64.exe -closemnf -y</p> <p>Note: PDR, EC BIOS or legacy addition could be used following FPTW64.exe -closemnf -y to allow various CPU/BIOS read/write access setting based on customer need. Check System Tool User Guide for more detail.</p> <p>11. Perform end of line check on Intel recommended default test item and also Boot Guard, PTT, and all the configuration check. Example: MEManufWin64.exe -EOL (It run Intel recommended default test) or Example (option): MEManufWin64.exe -EOL config -f MEManuf.xml (use the MEManuf.xml configuration file configured during preparation more sub tests enabled).</p> <p>Note: It is highly recommended you create own script file to automatically run the above steps in order to better simulate the manufacturing flow.</p>
Test Pass/Fail Criteria	<p>Pass only, when all the tools run above return pass result.</p> <p>Note: When encounter failure, check:</p> <ul style="list-style-type: none"> • CRB test result in Compliance kit. • Intel® CSME firmware release notes for known issues.

§ §



21 Platform Controller Hub (PCH) SoftStrap Configuration

Overview:

The Intel® PCH SoftStraps are load into the appropriate strapping registers within the PCH at boot time from the SPI flash device's Flash Descriptor. Some of the features within the PCH are configurable through the PCH SoftStraps such as the Flexible I/O, SMLINK, GbE, and Intel® ME. The PCH SoftStraps are configure using the FIT tool. Refer the SPI Programming Guide for the details description on all the available PCH SoftStraps.

All the test case in this chapter are currently cover automatically by PETS on the target system at runtime. Static checking on the image created by FIT is not supported.

Tools for Testing:

Intel® Platform Enablement Test Suite (PETS)—Latest version of tools from this kit. Refer the Intel® PETS user guide available in the Intel® Compliancy kit for exact instructions on how to load and setup the Intel® PETS software.

Intel® Flash Image Tool (FIT.exe)

Intel® Flash Programming Tool—Available in DOS (fpt.exe), EFI (fpt.efi), Windows* 32-bit (fptw.exe), and Windows* 64-bit operating systems.

Test Environment:

The System Under Test (SUT) is to be configured in manual configuration mode a with wired LAN dynamic IP address. The DHCP server connecting the SUT and Management Console (MC) must be configured to ensure that the wired LAN and wireless LAN addresses reside on separate subnets. The MC could be a laptop or desktop system running a version of Windows* supported by PETS. The network configuration consists of a hub or switch, network cables, and a wireless Access Point (AP).



21.1 Test Coverage Summary

Test ID	Test Case Title	PETS/Manual	Network Factor
PSS_001	Intel Integrated Wired LAN Test	PETS	LAN+WLAN; WLAN only
PSS_002	Wake On Wireless LAN (WoWLAN) Test	PETS	LAN+WLAN; WLAN only
PSS_003	Flexible I/O Test	PETS	LAN+WLAN; WLAN only
PSS_004	BIOS Boot-Block Size Test	PETS	LAN+WLAN; WLAN only
PSS_005	Intel® CSME SMBus ASD Address Test	PETS	LAN+WLAN; WLAN only
PSS_007	Power State Deep Sx Test	PETS	LAN+WLAN; WLAN only
PSS_008	TPM on SPI Test	PETS	LAN+WLAN; WLAN only

21.2 Intel Integrated Wired LAN Test

Test ID:	PSS_001
Test Case Title:	Intel Integrated Wired LAN Test
Mandatory/Optional:	Mandatory
Description:	The PCH SoftStraps for Intel Integrated Wired LAN has to be configure correctly to ensure proper operation. Even if not using Intel Integrated Wired LAN on the platform, these PCH SoftStraps must be configured correctly as well.
Objective:	To verify correct configuration of PCH SoftStraps related to Intel Integrated Wired LAN.



Test ID:

PSS_001

Procedure:

Boot to targeted OS. Verify correct configuration of the PCH SoftStraps below:

1. If using the Intel Integrated Wired LAN solution:

Name	Location	Value
SMLink0 Enable	Offset 0x189 [0] LP Offset 0x199 [0] H	1h 1h
GbE PHY SMBus Address	Offset 0x1BC [6:0] LP Offset 0x208 [6:0] H	64h 64h
GbE MAC SMBus Address	Offset 0x1B4 [6:0] LP Offset 0x200 [6:0] H	70h 70h
Gbe MAC SMBus Address Enable	Offset 0x1B7 [0] LP Offset 0x203 [0] H	1h 1h
PHY Connection	Offset 0x20A [2:0] LP Offset 0x25E [2:0] H	2h 2h
Intel® PHY Over PCIe Enable	Offset 0x1F4 [6] LP Only	1h
Intel® Integrated wired LAN Enable	Offset 0xC18 [0] Both	0h

a. What PCIe* port is the Intel® PHY attached?

Name	Location	Value
GBE PCIe* Port Select	Offset 0x1F4 [5:3] LP	0h = Port 7, 1h = Port 8, 2h = Port 9 3h = Port 13 4h = Port 14

Name	Location	Value
GBE PCIe* Port Select	Offset 0x23E [3:0] H Offset 0x244 [3:0] Offset 0x245 [7:4] Offset 0x246 [3:0]	Port 5 = 8h Port 9 = 8h Port 12 = 8h Port 13 = 8h

Caution:

Mapping GbE to any of the PCIe* ports means all 4 Lanes of that PCIe* no longer be available as PCIe* ports.

b. Is GPD11 from PCH routed to LAN_DISABLE_N on the Intel wired LAN PHY? (Requires Schematic Review)

— If YES:

Name	Location	Value
LAN PHY Power Control GPD11 Signal Configuration	Offset 0x10C [4] LP and H	0h

— If NO:

Name	Location	Value
LAN PHY Power Control GPD11 Signal Configuration	Offset 0x10C [4] LP and H	1h



Test ID:	PSS_001																		
	<div>2. If not using Intel Integrated Wired LAN solution:</div> <table><thead><tr><th>Name</th><th>Location</th><th>Value</th></tr></thead><tbody><tr><td>LAN PHY Power Control GPD11 Signal Configuration</td><td>Offset 0x10C [4] LP and H</td><td>1h</td></tr><tr><td>Gbe MAC SMBus Address Enable</td><td>Offset 0x1B4 [6:0] LP Offset 0x203 [6:0] H</td><td>0h</td></tr><tr><td>PHY Connection</td><td>Offset 0x20A [2:0] LP Offset 0x25E [2:0] H</td><td>0h</td></tr><tr><td>Intel® PHY Over PCIe Enable</td><td>Offset 0x1F4[6] LP Only</td><td>0h</td></tr><tr><td>Intel® Integrated wired LAN Enable</td><td>Offset 0xC18 [0] Both</td><td>1h</td></tr></tbody></table>	Name	Location	Value	LAN PHY Power Control GPD11 Signal Configuration	Offset 0x10C [4] LP and H	1h	Gbe MAC SMBus Address Enable	Offset 0x1B4 [6:0] LP Offset 0x203 [6:0] H	0h	PHY Connection	Offset 0x20A [2:0] LP Offset 0x25E [2:0] H	0h	Intel® PHY Over PCIe Enable	Offset 0x1F4[6] LP Only	0h	Intel® Integrated wired LAN Enable	Offset 0xC18 [0] Both	1h
Name	Location	Value																	
LAN PHY Power Control GPD11 Signal Configuration	Offset 0x10C [4] LP and H	1h																	
Gbe MAC SMBus Address Enable	Offset 0x1B4 [6:0] LP Offset 0x203 [6:0] H	0h																	
PHY Connection	Offset 0x20A [2:0] LP Offset 0x25E [2:0] H	0h																	
Intel® PHY Over PCIe Enable	Offset 0x1F4[6] LP Only	0h																	
Intel® Integrated wired LAN Enable	Offset 0xC18 [0] Both	1h																	
Test Pass/Fail Criteria:	Test passes if SoftStraps/register setting in this step matches to the configuration in the target system.																		

21.3 Wake On Wireless LAN (WoWLAN) Test

Test ID:	PSS_002												
Test Case Title:	Wake On Wireless LAN (WoWLAN) Test												
Mandatory/Optional:	Mandatory												
Description:	The PCH controls the voltage rails into the external wireless LAN PHY using the SLP_WLAN# pin. The corresponding SoftStrap has to be configured correctly to ensure proper function of wake on wireless LAN feature.												
Objective:	To verify correct configuration of the SLP_WLAN# SoftStrap setting.												
Procedure:	<p>Boot to targeted OS. Verify correct configuration of the PCH SoftStraps below:</p> <p>1. Is Wake On Wireless LAN (WoWLAN) required? — If YES:</p> <table><tr><th>Name</th><th>Location</th><th>Value</th></tr><tr><td>SLP_WLAN# / GPD9 Signal Configuration</td><td>Offset 0x10C [3] LP and H</td><td>0h</td></tr></table> <p> — If NO:</p> <table><tr><th>Name</th><th>Location</th><th>Value</th></tr><tr><td>SLP_WLAN# / GPD9 Signal Configuration</td><td>Offset 0x10C [3] LP and H</td><td>1h</td></tr></table>	Name	Location	Value	SLP_WLAN# / GPD9 Signal Configuration	Offset 0x10C [3] LP and H	0h	Name	Location	Value	SLP_WLAN# / GPD9 Signal Configuration	Offset 0x10C [3] LP and H	1h
Name	Location	Value											
SLP_WLAN# / GPD9 Signal Configuration	Offset 0x10C [3] LP and H	0h											
Name	Location	Value											
SLP_WLAN# / GPD9 Signal Configuration	Offset 0x10C [3] LP and H	1h											
Test Pass/Fail Criteria:	Test passes if SoftStraps/register setting in this step matches to the configuration in the target system.												



21.4 Flexible I/O Test

Test ID:	PSS_003																																										
Test Case Title:	Flexible I/O Test																																										
Mandatory/Optional:	Mandatory																																										
Description:	Flexible I/O is an architecture that allows some high speed signals to be configured as PCIe*, USB 3.x or SATA signals. Through SoftStraps, the functionality on these multiplexed signals are selected to meet I/O needs on the target platform.																																										
Objective:	To verify correct configuration of Flexible I/O SoftStraps.																																										
Procedure:	<p>Boot to targeted OS. Verify correct configuration of the PCH SoftStraps below:</p> <p>1. How do you have PCIe Controller 1 (Port 1-4) configured?</p> <p>a. 1x4 – one 4 lane PCIe* Port</p> <table><tr><th>Name</th><th>Location</th><th>Value</th></tr><tr><td>PCIe Controller 1 (Port 1-4)</td><td>Offset 0x14D [4:3] LP and H</td><td>3h</td></tr></table> <p>v. Are the lanes reversed? — If Reversed:</p> <table><tr><th>Name</th><th>Location</th><th>Value</th></tr><tr><td>PCIe Controller 1 Lane Reversal</td><td>Offset 0x14D [2] LP and H</td><td>1h</td></tr></table> <p>— If NOT Reversed:</p> <table><tr><th>Name</th><th>Location</th><th>Value</th></tr><tr><td>PCIe Controller 1 Lane Reversal</td><td>Offset 0x14D [2] LP and H</td><td>0h</td></tr></table> <p>b. 2x2 – two 2 lane PCIe* Port</p> <table><tr><th>Name</th><th>Location</th><th>Value</th></tr><tr><td>PCIe Controller 1 (Port 1-4)</td><td>Offset 0x14D [4:3] LP and H</td><td>2h</td></tr></table> <p>c. 1x2, 2x1- One 2 lane PCIe* Port, Two 1 lane PCIe* Port</p> <table><tr><th>Name</th><th>Location</th><th>Value</th></tr><tr><td>PCIe Controller 1 (Port 1-4)</td><td>Offset 0x14D [4:3] LP and H</td><td>1h</td></tr></table> <p>d. 4x1: Ports (1-4) (x1)</p> <table><tr><th>Name</th><th>Location</th><th>Value</th></tr><tr><td>PCIe Controller 1 (Port 1-4)</td><td>Offset 0x14D [4:3] LP and H</td><td>0h</td></tr></table> <p>2. How do you have PCIe Controller 2 (Port 5-8) configured?</p> <p>a. 1x4 – One 4 lanes PCIe* Port.</p> <table><tr><th>Name</th><th>Location</th><th>Value</th></tr><tr><td>PCIe Controller 2 (Port 5-8)</td><td>Offset 0x155 [4:3] LP and H</td><td>3h</td></tr></table>	Name	Location	Value	PCIe Controller 1 (Port 1-4)	Offset 0x14D [4:3] LP and H	3h	Name	Location	Value	PCIe Controller 1 Lane Reversal	Offset 0x14D [2] LP and H	1h	Name	Location	Value	PCIe Controller 1 Lane Reversal	Offset 0x14D [2] LP and H	0h	Name	Location	Value	PCIe Controller 1 (Port 1-4)	Offset 0x14D [4:3] LP and H	2h	Name	Location	Value	PCIe Controller 1 (Port 1-4)	Offset 0x14D [4:3] LP and H	1h	Name	Location	Value	PCIe Controller 1 (Port 1-4)	Offset 0x14D [4:3] LP and H	0h	Name	Location	Value	PCIe Controller 2 (Port 5-8)	Offset 0x155 [4:3] LP and H	3h
Name	Location	Value																																									
PCIe Controller 1 (Port 1-4)	Offset 0x14D [4:3] LP and H	3h																																									
Name	Location	Value																																									
PCIe Controller 1 Lane Reversal	Offset 0x14D [2] LP and H	1h																																									
Name	Location	Value																																									
PCIe Controller 1 Lane Reversal	Offset 0x14D [2] LP and H	0h																																									
Name	Location	Value																																									
PCIe Controller 1 (Port 1-4)	Offset 0x14D [4:3] LP and H	2h																																									
Name	Location	Value																																									
PCIe Controller 1 (Port 1-4)	Offset 0x14D [4:3] LP and H	1h																																									
Name	Location	Value																																									
PCIe Controller 1 (Port 1-4)	Offset 0x14D [4:3] LP and H	0h																																									
Name	Location	Value																																									
PCIe Controller 2 (Port 5-8)	Offset 0x155 [4:3] LP and H	3h																																									



Test ID:	PSS_003																																																
	<p>i. Are the lanes reversed? — If reversed:</p> <table border="1"> <thead> <tr> <th>Name</th> <th>Location</th> <th>Value</th> </tr> </thead> <tbody> <tr> <td>PCIe Controller 2 Lane Reversal</td> <td>Offset 0x155 [2] LP and H</td> <td>1h</td> </tr> </tbody> </table> <p>— If NOT reversed:</p> <table border="1"> <thead> <tr> <th>Name</th> <th>Location</th> <th>Value</th> </tr> </thead> <tbody> <tr> <td>PCIe Controller 2 Lane Reversal</td> <td>Offset 0x155 [2] LP and H</td> <td>0h</td> </tr> </tbody> </table> <p>b. 2x2 – two 2 lanes PCIe* Port.</p> <table border="1"> <thead> <tr> <th>Name</th> <th>Location</th> <th>Value</th> </tr> </thead> <tbody> <tr> <td>PCIe Controller 2 (Port 5-8)</td> <td>Offset 0x155 [4:3] LP and H</td> <td>2h</td> </tr> </tbody> </table> <p>c. 1x2, 2x1 – One 2 lanes PCIe* Port, Two 1 lane PCIe* Port.</p> <table border="1"> <thead> <tr> <th>Name</th> <th>Location</th> <th>Value</th> </tr> </thead> <tbody> <tr> <td>PCIe Controller 2 (Port 5-8)</td> <td>Offset 0x155 [4:3] LP and H</td> <td>1h</td> </tr> </tbody> </table> <p>d. 4x1- One 1 lane PCIe* Port.</p> <table border="1"> <thead> <tr> <th>Name</th> <th>Location</th> <th>Value</th> </tr> </thead> <tbody> <tr> <td>PCIe Controller 2 (Port 5-8)</td> <td>Offset 0x155 [4:3] LP and H</td> <td>0h</td> </tr> </tbody> </table> <p>3. How do you have PCIe Controller 3 (Port 9-12) configured?</p> <p>a. 1x4 – One 4 lanes PCIe* Port.</p> <table border="1"> <thead> <tr> <th>Name</th> <th>Location</th> <th>Value</th> </tr> </thead> <tbody> <tr> <td>PCIe Controller 3 (Port 9-12)</td> <td>Offset 0x15D [4:3] LP and H</td> <td>3h</td> </tr> </tbody> </table> <p>i. Are the lanes reversed? — If reversed:</p> <table border="1"> <thead> <tr> <th>Name</th> <th>Location</th> <th>Value</th> </tr> </thead> <tbody> <tr> <td>PCIe Controller 3 Lane Reversal</td> <td>Offset 0x15D [2] LP and H</td> <td>1h</td> </tr> </tbody> </table> <p>— If NOT reversed:</p> <table border="1"> <thead> <tr> <th>Name</th> <th>Location</th> <th>Value</th> </tr> </thead> <tbody> <tr> <td>PCIe Controller 3 Lane Reversal</td> <td>Offset 0x15D [2] LP and H</td> <td>0h</td> </tr> </tbody> </table>	Name	Location	Value	PCIe Controller 2 Lane Reversal	Offset 0x155 [2] LP and H	1h	Name	Location	Value	PCIe Controller 2 Lane Reversal	Offset 0x155 [2] LP and H	0h	Name	Location	Value	PCIe Controller 2 (Port 5-8)	Offset 0x155 [4:3] LP and H	2h	Name	Location	Value	PCIe Controller 2 (Port 5-8)	Offset 0x155 [4:3] LP and H	1h	Name	Location	Value	PCIe Controller 2 (Port 5-8)	Offset 0x155 [4:3] LP and H	0h	Name	Location	Value	PCIe Controller 3 (Port 9-12)	Offset 0x15D [4:3] LP and H	3h	Name	Location	Value	PCIe Controller 3 Lane Reversal	Offset 0x15D [2] LP and H	1h	Name	Location	Value	PCIe Controller 3 Lane Reversal	Offset 0x15D [2] LP and H	0h
Name	Location	Value																																															
PCIe Controller 2 Lane Reversal	Offset 0x155 [2] LP and H	1h																																															
Name	Location	Value																																															
PCIe Controller 2 Lane Reversal	Offset 0x155 [2] LP and H	0h																																															
Name	Location	Value																																															
PCIe Controller 2 (Port 5-8)	Offset 0x155 [4:3] LP and H	2h																																															
Name	Location	Value																																															
PCIe Controller 2 (Port 5-8)	Offset 0x155 [4:3] LP and H	1h																																															
Name	Location	Value																																															
PCIe Controller 2 (Port 5-8)	Offset 0x155 [4:3] LP and H	0h																																															
Name	Location	Value																																															
PCIe Controller 3 (Port 9-12)	Offset 0x15D [4:3] LP and H	3h																																															
Name	Location	Value																																															
PCIe Controller 3 Lane Reversal	Offset 0x15D [2] LP and H	1h																																															
Name	Location	Value																																															
PCIe Controller 3 Lane Reversal	Offset 0x15D [2] LP and H	0h																																															



Test ID:	PSS_003								
b. 2x2 – two 2 lanes PCIe* Port.									
<table border="1"><thead><tr><th>Name</th><th>Location</th><th>Value</th></tr></thead><tbody><tr><td>PCIe Controller 3 (Port 9-12)</td><td>Offset 0x15D [4:3] LP and H</td><td>2h</td></tr></tbody></table>				Name	Location	Value	PCIe Controller 3 (Port 9-12)	Offset 0x15D [4:3] LP and H	2h
Name	Location	Value							
PCIe Controller 3 (Port 9-12)	Offset 0x15D [4:3] LP and H	2h							
c. 1x2, 2x1 – One 2 lanes PCIe* Port, Two 1 lane PCIe*.									
<table border="1"><thead><tr><th>Name</th><th>Location</th><th>Value</th></tr></thead><tbody><tr><td>PCIe Controller 3 (Port 9-12)</td><td>Offset 0x15D [4:3] LP and H</td><td>1h</td></tr></tbody></table>				Name	Location	Value	PCIe Controller 3 (Port 9-12)	Offset 0x15D [4:3] LP and H	1h
Name	Location	Value							
PCIe Controller 3 (Port 9-12)	Offset 0x15D [4:3] LP and H	1h							
4x1- One 1 lane PCIe** Port.									
<table border="1"><thead><tr><th>Name</th><th>Location</th><th>Value</th></tr></thead><tbody><tr><td>PCIe Controller 3 (Port 9-12)</td><td>Offset 0x15D [4:3] LP and H</td><td>0h</td></tr></tbody></table>				Name	Location	Value	PCIe Controller 3 (Port 9-12)	Offset 0x15D [4:3] LP and H	0h
Name	Location	Value							
PCIe Controller 3 (Port 9-12)	Offset 0x15D [4:3] LP and H	0h							
4. How do you have PCIe Controller 4 (Port 13-16) configured?									
a. 1x4 – One 4 lanes PCIe* Port.									
<table border="1"><thead><tr><th>Name</th><th>Location</th><th>Value</th></tr></thead><tbody><tr><td>PCIe Controller 4 (Port 13-16)</td><td>Offset 0x165 [4:3] LP and H</td><td>3h</td></tr></tbody></table>				Name	Location	Value	PCIe Controller 4 (Port 13-16)	Offset 0x165 [4:3] LP and H	3h
Name	Location	Value							
PCIe Controller 4 (Port 13-16)	Offset 0x165 [4:3] LP and H	3h							
i. Are the lanes reversed? — If reversed:									
<table border="1"><thead><tr><th>Name</th><th>Location</th><th>Value</th></tr></thead><tbody><tr><td>PCIe Controller 4 Lane Reversal</td><td>Offset 0x165 [2] LP and H</td><td>1h</td></tr></tbody></table>				Name	Location	Value	PCIe Controller 4 Lane Reversal	Offset 0x165 [2] LP and H	1h
Name	Location	Value							
PCIe Controller 4 Lane Reversal	Offset 0x165 [2] LP and H	1h							
— If NOT reversed:									
<table border="1"><thead><tr><th>Name</th><th>Location</th><th>Value</th></tr></thead><tbody><tr><td>PCIe Controller 4 Lane Reversal</td><td>Offset 0x165 [2] LP and H</td><td>0h</td></tr></tbody></table>				Name	Location	Value	PCIe Controller 4 Lane Reversal	Offset 0x165 [2] LP and H	0h
Name	Location	Value							
PCIe Controller 4 Lane Reversal	Offset 0x165 [2] LP and H	0h							
b. 2x2 – two 2 lanes PCIe* Port.									
<table border="1"><thead><tr><th>Name</th><th>Location</th><th>Value</th></tr></thead><tbody><tr><td>PCIe Controller 4 (Port 13-16)</td><td>Offset 0x165 [4:3] LP and H</td><td>2h</td></tr></tbody></table>				Name	Location	Value	PCIe Controller 4 (Port 13-16)	Offset 0x165 [4:3] LP and H	2h
Name	Location	Value							
PCIe Controller 4 (Port 13-16)	Offset 0x165 [4:3] LP and H	2h							
c. 1x2, 2x1 – One 2 lanes PCIe* Port, Two 1 lane PCIe* Port.									
<table border="1"><thead><tr><th>Name</th><th>Location</th><th>Value</th></tr></thead><tbody><tr><td>PCIe Controller 4 (Port 13-16)</td><td>Offset 0x165 [4:3] LP and H</td><td>1h</td></tr></tbody></table>				Name	Location	Value	PCIe Controller 4 (Port 13-16)	Offset 0x165 [4:3] LP and H	1h
Name	Location	Value							
PCIe Controller 4 (Port 13-16)	Offset 0x165 [4:3] LP and H	1h							
4x1- One 1 lane PCIe** Port.									
<table border="1"><thead><tr><th>Name</th><th>Location</th><th>Value</th></tr></thead><tbody><tr><td>PCIe Controller 4 (Port 13-16)</td><td>Offset 0x165 [4:3] LP and H</td><td>0h</td></tr></tbody></table>				Name	Location	Value	PCIe Controller 4 (Port 13-16)	Offset 0x165 [4:3] LP and H	0h
Name	Location	Value							
PCIe Controller 4 (Port 13-16)	Offset 0x165 [4:3] LP and H	0h							



Test ID:	PSS_003																																						
	<p>Comet Lake -H</p> <p>5. How do you have PCIe Controller 5 (Port 17-20) configured?</p> <p>a. 1x4 – One 4 lanes PCIe* Port.</p> <table border="1"> <thead> <tr> <th>Name</th> <th>Location</th> <th>Value</th> </tr> </thead> <tbody> <tr> <td>PCIe Controller 5 (Port 13-16)</td> <td>Offset 0x16D [4:3] H Only</td> <td>3h</td> </tr> </tbody> </table> <p>i. Are the lanes reversed? — If reversed:</p> <table border="1"> <thead> <tr> <th>Name</th> <th>Location</th> <th>Value</th> </tr> </thead> <tbody> <tr> <td>PCIe Controller 5 Lane Reversal</td> <td>Offset 0x16D [2] H Only</td> <td>1h</td> </tr> </tbody> </table> <p>— If NOT reversed:</p> <table border="1"> <thead> <tr> <th>Name</th> <th>Location</th> <th>Value</th> </tr> </thead> <tbody> <tr> <td>PCIe Controller 5 Lane Reversal</td> <td>Offset 0x16D [2] H Only</td> <td>0h</td> </tr> </tbody> </table> <p>b. 2x2 – two 2 lanes PCIe* Port.</p> <table border="1"> <thead> <tr> <th>Name</th> <th>Location</th> <th>Value</th> </tr> </thead> <tbody> <tr> <td>PCIe Controller 5 (Port 13-16)</td> <td>Offset 0x16D [4:3] H Only</td> <td>2h</td> </tr> </tbody> </table> <p>c. 1x2, 2x1 – One 2 lanes PCIe* Port, Two 1 lane PCIe* Port.</p> <table border="1"> <thead> <tr> <th>Name</th> <th>Location</th> <th>Value</th> </tr> </thead> <tbody> <tr> <td>PCIe Controller 5 (Port 13-16)</td> <td>Offset 0x16D [4:3] H Only</td> <td>1h</td> </tr> </tbody> </table> <p>4x1- One 1 lane PCIe** Port.</p> <table border="1"> <thead> <tr> <th>Name</th> <th>Location</th> <th>Value</th> </tr> </thead> <tbody> <tr> <td>PCIe Controller 5 (Port 13-16)</td> <td>Offset 0x16D [4:3] H Only</td> <td>0h</td> </tr> </tbody> </table>			Name	Location	Value	PCIe Controller 5 (Port 13-16)	Offset 0x16D [4:3] H Only	3h	Name	Location	Value	PCIe Controller 5 Lane Reversal	Offset 0x16D [2] H Only	1h	Name	Location	Value	PCIe Controller 5 Lane Reversal	Offset 0x16D [2] H Only	0h	Name	Location	Value	PCIe Controller 5 (Port 13-16)	Offset 0x16D [4:3] H Only	2h	Name	Location	Value	PCIe Controller 5 (Port 13-16)	Offset 0x16D [4:3] H Only	1h	Name	Location	Value	PCIe Controller 5 (Port 13-16)	Offset 0x16D [4:3] H Only	0h
Name	Location	Value																																					
PCIe Controller 5 (Port 13-16)	Offset 0x16D [4:3] H Only	3h																																					
Name	Location	Value																																					
PCIe Controller 5 Lane Reversal	Offset 0x16D [2] H Only	1h																																					
Name	Location	Value																																					
PCIe Controller 5 Lane Reversal	Offset 0x16D [2] H Only	0h																																					
Name	Location	Value																																					
PCIe Controller 5 (Port 13-16)	Offset 0x16D [4:3] H Only	2h																																					
Name	Location	Value																																					
PCIe Controller 5 (Port 13-16)	Offset 0x16D [4:3] H Only	1h																																					
Name	Location	Value																																					
PCIe Controller 5 (Port 13-16)	Offset 0x16D [4:3] H Only	0h																																					



Test ID:	PSS_003		
	Comet Lake -H		
	6. How do you have PCIe Controller 6 (Port 21-24) configured?		
	a. 1x4 – One 4 lanes PCIe* Port.		
	Name	Location	Value
	PCIe Controller 6 (Port 21-24)	Offset 0x175 [4:3] H Only	3h
	i. Are the lanes reversed?		
	— If reversed:		
	Name	Location	Value
	PCIe Controller 6 Lane Reversal	Offset 0x175 [2] H Only	1h
	— If NOT reversed:		
	Name	Location	Value
	PCIe Controller 6 Lane Reversal	Offset 0x175 [2] H Only	0h
b. 2x2 – two 2 lanes PCIe* Port.			
Name	Location	Value	
PCIe Controller 6 (Port 21-24)	Offset 0x175 [4:3] H Only	2h	
c. 1x2, 2x1 – One 2 lanes PCIe* Port, Two 1 lane PCIe* Port.			
Name	Location	Value	
PCIe Controller 6 (Port 21-24)	Offset 0x175 [4:3] H Only	1h	
4x1- One 1 lane PCIe** Port.			
Name	Location	Value	
PCIe Controller 6 (Port 21-24)	Offset 0x175 [4:3] H Only	0h	



Test ID:	PSS_003																																																
	<div>7. Does this platform use PCH PCIe port 1 as USB3 Port 1?<div>— If yes, PCH PCIe Port 1 configured as USB3</div><table><tr><th>Name</th><th>Location</th><th>Value</th></tr><tr><td>USB3 / PCIe Combo Port 0</td><td>Offset 0x1FA [1:0] LP Only</td><td>0h</td></tr></table><div>— If no, PCH PCIe Port 1 configured as PCIe</div><table><tr><th>Name</th><th>Location</th><th>Value</th></tr><tr><td>USB3 / PCIe Combo Port 0</td><td>Offset 0x1FA [1:0] LP Only</td><td>1h</td></tr></table></div> <div>8. Does this platform use PCH PCIe Port 2 as USB3 Port 2?<div>— If yes, PCH PCIe Port 2 configured as USB3</div><table><tr><th>Name</th><th>Location</th><th>Value</th></tr><tr><td>USB3 / PCIe Combo Port 1</td><td>Offset 0x1FA [3:2] LP Only</td><td>0h</td></tr></table><div>— If no, PCH PCIe Port 2 configured as PCIe</div><table><tr><th>Name</th><th>Location</th><th>Value</th></tr><tr><td>USB3 / PCIe Combo Port 1</td><td>Offset 0x1FA [3:2] LP Only</td><td>1h</td></tr></table></div> <div>9. Does this platform use PCH PCIe Port 3 as USB3 Port 3?<div>— If yes, PCH PCIe Port 3 configured as USB3</div><table><tr><th>Name</th><th>Location</th><th>Value</th></tr><tr><td>USB3 / PCIe Combo Port 2</td><td>Offset 0x1FA [5:4] LP Only</td><td>0h</td></tr></table><div>— If no, PCH PCIe Port 3 configured as PCIe</div><table><tr><th>Name</th><th>Location</th><th>Value</th></tr><tr><td>USB3 / PCIe Combo Port 2</td><td>Offset 0x1FA [5:4] LP Only</td><td>1h</td></tr></table></div> <div>10. Does this platform use PCH PCIe Port 4 as USB3 Port 4?<div>— If yes, PCH PCIe Port 4 configured as USB3</div><table><tr><th>Name</th><th>Location</th><th>Value</th></tr><tr><td>USB3 / PCIe Combo Port 3</td><td>Offset 0x1FA [7:6] LP Only</td><td>0h</td></tr></table><div>— If no, PCH PCIe Port 4 configured as PCIe</div><table><tr><th>Name</th><th>Location</th><th>Value</th></tr><tr><td>USB3 / PCIe Combo Port 3</td><td>Offset 0x1FA [7:6] LP Only</td><td>1h</td></tr></table></div>	Name	Location	Value	USB3 / PCIe Combo Port 0	Offset 0x1FA [1:0] LP Only	0h	Name	Location	Value	USB3 / PCIe Combo Port 0	Offset 0x1FA [1:0] LP Only	1h	Name	Location	Value	USB3 / PCIe Combo Port 1	Offset 0x1FA [3:2] LP Only	0h	Name	Location	Value	USB3 / PCIe Combo Port 1	Offset 0x1FA [3:2] LP Only	1h	Name	Location	Value	USB3 / PCIe Combo Port 2	Offset 0x1FA [5:4] LP Only	0h	Name	Location	Value	USB3 / PCIe Combo Port 2	Offset 0x1FA [5:4] LP Only	1h	Name	Location	Value	USB3 / PCIe Combo Port 3	Offset 0x1FA [7:6] LP Only	0h	Name	Location	Value	USB3 / PCIe Combo Port 3	Offset 0x1FA [7:6] LP Only	1h
Name	Location	Value																																															
USB3 / PCIe Combo Port 0	Offset 0x1FA [1:0] LP Only	0h																																															
Name	Location	Value																																															
USB3 / PCIe Combo Port 0	Offset 0x1FA [1:0] LP Only	1h																																															
Name	Location	Value																																															
USB3 / PCIe Combo Port 1	Offset 0x1FA [3:2] LP Only	0h																																															
Name	Location	Value																																															
USB3 / PCIe Combo Port 1	Offset 0x1FA [3:2] LP Only	1h																																															
Name	Location	Value																																															
USB3 / PCIe Combo Port 2	Offset 0x1FA [5:4] LP Only	0h																																															
Name	Location	Value																																															
USB3 / PCIe Combo Port 2	Offset 0x1FA [5:4] LP Only	1h																																															
Name	Location	Value																																															
USB3 / PCIe Combo Port 3	Offset 0x1FA [7:6] LP Only	0h																																															
Name	Location	Value																																															
USB3 / PCIe Combo Port 3	Offset 0x1FA [7:6] LP Only	1h																																															



Test ID:	PSS_003	
11. Does this platform use PCH PCIe Port 5 as USB3 Port 5? — If yes, PCH PCIe Port 5 configured as USB3		
Name	Location	Value
USB3 / PCIe Combo Port 4	Offset 0x1FF [5:4] LP Only	0h
— If no, PCH PCIe Port 5 configured as PCIe		
Name	Location	Value
USB3 / PCIe Combo Port 4	Offset 0x1FF [5:4] LP Only	1h
12. Does this platform use PCH PCIe Port 6 as USB3 Port 6? — If yes, PCH PCIe Port 6 configured as USB3		
Name	Location	Value
USB3 / PCIe Combo Port 5	Offset 0x1FF [7:6] LP Only	0h
— If no, PCH PCIe Port 6 configured as PCIe		
Name	Location	Value
USB3 / PCIe Combo Port 5	Offset 0x1FF [7:6]	1h
Comet Lake -H		
13. Does this platform use PCH PCIe Port 1 as USB3 Port 7? — If yes, PCH PCIe Port 1 configured as USB3		
Name	Location	Value
USB3 / PCIe Combo Port 1	Offset 0x23C [3:0] H Only	1h
— If no, PCH PCIe Port 1 configured as PCIe		
Name	Location	Value
USB3 / PCIe Combo Port 1	Offset 0x23C [3:0] H Only	5h
14. Does this platform use PCH PCIe Port 2 as USB3 Port 8? — If yes, PCH PCIe Port 2 configured as USB3		
Name	Location	Value
USB3 / PCIe Combo Port 2	Offset 0x23C [7:4] H Only	1h
— If no, PCH PCIe Port 2 configured as PCIe		
Name	Location	Value
USB3 / PCIe Combo Port 2	Offset 0x23C [7:4] H Only	5h



Test ID:	PSS_003																								
	<div>15. Does this platform use PCH PCIe Port 3 as USB3 Port 9? — If yes, PCH PCIe Port 3 configured as USB3</div> <table><tr><th>Name</th><th>Location</th><th>Value</th></tr><tr><td>USB3 / PCIe Combo Port 3</td><td>Offset 0x23D [3:0] H Only</td><td>1h</td></tr></table> <div>— If no, PCH PCIe Port 5 configured as PCIe</div> <table><tr><th>Name</th><th>Location</th><th>Value</th></tr><tr><td>USB3 / PCIe Combo Port 3</td><td>Offset 0x23D [3:0] H Only</td><td>5h</td></tr></table> <div>16. Does this platform use PCH PCIe Port 4 as USB3 Port 10? — If yes, PCH PCIe Port 4 configured as USB3</div> <table><tr><th>Name</th><th>Location</th><th>Value</th></tr><tr><td>USB3 / PCIe Combo Port 4</td><td>Offset 0x23D [7:4] H Only</td><td>1h</td></tr></table> <div>— If no, PCH PCIe Port 6 configured as PCIe</div> <table><tr><th>Name</th><th>Location</th><th>Value</th></tr><tr><td>USB3 / PCIe Combo Port 4</td><td>Offset 0x23D [7:4] H Only</td><td>5h</td></tr></table>	Name	Location	Value	USB3 / PCIe Combo Port 3	Offset 0x23D [3:0] H Only	1h	Name	Location	Value	USB3 / PCIe Combo Port 3	Offset 0x23D [3:0] H Only	5h	Name	Location	Value	USB3 / PCIe Combo Port 4	Offset 0x23D [7:4] H Only	1h	Name	Location	Value	USB3 / PCIe Combo Port 4	Offset 0x23D [7:4] H Only	5h
Name	Location	Value																							
USB3 / PCIe Combo Port 3	Offset 0x23D [3:0] H Only	1h																							
Name	Location	Value																							
USB3 / PCIe Combo Port 3	Offset 0x23D [3:0] H Only	5h																							
Name	Location	Value																							
USB3 / PCIe Combo Port 4	Offset 0x23D [7:4] H Only	1h																							
Name	Location	Value																							
USB3 / PCIe Combo Port 4	Offset 0x23D [7:4] H Only	5h																							
Test Pass/Fail Criteria:	Test passes if SoftStraps/register setting in this step matches to the configuration in the target system.																								



Test ID:	PSS_003							
Comet Lake -LP								
1. How is SATA / PCIe* Combo Port 0 Strap configured on the platform?								
i. Statically assigned to SATA Port 0.								
<table><tr><th>Name</th><th>Location</th><th>Value</th></tr><tr><td>SATA / PCIe Combo Port 0 Strap</td><td>Offset 0x1F5 [1:0] LP Only</td><td>0h</td></tr></table>	Name	Location	Value	SATA / PCIe Combo Port 0 Strap	Offset 0x1F5 [1:0] LP Only	0h		
Name	Location	Value						
SATA / PCIe Combo Port 0 Strap	Offset 0x1F5 [1:0] LP Only	0h						
Caution: Selecting PCIe* / SATA Combo Port 0 Strap as SATA Port 0 means that all 4 Lanes of PCIe* Port 11 are no longer available. PCIe* Port 11 Lanes 1 thru 3 cannot be selected as individual PCIe* ports.								
ii. Statically assigned to PCIe* Port 11.								
<table><tr><th>Name</th><th>Location</th><th>Value</th></tr><tr><td>SATA / PCIe Combo Port 0 Strap</td><td>Offset 0x1F5 [1:0] LP Only</td><td>1h</td></tr></table>	Name	Location	Value	SATA / PCIe Combo Port 0 Strap	Offset 0x1F5 [1:0] LP Only	1h		
Name	Location	Value						
SATA / PCIe Combo Port 0 Strap	Offset 0x1F5 [1:0] LP Only	1h						
iii. Assigned based on the native mode of GPP_E0 pin.								
<table><tr><th>Name</th><th>Location</th><th>Value</th></tr><tr><td>SATA / PCIe Combo Port 0 Strap</td><td>Offset 0x1F5 [1:0] LP Only</td><td>3h</td></tr></table>	Name	Location	Value	SATA / PCIe Combo Port 0 Strap	Offset 0x1F5 [1:0] LP Only	3h		
Name	Location	Value						
SATA / PCIe Combo Port 0 Strap	Offset 0x1F5 [1:0] LP Only	3h						
2. How is SATA / PCIe* Combo Port 1 Strap configured on the platform?								
i. Statically assigned to SATA Port 1a.								
<table><tr><th>Name</th><th>Location</th><th>Value</th></tr><tr><td>SATA / PCIe Combo Port 1 Strap</td><td>Offset 0x1F5 [3:2] LP Only</td><td>0h</td></tr></table>	Name	Location	Value	SATA / PCIe Combo Port 1 Strap	Offset 0x1F5 [3:2] LP Only	0h		
Name	Location	Value						
SATA / PCIe Combo Port 1 Strap	Offset 0x1F5 [3:2] LP Only	0h						
ii. Statically assigned to PCIe* Port 12.								
<table><tr><th>Name</th><th>Location</th><th>Value</th></tr><tr><td>SATA / PCIe Combo Port 1 Strap</td><td>Offset 0x1F5 [3:2] LP Only</td><td>1h</td></tr></table>	Name	Location	Value	SATA / PCIe Combo Port 1 Strap	Offset 0x1F5 [3:2] LP Only	1h		
Name	Location	Value						
SATA / PCIe Combo Port 1 Strap	Offset 0x1F5 [3:2] LP Only	1h						
iii. Assigned based on the native mode of GPP_E1 pin.								
<table><tr><th>Name</th><th>Location</th><th>Value</th></tr><tr><td>SATA / PCIe Combo Port 1 Strap</td><td>Offset 0x1F5 [3:2] LP Only</td><td>3h</td></tr></table>	Name	Location	Value	SATA / PCIe Combo Port 1 Strap	Offset 0x1F5 [3:2] LP Only	3h		
Name	Location	Value						
SATA / PCIe Combo Port 1 Strap	Offset 0x1F5 [3:2] LP Only	3h						
3. How is SATA / PCIe* Combo Port 2 Strap configured on the platform?								
i. Statically assigned to SATA Port 1b (Comet Lake -U Only).								
<table><tr><th>Name</th><th>Location</th><th>Value</th></tr><tr><td>SATA / PCIe Combo Port 2 Strap</td><td>Offset 0x1F5 [5:4] LP Only</td><td>0h</td></tr></table>	Name	Location	Value	SATA / PCIe Combo Port 2 Strap	Offset 0x1F5 [5:4] LP Only	0h		
Name	Location	Value						
SATA / PCIe Combo Port 2 Strap	Offset 0x1F5 [5:4] LP Only	0h						
ii. Statically assigned to PCIe* Port 15.								
<table><tr><th>Name</th><th>Location</th><th>Value</th></tr><tr><td>SATA / PCIe Combo Port 2 Strap</td><td>Offset 0x1F5 [5:4] LP Only</td><td>1h</td></tr></table>	Name	Location	Value	SATA / PCIe Combo Port 2 Strap	Offset 0x1F5 [5:4] LP Only	1h		
Name	Location	Value						
SATA / PCIe Combo Port 2 Strap	Offset 0x1F5 [5:4] LP Only	1h						
iii. Assigned based on the native mode of GPP_E2 pin.								
<table><tr><th>Name</th><th>Location</th><th>Value</th></tr><tr><td>SATA / PCIe Combo Port 2 Strap</td><td>Offset 0x1F5 [5:4] LP Only</td><td>3h</td></tr></table>	Name	Location	Value	SATA / PCIe Combo Port 2 Strap	Offset 0x1F5 [5:4] LP Only	3h		
Name	Location	Value						
SATA / PCIe Combo Port 2 Strap	Offset 0x1F5 [5:4] LP Only	3h						



Test ID:	PSS_003								
	4. How is SATA / PCIe* Combo Port 3 Strap configured on the platform?								
	i. Statically assigned to SATA Port 2 (Comet Lake -U Only).								
	<table><tr><th>Name</th><th>Location</th><th>Value</th></tr><tr><td>SATA / PCIe Combo Port 3 Strap</td><td>Offset 0x1F8 [1:0] LP Only</td><td>0h</td></tr></table>	Name	Location	Value	SATA / PCIe Combo Port 3 Strap	Offset 0x1F8 [1:0] LP Only	0h		
	Name	Location	Value						
	SATA / PCIe Combo Port 3 Strap	Offset 0x1F8 [1:0] LP Only	0h						
	ii. Statically assigned to PCIe* Port 16.								
	<table><tr><th>Name</th><th>Location</th><th>Value</th></tr><tr><td>SATA / PCIe Combo Port 3 Strap</td><td>Offset 0x1F8 [1:0] LP Only</td><td>1h</td></tr></table>	Name	Location	Value	SATA / PCIe Combo Port 3 Strap	Offset 0x1F8 [1:0] LP Only	1h		
	Name	Location	Value						
	SATA / PCIe Combo Port 3 Strap	Offset 0x1F8 [1:0] LP Only	1h						
	iii. Assigned based on the native mode of GPP_E0 pin.								
<table><tr><th>Name</th><th>Location</th><th>Value</th></tr><tr><td>SATA / PCIe Combo Port 3 Strap</td><td>Offset 0x1F8 [1:0] LP Only</td><td>3h</td></tr></table>	Name	Location	Value	SATA / PCIe Combo Port 3 Strap	Offset 0x1F8 [1:0] LP Only	3h			
Name	Location	Value							
SATA / PCIe Combo Port 3 Strap	Offset 0x1F8 [1:0] LP Only	3h							



Test ID:	PSS_003								
	Comet Lake -H								
	1. How is SATA / PCIe* Combo Port 0 Strap configured on the platform?								
	i. Statically assigned to SATA Port 0a.								
	<table><tr><th>Name</th><th>Location</th><th>Value</th></tr><tr><td>SATA / PCIe Combo Port 0 Strap</td><td>Offset 245 [3:0] H Only</td><td>7h</td></tr></table>	Name	Location	Value	SATA / PCIe Combo Port 0 Strap	Offset 245 [3:0] H Only	7h		
	Name	Location	Value						
	SATA / PCIe Combo Port 0 Strap	Offset 245 [3:0] H Only	7h						
	ii. Statically assigned to PCIe* Port 11.								
	<table><tr><th>Name</th><th>Location</th><th>Value</th></tr><tr><td>SATA / PCIe Combo Port 0 Strap</td><td>Offset 245 [3:0] H Only</td><td>5h</td></tr></table>	Name	Location	Value	SATA / PCIe Combo Port 0 Strap	Offset 245 [3:0] H Only	5h		
	Name	Location	Value						
	SATA / PCIe Combo Port 0 Strap	Offset 245 [3:0] H Only	5h						
	iii. Assigned to PCIe based on the native mode of GPP_E0 pin.								
	<table><tr><th>Name</th><th>Location</th><th>Value</th></tr><tr><td>SATA / PCIe Combo Port 0 Strap</td><td>Offset 245 [3:0] H Only</td><td>Ch</td></tr></table>	Name	Location	Value	SATA / PCIe Combo Port 0 Strap	Offset 245 [3:0] H Only	Ch		
	Name	Location	Value						
	SATA / PCIe Combo Port 0 Strap	Offset 245 [3:0] H Only	Ch						
	iv. Assigned to SATA based on the native mode of GPP_E0 pin.								
	<table><tr><th>Name</th><th>Location</th><th>Value</th></tr><tr><td>SATA / PCIe Combo Port 0 Strap</td><td>Offset 245 [3:0] H Only</td><td>Dh</td></tr></table>	Name	Location	Value	SATA / PCIe Combo Port 0 Strap	Offset 245 [3:0] H Only	Dh		
	Name	Location	Value						
	SATA / PCIe Combo Port 0 Strap	Offset 245 [3:0] H Only	Dh						
	2. How is SATA / PCIe* Combo Port 1 Strap configured on the platform?								
	i. Statically assigned to SATA Port 1a.								
<table><tr><th>Name</th><th>Location</th><th>Value</th></tr><tr><td>SATA / PCIe Combo Port 1 Strap</td><td>Offset 245 [7:4] H Only</td><td>7h</td></tr></table>	Name	Location	Value	SATA / PCIe Combo Port 1 Strap	Offset 245 [7:4] H Only	7h			
Name	Location	Value							
SATA / PCIe Combo Port 1 Strap	Offset 245 [7:4] H Only	7h							
ii. Statically assigned to PCIe* Port 12.									
<table><tr><th>Name</th><th>Location</th><th>Value</th></tr><tr><td>SATA / PCIe Combo Port 1 Strap</td><td>Offset 245 [7:4] H Only</td><td>5h</td></tr></table>	Name	Location	Value	SATA / PCIe Combo Port 1 Strap	Offset 245 [7:4] H Only	5h			
Name	Location	Value							
SATA / PCIe Combo Port 1 Strap	Offset 245 [7:4] H Only	5h							
iii. Assigned to PCIe based on the native mode of GPP_E1 pin.									
<table><tr><th>Name</th><th>Location</th><th>Value</th></tr><tr><td>SATA / PCIe Combo Port 1 Strap</td><td>Offset 245 [7:4] H Only</td><td>Ch</td></tr></table>	Name	Location	Value	SATA / PCIe Combo Port 1 Strap	Offset 245 [7:4] H Only	Ch			
Name	Location	Value							
SATA / PCIe Combo Port 1 Strap	Offset 245 [7:4] H Only	Ch							
iv. Assigned to SATA based on the native mode of GPP_E1 pin.									
<table><tr><th>Name</th><th>Location</th><th>Value</th></tr><tr><td>SATA / PCIe Combo Port 1 Strap</td><td>Offset 245 [7:4] H Only</td><td>Dh</td></tr></table>	Name	Location	Value	SATA / PCIe Combo Port 1 Strap	Offset 245 [7:4] H Only	Dh			
Name	Location	Value							
SATA / PCIe Combo Port 1 Strap	Offset 245 [7:4] H Only	Dh							
v. Assigned as GbE through GbE PCIe Port Select									
<table><tr><th>Name</th><th>Location</th><th>Value</th></tr><tr><td>SATA / PCIe Combo Port 1 Strap</td><td>Offset 245 [7:4] H Only</td><td>8h</td></tr></table>	Name	Location	Value	SATA / PCIe Combo Port 1 Strap	Offset 245 [7:4] H Only	8h			
Name	Location	Value							
SATA / PCIe Combo Port 1 Strap	Offset 245 [7:4] H Only	8h							



Test ID:	PSS_003																																																						
	<div>Comet Lake -H</div> <div>3. How is SATA / PCIe* Combo Port 2 Strap configured on the platform?</div> <div><div>i. Statically assigned to SATA Port 0b.</div><table><tr><th>Name</th><th>Location</th><th>Value</th></tr><tr><td>SATA / PCIe Combo Port 0 Strap</td><td>Offset 246 [3:0] H Only</td><td>7h</td></tr></table></div> <div><div>ii. Statically assigned to PCIe* Port 13.</div><table><tr><th>Name</th><th>Location</th><th>Value</th></tr><tr><td>SATA / PCIe Combo Port 0 Strap</td><td>Offset 246 [3:0] H Only</td><td>5h</td></tr></table></div> <div><div>iii. Assigned to PCIe based on the native mode of GPP_E0 pin.</div><table><tr><th>Name</th><th>Location</th><th>Value</th></tr><tr><td>SATA / PCIe Combo Port 0 Strap</td><td>Offset 246 [3:0] H Only</td><td>Ch</td></tr></table></div> <div><div>iv. Assigned to SATA based on the native mode of GPP_E0 pin.</div><table><tr><th>Name</th><th>Location</th><th>Value</th></tr><tr><td>SATA / PCIe Combo Port 0 Strap</td><td>Offset 246 [3:0] H Only</td><td>Dh</td></tr></table></div> <div><div>v. Assigned as GbE through GbE PCIe Port Select</div><table><tr><th>Name</th><th>Location</th><th>Value</th></tr><tr><td>SATA / PCIe Combo Port 0 Strap</td><td>Offset 246 [3:0] H Only</td><td>8h</td></tr></table></div> <div>4. How is SATA / PCIe* Combo Port 3 Strap configured on the platform?</div> <div><div>i. Statically assigned to SATA Port 1b.</div><table><tr><th>Name</th><th>Location</th><th>Value</th></tr><tr><td>SATA / PCIe Combo Port 1 Strap</td><td>Offset 246 [7:4] H Only</td><td>7h</td></tr></table></div> <div><div>ii. Statically assigned to PCIe* Port 14.</div><table><tr><th>Name</th><th>Location</th><th>Value</th></tr><tr><td>SATA / PCIe Combo Port 1 Strap</td><td>Offset 246 [7:4] H Only</td><td>5h</td></tr></table></div> <div><div>iii. Assigned to PCIe based on the native mode of GPP_E1 pin.</div><table><tr><th>Name</th><th>Location</th><th>Value</th></tr><tr><td>SATA / PCIe Combo Port 1 Strap</td><td>Offset 246 [7:4] H Only</td><td>Ch</td></tr></table></div> <div><div>iv. Assigned to SATA based on the native mode of GPP_E1 pin.</div><table><tr><th>Name</th><th>Location</th><th>Value</th></tr><tr><td>SATA / PCIe Combo Port 1 Strap</td><td>Offset 246 [7:4] H Only</td><td>Dh</td></tr></table></div>	Name	Location	Value	SATA / PCIe Combo Port 0 Strap	Offset 246 [3:0] H Only	7h	Name	Location	Value	SATA / PCIe Combo Port 0 Strap	Offset 246 [3:0] H Only	5h	Name	Location	Value	SATA / PCIe Combo Port 0 Strap	Offset 246 [3:0] H Only	Ch	Name	Location	Value	SATA / PCIe Combo Port 0 Strap	Offset 246 [3:0] H Only	Dh	Name	Location	Value	SATA / PCIe Combo Port 0 Strap	Offset 246 [3:0] H Only	8h	Name	Location	Value	SATA / PCIe Combo Port 1 Strap	Offset 246 [7:4] H Only	7h	Name	Location	Value	SATA / PCIe Combo Port 1 Strap	Offset 246 [7:4] H Only	5h	Name	Location	Value	SATA / PCIe Combo Port 1 Strap	Offset 246 [7:4] H Only	Ch	Name	Location	Value	SATA / PCIe Combo Port 1 Strap	Offset 246 [7:4] H Only	Dh
Name	Location	Value																																																					
SATA / PCIe Combo Port 0 Strap	Offset 246 [3:0] H Only	7h																																																					
Name	Location	Value																																																					
SATA / PCIe Combo Port 0 Strap	Offset 246 [3:0] H Only	5h																																																					
Name	Location	Value																																																					
SATA / PCIe Combo Port 0 Strap	Offset 246 [3:0] H Only	Ch																																																					
Name	Location	Value																																																					
SATA / PCIe Combo Port 0 Strap	Offset 246 [3:0] H Only	Dh																																																					
Name	Location	Value																																																					
SATA / PCIe Combo Port 0 Strap	Offset 246 [3:0] H Only	8h																																																					
Name	Location	Value																																																					
SATA / PCIe Combo Port 1 Strap	Offset 246 [7:4] H Only	7h																																																					
Name	Location	Value																																																					
SATA / PCIe Combo Port 1 Strap	Offset 246 [7:4] H Only	5h																																																					
Name	Location	Value																																																					
SATA / PCIe Combo Port 1 Strap	Offset 246 [7:4] H Only	Ch																																																					
Name	Location	Value																																																					
SATA / PCIe Combo Port 1 Strap	Offset 246 [7:4] H Only	Dh																																																					



Test ID:	PSS_003						
	Comet Lake -H						
	5. How is SATA / PCIe* Combo Port 4 Strap configured on the platform?						
	i. Statically assigned to SATA Port 2.						
	<table><tr><th>Name</th><th>Location</th><th>Value</th></tr><tr><td>SATA / PCIe Combo Port 0 Strap</td><td>Offset 247 [3:0] H Only</td><td>7h</td></tr></table>	Name	Location	Value	SATA / PCIe Combo Port 0 Strap	Offset 247 [3:0] H Only	7h
	Name	Location	Value				
	SATA / PCIe Combo Port 0 Strap	Offset 247 [3:0] H Only	7h				
	ii. Statically assigned to PCIe* Port 15.						
	<table><tr><th>Name</th><th>Location</th><th>Value</th></tr><tr><td>SATA / PCIe Combo Port 0 Strap</td><td>Offset 247 [3:0] H Only</td><td>5h</td></tr></table>	Name	Location	Value	SATA / PCIe Combo Port 0 Strap	Offset 247 [3:0] H Only	5h
	Name	Location	Value				
	SATA / PCIe Combo Port 0 Strap	Offset 247 [3:0] H Only	5h				
	iii. Assigned to PCIe based on the native mode of GPP_E2 pin.						
	<table><tr><th>Name</th><th>Location</th><th>Value</th></tr><tr><td>SATA / PCIe Combo Port 0 Strap</td><td>Offset 247 [3:0] H Only</td><td>Ch</td></tr></table>	Name	Location	Value	SATA / PCIe Combo Port 0 Strap	Offset 247 [3:0] H Only	Ch
	Name	Location	Value				
	SATA / PCIe Combo Port 0 Strap	Offset 247 [3:0] H Only	Ch				
	iv. Assigned to SATA based on the native mode of GPP_E2 pin.						
	<table><tr><th>Name</th><th>Location</th><th>Value</th></tr><tr><td>SATA / PCIe Combo Port 0 Strap</td><td>Offset 247 [3:0] H Only</td><td>Dh</td></tr></table>	Name	Location	Value	SATA / PCIe Combo Port 0 Strap	Offset 247 [3:0] H Only	Dh
	Name	Location	Value				
SATA / PCIe Combo Port 0 Strap	Offset 247 [3:0] H Only	Dh					
6. How is SATA / PCIe* Combo Port 5Strap configured on the platform?							
i. Statically assigned to SATA Port 3.							
<table><tr><th>Name</th><th>Location</th><th>Value</th></tr><tr><td>SATA / PCIe Combo Port 1 Strap</td><td>Offset 247 [7:4] H Only</td><td>7h</td></tr></table>	Name	Location	Value	SATA / PCIe Combo Port 1 Strap	Offset 247 [7:4] H Only	7h	
Name	Location	Value					
SATA / PCIe Combo Port 1 Strap	Offset 247 [7:4] H Only	7h					
ii. Statically assigned to PCIe* Port 16.							
<table><tr><th>Name</th><th>Location</th><th>Value</th></tr><tr><td>SATA / PCIe Combo Port 1 Strap</td><td>Offset 247 [7:4] H Only</td><td>5h</td></tr></table>	Name	Location	Value	SATA / PCIe Combo Port 1 Strap	Offset 247 [7:4] H Only	5h	
Name	Location	Value					
SATA / PCIe Combo Port 1 Strap	Offset 247 [7:4] H Only	5h					
iii. Assigned to PCIe based on the native mode of GPP_E3 pin.							
<table><tr><th>Name</th><th>Location</th><th>Value</th></tr><tr><td>SATA / PCIe Combo Port 1 Strap</td><td>Offset 247 [7:4] H Only</td><td>Ch</td></tr></table>	Name	Location	Value	SATA / PCIe Combo Port 1 Strap	Offset 247 [7:4] H Only	Ch	
Name	Location	Value					
SATA / PCIe Combo Port 1 Strap	Offset 247 [7:4] H Only	Ch					
iv. Assigned to SATA based on the native mode of GPP_E3 pin.							
<table><tr><th>Name</th><th>Location</th><th>Value</th></tr><tr><td>SATA / PCIe Combo Port 1 Strap</td><td>Offset 247 [7:4] H Only</td><td>Dh</td></tr></table>	Name	Location	Value	SATA / PCIe Combo Port 1 Strap	Offset 247 [7:4] H Only	Dh	
Name	Location	Value					
SATA / PCIe Combo Port 1 Strap	Offset 247 [7:4] H Only	Dh					
Test Pass/Fail Criteria:	Test passes if SoftStraps/register setting in this step matches to the configuration in the target system.						



21.5 BIOS Boot-Block Size Test

Test ID:	PSS_004																															
Test Case Title:	BIOS Boot-Block size Test																															
Mandatory/Optional:	Mandatory																															
Description:	BIOS Boot-Block size deals with a BIOS recovery mechanism. If this is not set correctly, then BIOS boot-block recovery mechanism would not work.																															
Objective:	To verify BIOS boot-block size of correctly setup.																															
Procedure:	<p>Boot to targeted OS. Verify correct configuration of the PCH SoftStraps below:</p> <p>1. What size is the SPI flash BIOS boot block?</p> <p>a. If 64KB</p> <table border="1"> <thead> <tr> <th>Name</th><th>Location</th><th>Value</th></tr> </thead> <tbody> <tr> <td>Top Swap Block size</td><td>Offset 0x138 [6:4] LP and H</td><td>0h</td></tr> </tbody> </table> <p>b. 128KB</p> <table border="1"> <thead> <tr> <th>Name</th><th>Location</th><th>Value</th></tr> </thead> <tbody> <tr> <td>Top Swap Block size</td><td>Offset 0x138 [6:4] LP and H</td><td>1h</td></tr> </tbody> </table> <p>c. 256KB</p> <table border="1"> <thead> <tr> <th>Name</th><th>Location</th><th>Value</th></tr> </thead> <tbody> <tr> <td>Top Swap Block size</td><td>Offset 0x138 [6:4] LP and H</td><td>2h</td></tr> </tbody> </table> <p>d. 512KB</p> <table border="1"> <thead> <tr> <th>Name</th><th>Location</th><th>Value</th></tr> </thead> <tbody> <tr> <td>Top Swap Block size</td><td>Offset 0x138 [6:4] LP and H</td><td>3h</td></tr> </tbody> </table> <p>e. 1MB</p> <table border="1"> <thead> <tr> <th>Name</th><th>Location</th><th>Value</th></tr> </thead> <tbody> <tr> <td>Top Swap Block size</td><td>Offset 0x138 [6:4] LP and H</td><td>4h</td></tr> </tbody> </table>		Name	Location	Value	Top Swap Block size	Offset 0x138 [6:4] LP and H	0h	Name	Location	Value	Top Swap Block size	Offset 0x138 [6:4] LP and H	1h	Name	Location	Value	Top Swap Block size	Offset 0x138 [6:4] LP and H	2h	Name	Location	Value	Top Swap Block size	Offset 0x138 [6:4] LP and H	3h	Name	Location	Value	Top Swap Block size	Offset 0x138 [6:4] LP and H	4h
Name	Location	Value																														
Top Swap Block size	Offset 0x138 [6:4] LP and H	0h																														
Name	Location	Value																														
Top Swap Block size	Offset 0x138 [6:4] LP and H	1h																														
Name	Location	Value																														
Top Swap Block size	Offset 0x138 [6:4] LP and H	2h																														
Name	Location	Value																														
Top Swap Block size	Offset 0x138 [6:4] LP and H	3h																														
Name	Location	Value																														
Top Swap Block size	Offset 0x138 [6:4] LP and H	4h																														
Test Pass/Fail Criteria:	Test passes if SoftStraps/register setting in this step matches to the configuration in the target system.																															



21.6 Intel® CSME SMBus Alert Sending Device (ASD) Address Test

Test ID:	PSS_005												
Test Case Title:	Intel® CSME SMBus Alert Sending Device (ASD) Address Test												
Mandatory/Optional:	Mandatory for target system with Intel® AMT.												
Description:	This field is only applicable if there is an ASD attached to SMBus and using Intel® AMT.												
Objective:	To verify Intel® CSME SMBus ASD enable and address bits are correctly configure.												
Procedure:	Boot to targeted OS. Verify correct configuration of the PCH SoftStraps below:												
	1. Is there an Alert Sending Device (ASD) on Host SMBus?												
	Note: This is only valid for Intel® AMT enabled platforms (Refer SPI Programming Guide for more information)												
	— If YES,												
	<table><tr><th>Name</th><th>Location</th><th>Value</th></tr><tr><td>Intel® CSME SMBus ASD Address</td><td>Offset 0x178 [6:0] LP Offset 0x188 [6:0] H</td><td>Refer details in ¹SPI Programming Guide</td></tr><tr><td>Intel® CSME SMBus ASD Address Enable</td><td>Offset 0x17B [0] LP Offset 0x18B [0] H</td><td>1h</td></tr><tr><td>Intel® CSME SMBus Subsystem Device ID for ASF</td><td>Offset 0x17E [31:0] LP Offset 0x18E [31:0] H</td><td>Refer details in ²SPI Programming Guide</td></tr></table>	Name	Location	Value	Intel® CSME SMBus ASD Address	Offset 0x178 [6:0] LP Offset 0x188 [6:0] H	Refer details in ¹ SPI Programming Guide	Intel® CSME SMBus ASD Address Enable	Offset 0x17B [0] LP Offset 0x18B [0] H	1h	Intel® CSME SMBus Subsystem Device ID for ASF	Offset 0x17E [31:0] LP Offset 0x18E [31:0] H	Refer details in ² SPI Programming Guide
	Name	Location	Value										
	Intel® CSME SMBus ASD Address	Offset 0x178 [6:0] LP Offset 0x188 [6:0] H	Refer details in ¹ SPI Programming Guide										
	Intel® CSME SMBus ASD Address Enable	Offset 0x17B [0] LP Offset 0x18B [0] H	1h										
	Intel® CSME SMBus Subsystem Device ID for ASF	Offset 0x17E [31:0] LP Offset 0x18E [31:0] H	Refer details in ² SPI Programming Guide										
	— If NO,												
<table><tr><th>Name</th><th>Location</th><th>Value</th></tr><tr><td>Intel® CSME SMBus ASD Address</td><td>Offset 0x178 [6:0] LP Offset 0x188 [6:0] H</td><td>0h</td></tr><tr><td>Intel® CSME SMBus ASD Address Enable</td><td>Offset 0x17B [0] LP Offset 0x18B [0] H</td><td>0h</td></tr><tr><td>Intel® CSME SMBus Subsystem Device ID for ASF</td><td>Offset 0x17E [31:0] LP Offset 0x18E [31:0] H</td><td>0h</td></tr></table>	Name	Location	Value	Intel® CSME SMBus ASD Address	Offset 0x178 [6:0] LP Offset 0x188 [6:0] H	0h	Intel® CSME SMBus ASD Address Enable	Offset 0x17B [0] LP Offset 0x18B [0] H	0h	Intel® CSME SMBus Subsystem Device ID for ASF	Offset 0x17E [31:0] LP Offset 0x18E [31:0] H	0h	
Name	Location	Value											
Intel® CSME SMBus ASD Address	Offset 0x178 [6:0] LP Offset 0x188 [6:0] H	0h											
Intel® CSME SMBus ASD Address Enable	Offset 0x17B [0] LP Offset 0x18B [0] H	0h											
Intel® CSME SMBus Subsystem Device ID for ASF	Offset 0x17E [31:0] LP Offset 0x18E [31:0] H	0h											
Note:													
¹ Intel® CSME SMBus Alert Sending Device (ASD) Address (MESMASDA) address must be Non-zero, unique address on the Host SMBus segment, and compatible with the master on SMBus.													
² Intel® CSME SMBus Subsystem Vendor and Device ID.													
Test Pass/Fail Criteria:	Test passes if SoftStraps/register setting in this step matches to the configuration in the target system.												



21.7 Power State Deep Sx Test

Test ID:	PSS_007						
Test Case Title:	Power State Deep Sx Test						
Mandatory/Optional:	Mandatory						
Description:	To minimize power consumption while in S3/S4/S5, the PCH supports a lower power, lower featured version of these power states known as Deep Sx. In the Deep Sx state, the Suspend wells are powered off, while the Deep Sx Well (DSW) remains powered. A limited set of wake events are supported by the logic located in the DSW. The Deep Sx capability and the SUSPWRDNACK pin functionality are mutually exclusive.						
Objective:	To verify correct configuration of Power State Deep Sx.						
Procedure:	Boot to targeted OS. Verify correct configuration of the PCH SoftStraps below:						
	1. Does the platform support power state Deep Sx? — If YES:						
	<table><tr><th>Name</th><th>Location</th><th>Value</th></tr><tr><td>Deep Sx Enable</td><td>Offset 0x170 [20] LP Offset 0xC14 [20]</td><td>1h 1h</td></tr></table>	Name	Location	Value	Deep Sx Enable	Offset 0x170 [20] LP Offset 0xC14 [20]	1h 1h
	Name	Location	Value				
	Deep Sx Enable	Offset 0x170 [20] LP Offset 0xC14 [20]	1h 1h				
	<table><tr><th>Name</th><th>Location</th><th>Value</th></tr><tr><td>Deep Sx Enable</td><td>Offset 0x180 [20] H Offset 0xC14 [20]</td><td>1h 1h</td></tr></table>	Name	Location	Value	Deep Sx Enable	Offset 0x180 [20] H Offset 0xC14 [20]	1h 1h
	Name	Location	Value				
	Deep Sx Enable	Offset 0x180 [20] H Offset 0xC14 [20]	1h 1h				
	— If NO,						
	<table><tr><th>Name</th><th>Location</th><th>Value</th></tr><tr><td>Deep Sx Enable</td><td>Offset 0x180 [20] LP Offset 0xC14 [20]</td><td>0h 0h</td></tr></table>	Name	Location	Value	Deep Sx Enable	Offset 0x180 [20] LP Offset 0xC14 [20]	0h 0h
Name	Location	Value					
Deep Sx Enable	Offset 0x180 [20] LP Offset 0xC14 [20]	0h 0h					
<table><tr><th>Name</th><th>Location</th><th>Value</th></tr><tr><td>Deep Sx Enable</td><td>Offset 0x180 [20] H Offset 0xC14 [20]</td><td>0h 0h</td></tr></table>	Name	Location	Value	Deep Sx Enable	Offset 0x180 [20] H Offset 0xC14 [20]	0h 0h	
Name	Location	Value					
Deep Sx Enable	Offset 0x180 [20] H Offset 0xC14 [20]	0h 0h					
Note: This is not the same as Intel® CSME power state M3.							
Test Pass/Fail Criteria:	Test passes if SoftStraps/register setting in this step matches to the configuration in the target system.						



21.8 Trusted Platform Module (TPM) on SPI Test

Test ID:	PSS_008						
Test Case Title:	Trusted Platform Module on SPI Test						
Mandatory/Optional:	Mandatory						
Description:	TPM can be configured through PCH SoftStraps to operate over LPC or SPI, but no more than 1 TPM is allowed in the target system.						
Objective:	To verify TPM on SPI is correctly configured.						
Procedure:	Boot to targeted OS. Verify correct configuration of the PCH SoftStraps below: 1. Does this platform have a TPM connected to SPI controller? — If YES, Skip to Boot to targeted OS testing step.						
	<table><tr><th>Name</th><th>Location</th><th>Value</th></tr><tr><td>TPM Over SPI Bus Enable</td><td>Offset 0x1F0 [0] LP Offset 0x234 [0] H</td><td>1h 1h</td></tr></table>	Name	Location	Value	TPM Over SPI Bus Enable	Offset 0x1F0 [0] LP Offset 0x234 [0] H	1h 1h
	Name	Location	Value				
	TPM Over SPI Bus Enable	Offset 0x1F0 [0] LP Offset 0x234 [0] H	1h 1h				
	— If NO (default),						
	<table><tr><th>Name</th><th>Location</th><th>Value</th></tr><tr><td>TPM Over SPI Bus Enable</td><td>Offset 0x1F0 [0] LP Offset 0x234 [0] H</td><td>0h</td></tr></table>	Name	Location	Value	TPM Over SPI Bus Enable	Offset 0x1F0 [0] LP Offset 0x234 [0] H	0h
	Name	Location	Value				
	TPM Over SPI Bus Enable	Offset 0x1F0 [0] LP Offset 0x234 [0] H	0h				
	Boot to targeted OS. Verify correct configuration of the PCH SoftStraps below: 1. What Clock Frequency is being used for TPM on SPI? a. If 48MHz						
	<table><tr><th>Name</th><th>Location</th><th>Value</th></tr><tr><td>SPI TPM Clock Frequency</td><td>Offset 0x13D [2:0] LP and H</td><td>2h</td></tr></table>	Name	Location	Value	SPI TPM Clock Frequency	Offset 0x13D [2:0] LP and H	2h
Name	Location	Value					
SPI TPM Clock Frequency	Offset 0x13D [2:0] LP and H	2h					
b. 30MHz							
<table><tr><th>Name</th><th>Location</th><th>Value</th></tr><tr><td>SPI TPM Clock Frequency</td><td>Offset 0x13D [2:0] LP and H</td><td>4h</td></tr></table>	Name	Location	Value	SPI TPM Clock Frequency	Offset 0x13D [2:0] LP and H	4h	
Name	Location	Value					
SPI TPM Clock Frequency	Offset 0x13D [2:0] LP and H	4h					
c. 17MHz							
<table><tr><th>Name</th><th>Location</th><th>Value</th></tr><tr><td>SPI TPM Clock Frequency</td><td>Offset 0x13D [2:0] LP and H</td><td>6h</td></tr></table>	Name	Location	Value	SPI TPM Clock Frequency	Offset 0x13D [2:0] LP and H	6h	
Name	Location	Value					
SPI TPM Clock Frequency	Offset 0x13D [2:0] LP and H	6h					
Test Pass/Fail Criteria:	Test passes if SoftStraps/register setting in this step matches to the configuration in the target system.						





22 Intel® ISH FW Compliance

This chapter provides the ISH FW testing (performed using PETS) from the image creating stage to OS level, in each stage checking the ISH FW and sensors status.

PETS (Platform Enablement Test Suite) is a test design application and execution engine that enable users to design and run work flows on various devices. It is used for sensor compliance testing.

Prerequisites:

- PDT Editor tool can be found in the ISH FW Kit
- Sensor Viewer Tool can be found in the ISH FW Kit

22.1 Test Coverage Summary

Test ID	Test Case Title	Target OS	Automated/ Manual	Mandatory/ Optional
ISS_TST_01	Sensor communication test	Windows*	PETS	Mandatory
ISS_TST_02	Sensor Data check	Windows*	Manual	Mandatory
ISS_TST_03	ISH FW loading and execution	Windows*	Manual	Mandatory
ISS_TST_04	Sensor diagnostic test	Windows*	Manual	Mandatory
ISS_TST_05	Test System Sensor Noise and Effects on Sensor Algorithms	Windows*	PETS	Optional
ISS_TST_06	Test worst case system interference and effect on sensor algorithms	Windows*	PETS	Optional
ISS_TST_07	Test system performance and effective calibration under a specific range of movements	Windows*	PETS	Mandatory if motion sensors are present
ISS_TST_08	This test confirms that the Barometer (Pressure) sensor is working correctly on the system.	Windows*	Semi-Automated (PETS)	Mandatory if a Barometer is present
ISS_TST_09	Light sensor (ALS) accuracy test	Windows*	Semi-Automated (PETS)	Mandatory
ISS_TST_10	Light sensor (ALS) angular response test	Windows*	Semi-Automated (PETS)	Mandatory
ISS_TST_11	360 Hinge and swivel accuracy test with Second Accelerometer	Windows*	Semi-Automated (PETS)	Mandatory only if the Second Accelerometer is present on the design
ISS_TST_12A	PLM Functionality verification in S0	Windows*	Manual	Mandatory only if the Second Accelerometer is present on the design



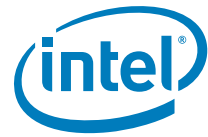
Test ID	Test Case Title	Target OS	Automated/ Manual	Mandatory/ Optional
ISS_TST_12B	PLM Functionality verification with power transitions	Windows*	Manual	Mandatory only if the Second Accelerometer is present on the design
ISS_TST_13	Heading sensor accuracy and drift test	Windows*	Semi-Automated (PETS)	Mandatory—Required if the system supports a magnetometer.
ISS_TST_14	Intel Integrated Sensor Solution Power States	Windows*	PETS	Mandatory
ISS_TST_15	Sensor Activity Contexts	Windows*	Semi-Automated (PETS)	Optional. Perform the test if the system holds motion sensors.
ISS_TST_17	Sensor Gesture Contexts	Windows*	Semi-Automated (PETS)	Optional. Perform the test if the system holds motion sensors.
ISS_TST_18	Wake on shake test	Windows*	Manual	Mandatory if Wake on Shake is implemented
ISS_TST_19	Step counting test	Windows*	Manual	Optional

22.2 Sensor Communication Test

Test ID:	ISS_TST_01
Test Case Title:	Sensor communication test
Mandatory/Optional:	Mandatory
Description:	This test is checking basic communication with the ISH, and that the ISH FW can be read.
Objective:	Verify communication with the ISH sensors
Windows*/Android Procedure:	<ol style="list-style-type: none">1. Boot the platform to AOS/WOS/EFI shell.2. From elevated command line run the MEmanuf Tool: "MEmanuf -ISH -test 0 -verbose" "MEmanuf -ISH -test 1 -verbose" "MEmanuf -ISH -test 2 -verbose" "MEmanuf -ISH -test 3 -verbose"3. In the tool output the test results for each of the tests should be "test pass for all sensors"
Test Pass/Fail Criteria:	

22.3 Sensor Data Check

Test ID:	ISS_TST_02
Test Case Title:	Sensor Data check
Mandatory/Optional:	Mandatory
Description:	In the PDT Editor we are configuring the Sensors drivers, I2C data, and calibration data, this test checks that the sensors information was configured correctly in PDT table.



Test ID:	ISS_TST_02
Objective:	Check the sensor data in the PDT editor to make sure it is compliant with the board.
Windows* Procedure:	Verify the sensors information in the PDT Editor: 1. Open the full SPI image in the FITC tool (Decompose it) 2. In the FITC tool folder, a folder is created with the name of the image that was decomposed using FITC 3. Using the PDT Editor open the PDT table from that image, it is located under: FITC\image_name\Decomp\PdtBinary.bin 4. In the PDT Editor verify that each of the sensors in configured with the rights settings.
Test Pass/Fail Criteria:	Test passes if the sensors information was configured correctly in the PDT Editor.

22.4 Loading and Execution

Test ID:	ISS_TST_03
Test Case Title:	ISH FW Version Check
Mandatory/Optional:	Mandatory
Description:	This test is checking basic communication with the ISH, and that the ISH FW can be read.
Objective:	Verify that ISH is responsive and that ISH FW can be read.
Windows* Procedure:	1. Boot the platform to AOS/WOS shell. 2. From elevated command line run the MEInfo Tool. 3. In the tool output check that: b. ISH Status is "responding" c. ISH FW Version can be read and is as follow: "3.x.x.XXXX" (X-Stand for do not care)
Test Pass/Fail Criteria:	Test passes if ISH status is "responding" and ISH FW can be read.

22.5 Sensor Diagnostic Test

Test ID:	ISS_TST_04
Test Case Title:	Sensor Diagnostic test
Mandatory/Optional:	Mandatory
Description:	This test is checking that the ISH sensors are ready for use.
Objective:	Verify that the ISH sensors are ready for use and that data is received from the sensor.
Windows* Procedure:	1. Boot the platform to Windows*. 2. Open the Sensor Diagnostic Tool. 3. For each sensor on the platform check that the state is "Ready" and that Data is received, this may require a trigger of the sensor event, for example for the Orientation sensor the platform need to be moved in order to receive data in the sensor Diagnostic Tool.
Test Pass/Fail Criteria:	Test passes if in the Sensor Diagnostic Tool, all of the sensors state is "Ready" and the data is received for each of the sensors.



22.6 Test System Sensors

22.6.1 Sensor Noise and Error Levels

Included below is a table of sensor noise and error levels that is monitored by some tests within the compliance guide. These numbers should be measured after calibration has been applied.

Values Measured from the Physical Sensor:

	Maximum Offset per Axis Compared to Average	Noise per Axis
Accelerometer	30 mg	10 mg
Magnetometer	50 mGauss	10 mGauss
Gyroscope	15 dps	0.2 dps

Values Measured from the IISS Algorithms (Static—No Movement):

	Maximum Error	Average Error	STD
Inclinometer	2 degrees	2 degrees	0.75 deg
3D Compass	2 degrees	2 degrees	0.75 deg
3D Gyro	1.0 dps	1.0 dps	0.2 dps
3D Accelerometer	40 mg	40 mg	

Note: 3D Gyroscope and 3D Accelerometer values are “per axis.”



22.6.2 Test System Sensor Noise and Effects on Sensor Algorithms

Test ID:	ISS_TST_05
Test Case Title:	Test System Sensor Noise and Effects on Sensor Algorithms
Mandatory/Optional:	Optional
Description:	<p>The performance of the ISS sensor algorithms may degrade if the noise levels are too high. This test measures the noise levels on each sensor at when the system is at rest to indicate the likelihood of an impact to overall system sensor performance.</p> <p>The causes for higher noise levels can include selecting a poor quality sensor or could be related to system interference from other components (i.e. CPU) or due to PCB design issues.</p> <p>The test also measures any variance seen at the output of the sensor algorithms to also indicate unexpected variance (i.e. e-compass moving or drifting) that would also indicate a performance issue with the system.</p>
Objective:	Gather statistical data on both sensor data input (RAW sensor data) and data output of sensor algorithms.
Procedure:	<p>Automated (PETS)</p> <p>Initial state of the SUT should be S0.</p> <p>If the system is a 2-in-1 device, the test should start with the system in the "PC" context (screen facing user with keyboard facing-up on the table).</p> <p>Intel® Platform Enablement Test Suite (Intel® PETS) performs the following steps:</p> <ol style="list-style-type: none"> 1. Gather RAW and virtual sensor data over a designated period (i.e. 10 seconds). Data is gathered from all present physical sensors on platform and all available sensor SW drivers. 2. If the System is a 2-in-1 device, convert it into a tablet form-factor (screen on top of keyboard or detached from it_ and repeat step #1
Test Pass/Fail Criteria:	<p>Test passes if all sequences show:</p> <ol style="list-style-type: none"> 1. RAW sensor statistical data shows noise levels within acceptable ranges. 2. Data output from sensor algorithms do not show movement or other performance issues when the system is at rest. <p>For #1 and #2 - the tool refers to the pass/fail levels placed in the section "Sensor Noise and Error Levels".</p> <p>In the case that the test results are above the pass/fail limits - the tests raises a "warning" to the user.</p>



22.6.3 Test Worst Case System Interference and Effect on Sensor Algorithms

Test ID:	ISS_TST_06
Test Case Title:	Test worst case system interference and effect on sensor algorithms
Mandatory/Optional:	Optional
Description:	<p>The system may contain noise sources that cause the worst system sensor performance issues when enabled. This can include the speakers, CPU, GPU, and others.</p> <p>The goal of this test is to measure both physical RAW sensor data and the outputs seen at the output of the sensor algorithms to understand if increased noise levels (or movement) is seen when typical noise sources are operated at their worst condition.</p>
Objective:	Determine the worst-case system interference that can be seen on the sensors. Measures both interference seen on RAW sensor data and effect to virtual sensors.
Procedure:	<p>Semi -Automated (PETS)</p> <p>Initial state of the SUT should be S0. The audio sub-system should be fully functional.</p> <p>If the system is a 2-in-1 device, the test should start with the system in the "PC" context (screen facing user with keyboard facing-up on the table).</p> <p>Intel® Platform Enablement Test Suite (Intel® PETS) performs the following steps:</p> <ol style="list-style-type: none">1. The system exercises known interference sources to refer if they have influences on the system. Data should be gathered at each step for at least 10 seconds. The interference sources include:<ul style="list-style-type: none">— Outputting speaker data at maximum frequency with a tonal frequency of 100 Hz to 2000 Hz (100 Hz/step). This should be operated at maximum volume.— CPU operated at minimum and maximum load.— GPU operated at minimum and maximum load.— Turn the computer screen on/off <p>For each sample data sample - the system gathers RAW and virtual sensor data. The noise levels and any movement should be recorded and compared to pass/fail levels.</p> <ol style="list-style-type: none">2. The system exercises known interference sources to refer if they have influences on the system. Data Should be gathered at each step.3. If the system is a 2-in-1 device, convert it into a tablet form-factor (detached/screen on to of keyboard) and repeat steps #1 and #2
Test Pass/Fail Criteria:	<p>Test passes if all sequences show:</p> <ol style="list-style-type: none">1. RAW sensor statistical data shows noise levels within acceptable ranges.2. Data output from sensor algorithms do not show movement or other performance issues when the system is at rest. <p>Notes:</p> <ol style="list-style-type: none">1. For #1 and #2 - the tool refers to the pass/fail levels placed in the section "Sensor Noise and Error Levels".2. In the case that the test results are above the pass/fail limits - the tests raises a "warning" to the user.



22.7 Test System Performance and Effective Calibration Under a Specific Range of Movements

Test ID:	ISS_TST_07
Test Case Title:	Test system performance and effective calibration under a specific range of movements
Mandatory/Optional:	Mandatory if motion sensors are present
Description:	The data quality of the sensor algorithms can be impacted by a number of factors (example: inaccurate sensor calibration). This test moves the sensor across a number of positions and tests that all pass-through sensors and virtual algorithms respond as expected.
Objective:	Tests sensor configuration for correct orientation and data during both rest and movement.
Procedure:	<p>Semi-Automated (PETS) Initial state of the SUT should be S0. The system should have run through the ISS sensor calibration procedure with the calibration data stored and used on the system. The system should be configured in a tablet context. If the device is a 2- in-1, suggest repeating in the PC form-factor with the system placed in a box that can be moved in the pattern shown below. The user is asked to run through the following movements to test the gyroscope:</p> <p>Test Sub-Section A: Gyroscope Z-Axis:</p> <ol style="list-style-type: none"> 1. Place the system flat on the table with the screen facing upwards. 2. Rotate the system clockwise - the gyroscope should identify a negative angular velocity on the Z-axis. 3. Rotate the system counter-clockwise - the gyroscope should identify a positive angular velocity on the Z-axis. <p>Test Sub-Section B: Gyroscope X-Axis:</p> <ol style="list-style-type: none"> 1. Place the system face-up on the table with the screen facing towards you in the "portrait" position. 2. Rotate the system clockwise - the gyroscope should identify a positive angular velocity on the Y-axis. 3. Rotate the system counter-clockwise - the gyroscope should identify a negative angular velocity on the Y-axis. <p>Test Sub-Section C: Gyroscope Y-Axis:</p> <ol style="list-style-type: none"> 1. Place the system face-up on the table with the screen facing towards you in the "landscape" position. The right-hand side of the screen should be pointing upwards. 2. Rotate the system clockwise - the gyroscope should identify a negative angular velocity on the X-axis. 3. Rotate the system counter-clockwise - the gyroscope should identify a positive angular velocity on the X-axis. <p>Test Sub-Section D: Accelerometer:</p> <p>Place the system in the following positions:</p> <ol style="list-style-type: none"> 1. Flat on the table facing up. (Z-UP) The accelerometer should read (0,0,-g0). 2. Flat on the table facing down. (Z-down) The accelerometer should read (0,0,g0). 3. Facing the user on the table in landscape mode. (X-DOWN) The accelerometer should read (g0,0,0). 4. The same position as the previous step but now placed up-side-down. The accelerometer should read (-g0,0,0). 5. Facing the user on the table in portrait mode. (Y-DOWN) The accelerometer should read (0,-g0,0). 6. The same position as the previous step but now placed up-side-down. The accelerometer should read (0,g0,0).
Test Pass/Fail Criteria:	<p>Test passes if all sequences show:</p> <p>For the gyroscope: The correct direction was recorded from the gyroscope when moving the system.</p> <p>For the accelerometer: The accelerometer reading was correct within a 5 degree error.</p>

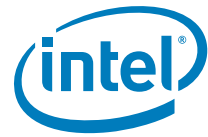


22.8 Barometer (Pressure) Sensor Sanity Test

Test ID:	ISS_TST_08
Test Case Title:	Barometer (pressure) sensor sanity test
Mandatory/Optional:	Optional—Mandatory if a Barometer is present.
Description:	This test confirms that the Barometer (Pressure) sensor is working correctly on the system.
Objective:	Test that the barometer sensor is present and responsive to changing elevations
Procedure:	<p>Semi-Automated (PETS)</p> <p>Initial state of the SUT should be S0 (OS up). The ISS should be configured in the system FW.</p> <ol style="list-style-type: none">1. Lift the system to a height of 1.5-2.0 meters. Wait 10 seconds.2. Place the system on the ground. Wait 10 seconds. <p>For each sample data sample - the system gathers RAW and virtual sensor data.</p>
Test Pass/Fail Criteria:	<p>Test passes if all sequences show:</p> <p>The pressure sensor recorded a change in altitude relative.</p>

22.9 Light Sensor (ALS) Accuracy Test

Test ID:	ISS_TST_09
Test Case Title:	Light sensor (ALS) accuracy test
Mandatory/Optional:	Mandatory
Description:	This test reviews the accuracy of the Ambient Light Sensor after it has been characterized.



Test ID:	ISS_TST_09
Objective:	<p>The Ambient Light Sensor accuracy may be affected by a number of factors including the mechanical design of the housing, cover glass, and the calibration applied within the ISS system.</p> <p>The test is meant to test the accuracy of the ALS after it has been calibrated.</p>
Procedure:	<p>Semi-Automated (PETS)</p> <p>Initial state of the SUT should be S0 (OS up). The ISS should be configured in the system FW.</p> <p>System is in a dark room or placed within a lighting tent (made out of diffused lighting material) and covered with a black cloth. The following equipment should be used:</p> <ol style="list-style-type: none"> 1. Tunable light source that can emit halogen light. 2. Light meter to measure the lighting level incident on the SUT. <p>The light meter is placed next to the system ALS sensor. The system should be orientated orthogonal to the light source.</p> <ol style="list-style-type: none"> 1. Light source is tuned to maximum amplitude. ALS reading should be displayed on the screen. Check that the received ALS value is within +/- 10% of the recorded light meter value. The screen brightness should appear not too bright or too dark. 2. Lower the light source to mid-way. Compare again the difference between the ALS and light meter value. The screen brightness should adjust such that it is not too bright or too dark relative to the ambient light level. 3. Tune light source to the lowest level. Compare again the difference between the ALS and light meter value. The screen brightness should adjust such that it is not too bright or too dark relative to the ambient light level. 4. (optional) If a fluorescent light source is available, expose the system to the same "low" light level seen in the previous step. Check that the ALS light levels are correct relative to the light meter. And that the screen brightness is not too bright or too dark.
Test Pass/Fail Criteria:	<p>Test passes if all sequences show:</p> <p>For all light levels tested - the ALS is correct within +/- 10%.</p>

22.10 Light Sensor (ALS) Angular Response Test

Test ID:	ISS_TST_10
Test Case Title:	Light sensor (ALS) angular response test
Mandatory/Optional:	Mandatory
Description:	<p>This test will test the angular response of the ALS sensor to determine if it falls within the requirements of the MSFT HW certification guidelines. MSFT asks that the light response does not fall by more than 50% when changing the angle of incident light from 0 to 35 degrees.</p> <p>Issues can occur with the sensor angular response due to the light sensor cavity/hole design or other materials covering the light sensor.</p>



Test ID:	ISS_TST_10
Objective:	Confirm that the ambient light sensor angular response is greater than 50% at a 35 degree angle of incidence.
Procedure:	<p>Semi-Automated (PETS)</p> <p>Initial state of the SUT should be S0 (OS up). The ISS should be configured in the system FW. System is in a dark room or placed within a lighting tent (made out of diffused lighting material) and covered with a black cloth. The following equipment should be used:</p> <ol style="list-style-type: none">1. Tunable light source that can emit halogen light.2. Light meter to measure the lighting level incident on the SUT. The light meter is placed next to the system ALS sensor. <p>The system should be orientated orthogonal to the light source.</p> <p>Before starting the test:</p> <ol style="list-style-type: none">1. The system should be directly facing the light source.2. The ALS reading should be within +/- 10% of the value read by the light meter. Recommended target lighting is 100lux with the ALS reading 90-110 lux. <p>When running the test:</p> <ol style="list-style-type: none">1. Rotate the system so that the ALS is at a 35 degree angle to the incident light without changing the distance.
Test Pass/Fail Criteria:	Test passes if all sequences show: The recorded light level of the ALS does not fall more than 50%.

22.11 360 Hinge and Swivel Accuracy Test with 2nd Accelerometer

Test ID:	ISS_TST_11
Test Case Title:	360 Hinge and swivel accuracy test with 2nd Accelerometer
Mandatory/Optional:	Required only if the 2nd Accelerometer is present on the design.
Description:	<p>Placing an accelerometer both in the base and lid of the system design enables the system to determine the angle between the lid and base. This algorithm (also called a virtual protractor) tell the system how to operate if the system is closed, in a PC use case, or if the lid is flipped such that the system is in a tablet mode.</p> <p>The goal of this test is to confirm that the lid angles are reported correctly.</p>
Objective:	Confirm that the angle between the base and lid is accurately reported.
Procedure:	<p>Semi-Automated (PETS)</p> <p>Initial state of the SUT should be S0 (OS up). The ISS should be configured in the system FW.</p> <p>Place the system on a flat table. Record the reported angle over a 5 second period.</p> <ol style="list-style-type: none">1. 0 degrees. Lid closed (screen facing keyboard).2. 90deg. Screen open and facing the user. Screen and keyboard are orthogonal with user seeing screen and keyboard at the same time.3. 180 degrees. Screen and keyboard both facing up.4. 270 degrees. Screen and keyboard are orthogonal. The user cannot view the screen and keyboard at the same time.5. 360 degrees. System flat on table. The screen is facing up and the keyboard is facing down.
Test Pass/Fail Criteria:	Test passes if all sequences show: The detected angle should be within a ± 10 degrees of accuracy. Over the 5 seconds, the variance of the angle should have been less than ± 5 degrees.



22.12 PLM Functionality Verification

Test ID:	ISS_TST_12A
Test Case Title:	PLM Functionality Verification without System Power Transitions
Mandatory/Optional:	Mandatory if PLM is implemented
Description:	Test requires to go through the system modes configured in the PDT Config by adjusting the system position per each mode definition, while verifying and comparing the actual data reported by the PLM algorithm.
Objective:	To verify proper configuration and functionality of the PLM algorithm on customer system in S0
Procedure:	<ol style="list-style-type: none"> 1. Boot the system to OS. 2. Set the system in a first position according to the last PLM Mode configured in the PDT Config file. 3. User should manually acknowledge when the system is placed in the position as requested in previous step. 4. User should verify if the actual system position reported by the PLM algorithm is aligned to what user confirmed. 5. Continue to the next PLM Mode looping steps 2-4.
Test Pass/Fail Criteria:	Test passes only if all PLM Modes are matching the actual system position. i.e. all PLM Modes are successfully matched.

Test ID:	ISS_TST_12B
Test Case Title:	PLM Functionality Verification with System Power Transitions
Mandatory/Optional:	Mandatory if PLM is implemented
Description:	Test requires to make system power transitions while going through the system modes as configured in the PDT Config file. User is requested to adjust the system position as defined by each Platform Mode, while verifying and comparing the actual data reported by the PLM algorithm to the system position reported by the user.
Objective:	To verify proper configuration and functionality of the PLM algorithm on customer system while involving system power transition
Procedure:	<ol style="list-style-type: none"> 1. Boot the system to OS. 2. Set the system in a first position according to the last PLM Mode configured in the PDT Config file. 3. User should manually acknowledge when the system is placed in the position as requested in previous step. 4. User should verify if the actual system position reported by the PLM algorithm is aligned to what user confirmed. 5. Change the system state to S3. 6. User set the system in the next position according to the last PLM Mode configured in the PDT Config file. 7. User should manually acknowledge when the system is placed in the position as requested in previous step. 8. User to wake the system to OS/S0. 9. User should verify if the actual system position reported by the PLM algorithm is aligned to what user confirmed. 10. Continue to the next PLM Mode looping steps 5-9.
Test Pass/Fail Criteria:	Test passes only if all PLM Modes are matching the actual system position. i.e. all PLM Modes are successfully matched.



22.13 Heading Sensor Accuracy and Drift Test

Test ID:	ISS_TST_13
Test Case Title:	Heading sensor accuracy and drift test
Mandatory/Optional:	Mandatory—Required if the system supports a magnetometer.
Description:	<p>The e-compass using the system accelerometer and magnetometer can experience errors for multiple reasons including incorrect sensor calibration.</p> <p>This test is designed to show that the heading accuracy is correct in a number of angles/directions.</p>
Objective:	Confirm that the system reports the correct heading accuracy.
Procedure:	<p>Semi-Automated (PETS) Initial state of the SUT should be S0 (OS up). The ISS should be configured in the system FW. If the system is a 2-in-1 device, the test should start with the system in the "PC" context (screen facing user with keyboard facing-up on the table). To test that the system is free of external magnetic influence:</p> <ol style="list-style-type: none">1. Gather data from the magnetometer (@ rest) - confirm that the magnetometer is not moving more than 1-2 degrees while the system remains still.2. Move the system 0.5 meters in each direction. Confirm that the compass reading does not change more than 1-2 degrees. <p>Intel® Platform Enablement Test Suite (Intel® PETS) performs the following steps:</p> <p>Test System Flat on Table (Z-UP) With a compass, place the system facing north on a flat table:</p> <ol style="list-style-type: none">1. Start with the system placed facing north and flat on the table.2. Rotate the system to 45 degrees from North3. Rotate the system to 90 degrees from North4. Rotate the system to 135 degrees from North5. Rotate the system to 180 degrees from North <p>Note: If system is a 2-in-1 device, convert it into a tablet form-factor (detached / screen on top of keyboard) and repeat this test sub-section.</p>
Test Pass/Fail Criteria:	Test passes if all sequences show: System heading error should not exceed 10 degrees at any rest position.

22.14 Intel Integrated Sensor Solution Power States

Test ID:	ISS_TST_14
Test Case Title:	Intel Integrated Sensor Solution Power States
Mandatory/Optional:	Mandatory
Description:	The purpose of this test is validate that the IISS is alive after system power transitions.



Test ID:	ISS_TST_14
Objective:	IISS is alive without errors after power transitions.
Procedure:	<p>Automated (PETS)</p> <p>Initial state of the SUT should be S0 (OS up) with the IISS configured in the system FW.</p> <p>Before running this test record the output of each IISS algorithm seen at the OS level. And confirm that the full sensor functional test has passed.</p> <p>Run the following power transitions from S0:</p> <ol style="list-style-type: none"> 1. Resume from S3 on AC + DC 2. Resume from S3 on DC 3. Resume from S4 on AC + DC 4. Resume from S4 on DC 5. Resume from S5 on AC + DC 6. Resume from S5 on DC 7. Resume from DeepS4* (Optional if FW image supports DeepSx) 8. Resume from DeepS5* (Optional if FW image supports DeepSx) 9. Resume from G3 on AC + DC 10. Resume from G3 on DC 11. Resume from G3 with no coin battery (if coin battery exists) 12. Resume after system reset (cold reset, HW RST button) 13. Resume after system reboot (warm reset, host based) <p>After each system resume - check the output of each IISS algorithm seen at the OS level. And confirm that the full sensor functional test has passed.</p> <p>** To test DeepSx the user must enter the BIOS menu: 'BIOS' -> 'Intel Advanced Menu' -> 'PCH-IO Configuration' -> 'DeepSx Power Policies' -> 'Enabled in S3-S4-S5'</p> <p>For manual testing - the sensor diagnostic tool can be used to read the output of the sensors. The sensor functional test can be run with the MEMANUF tool ("memanuf -ish -test 4").</p>
Test Pass/Fail Criteria:	<p>Test passes if all sequences show:</p> <ol style="list-style-type: none"> 1. System functional test records a "pass" after the system resumes to S0. 2. The algorithm outputs are within a +/-10% range of their previous values prior to the system power transition. <p>Note: If the sensor or sensor micro-driver does not support the "built in functional test" (test level 3) then the test returns a warning to the user.</p>

22.15 Sensor Activity Contexts

Test ID:	ISS_TST_15
Test Case Title:	Sensor Activity Contexts
Mandatory/Optional:	Optional. Perform the test if the system holds motion sensors.
Description:	<p>The IISS contains activity context algorithms that can determine the user activities. This includes determining if the user is (1) sitting, (2) walking, or (3) running [at a safe speed].</p> <p>These tests confirm if the sensor activity contexts algorithms within the IISS are working properly.</p>



Test ID:	ISS_TST_15
Objective:	Confirm that the system detects the system user activity contexts.
Procedure:	<p>Semi-Automated (PETS) Initial state of the SUT should be S0 (OS up). The ISS should be configured in the system FW. Place the system on a flat table. If the system is a 2-in-1 system start in the tablet form factor.</p> <ol style="list-style-type: none">1. Sit on a chair while looking at the system. The system should detect that the system is sedentary.2. Pick up the system and begin walking with it. The system should detect that you are walking with the system.3. Start lightly running with the system. The system should detect that you are running with the system.
Test Pass/Fail Criteria:	Test passes if all sequences show: The system accurately detected the user contexts.

22.16 Sensor Terminal Contexts

Test ID:	ISS_TST_16
Test Case Title:	Sensor Terminal Contexts
Mandatory/Optional:	Optional. Perform the test if the system holds motion sensors.
Description:	The IISS contains terminal context algorithms that can determine how the user is holding the system. This includes determining if the system is held (1) face up / down, (2) portrait up / down, or (3) landscape left / right. These tests confirm if the sensor terminal contexts algorithms within the IISS are working properly.
Objective:	Confirm that the system detects the system user terminal contexts.
Procedure:	<p>Semi-Automated (PETS) Initial state of the SUT should be S0 (OS up). The ISS should be configured in the system FW. Place the system on a flat table. If the system is a 2-in-1 system start in the tablet form factor.</p> <ol style="list-style-type: none">1. Place the system face up and face down.2. Place the system portrait up and portrait down.3. Place the system landscape left and landscape right.
Test Pass/Fail Criteria:	Test passes if all sequences show: The system accurately detected the terminal contexts.

22.17 Sensor Gesture Contexts

Test ID:	ISS_TST_17
Test Case Title:	Sensor Gesture Contexts
Mandatory/Optional:	Optional. Perform the test if the system holds motion sensors.
Description:	The IISS contains gesture context algorithms that can determine how the user is holding the system. This tests confirm if the sensor gesture contexts algorithm within the IISS are working properly.



Test ID:	ISS_TST_17
Objective:	Confirm that the system detects the system user gesture contexts.
Procedure:	Semi-Automated (PETS) Initial state of the SUT should be S0 (OS up). The ISS should be configured in the system FW. Place the system on a flat table. If the system is a 2-in-1 system start in the tablet form factor. 1. Lift the system from the table and look at the system.
Test Pass/Fail Criteria:	Test passes if all sequences show: The system accurately detected the terminal contexts.

22.18 Wake On Shake Test

Test ID:	ISS_TST_18
Test Case Title:	Wake on shake test
Mandatory/Optional:	Mandatory
Description:	Wake on different events is a mandatory feature in Win10. As such a test that focuses on the ability to wake the system from S0i3 (CS) is a must.
Objective:	Test that ISH can send a wake event to Win OS and the OS wakes from S0i3 to S0
Procedure:	<ol style="list-style-type: none"> 1. Make sure that system is set in CS state (S0ix) 2. Make sure that shake event is defined in PDT and in Windows* (use SDT to check it) 3. Shake the system 4. Windows* should wake and log on screen should appear. 5. Repeat the test 3 times 6. There is a timeout (usually 2 minutes) until Win goes to SC again, unless the configuration of the specific copy of Windows* on the device set the timer to a different value.
Test Pass/Fail Criteria:	The test passes if Windows* awakes all 3 times

22.19 Step Counting Test

Test ID:	ISS_TST_19
Test Case Title:	Step counting test
Mandatory/Optional:	Optional—Mandatory if the step counting is operational.
Description:	Step counting is a standard virtual sensor that is being exposed in Win10. The goal is to test that step counting sensor is working correctly



Test ID:	ISS_TST_19
Objective:	Test that step counting sensor is working correctly and measure user steps
Procedure:	<p>Initial state of the SUT should be S0 (OS up). The ISS should be configured in the system FW.</p> <p>User should hold the tablet/notebook while he/she stands.</p> <p>User should check SDT or any other sensor data report SW on the OS for the current number of step counter</p> <p>User should start walking while counting his/her steps in a straight line.</p> <p>After counting 50 steps user should stop.</p> <p>User should compare the 50 steps he/she made to the number of steps shown on the software (after doing the needed math of subtracting the initial number of steps...).</p> <p>Remark: the step counter starts acting of 10 sec of stepping, so tests that takes 10 sec or would not be able to check the counter.</p>
Test Pass/Fail Criteria:	Amount of steps made by the user should be identical to step counter number on the SDT or any other sensor data SW.

§ §



23 Intel® Software Guard Extension (Intel® SGX)

23.1 Introduction

Intel® Software Guard Extension (Intel® SGX) Technology is a CPU based capability that allows application developers to better protect selected code and data from disclosure or modifications. Intel® SGX makes such protections possible through the use of enclaves. Enclaves are protected areas of execution. Application code can be executed in an enclave area via special instructions and software that are available to developers via the Intel® SGX SDK.

Intel® SGX compliance is available in two forms:

1. PETS packages ("Compliance_SGX.xml).
2. Standalone kits published. Kit name: "Intel® SGX Functional validation Tool Rev. <version>" and "Intel® SGX BIOS Info Tool Software utility Updates Rev. <version>". The standalone kits contain the same compliance components as PETS packages.

PETS Package - In this document the Standalone option is discussed in details, for PETS clarifications, read Intel® PETS User Guide.

Standalone Kits - The Standalone kits should be executed locally (with administrator permission) on the tested platform. For all tests, first extract the tools kits to a temporary folder on the tested system.

23.2 Test Coverage Summary

Test ID	Test Case Title	Manual	Form Factor
SGX_001	SGX Enabled	Manual	Desktop, Mobile, and High End Desktop
SGX_002	SGX Disabled	Manual	Desktop, Mobile, and High End Desktop
SGX_003	SGX SW Controlled	Manual	Desktop, Mobile, and High End Desktop
SGX_004	Memory Allocation	Manual	Desktop, Mobile, and High End Desktop
SGX_005	SGX Functionality	Manual	Desktop, Mobile, and High End Desktop
SGX_006	EPID/PSE Provisioning	Manual	Desktop, Mobile, and High End Desktop



SGX Tests

Test ID	SGX_001
Test Case Title	SGX Enabled
Mandatory/Optional	Mandatory
Description	Confirm Intel® SGX functionality when SGX feature state is set to 'Enabled'.
Objective	Test the BIOS to ensure proper configuration of Intel® SGX
Procedure	<ol style="list-style-type: none">1. In BIOS, Select SGX Enabled option.2. Boot to Windows3. Open new CMD as Administrator (Do not use a pre opened CMD). Change directory to SGX BIOS Info tool. Run command "SgxBIOSInfoTool.exe -v -l". Allow the tool to install the SGX SW when required.4. Verify in file "SgxBIOSInfoToolOutput.txt" (under same directory) result as SGX enabled.5. Reboot.6. Perform 2-5 again.7. Perform S3, resume.8. Run c-d again.9. Perform S4, S5.10. Run b-d again.
Test Pass/Fail Criteria	Result is verified as SGX enabled in the "SgxBIOSInfoToolOutput.txt" file.

Test ID	SGX_002
Test Case Title	SGX Disabled
Mandatory/Optional	Mandatory
Description	Confirm Intel® SGX functionality when SGX feature state is set to 'Disabled'.
Objective	Test the BIOS to ensure proper configuration of Intel® SGX
Procedure	<ol style="list-style-type: none">1. In BIOS, Select SGX Disabled option.2. Boot to Windows3. Open new CMD as Administrator (Do not use a pre opened CMD). Change directory to SGX BIOS Info tool. Run command "SgxBIOSInfoTool.exe -v -l". Allow the tool to install the SGX SW when required.4. Verify in file "SgxBIOSInfoToolOutput.txt" (under same directory) result as SGX disabled.5. Reboot.6. Perform 2-5 again.7. Perform S3, resume8. Run c-d again.9. Perform S4, S5.10. Run b-d again.
Test Pass/Fail Criteria	Result is verified as SGX disabled in the "SgxBIOSInfoToolOutput.txt" file.

Test ID	SGX_003
Test Case Title	SGX SW Controlled
Mandatory/Optional	Mandatory
Description	Confirm Intel® SGX functionality when SGX feature state is set to 'SW Controlled'.



Objective	Test the BIOS to ensure proper configuration of Intel® SGX
Procedure	<ol style="list-style-type: none"> In Bios, Select SGX SW Controlled option. Boot to Windows. Open new CMD as Administrator (Do not use pre-opened CMD). Change directory to SGX Bios Info tool. Run command "SgxBIOSInfoTool.exe -v -l". Allow the tool to install SGX SW when required. Verify SGX is disabled in SGX Bios Info Tool log and reboot requested. Reboot. Open new CMD as Administrator (Do not use pre-opened CMD). Change directory to SGX Bios Info tool. Run command "SgxBIOSInfoTool.exe -v -l". Check if SGX is enabled in SGX Bios Info Tool log. Perform S3, resume. Run f-g again. Perform S4. Run f-g again. Perform S5 Run f-g again.
Test Pass/Fail Criteria	Result is verified as Intel® SGX SW Controlled in the "SgxBIOSInfoToolOutput.txt" file.

Test ID	SGX_004
Test Case Title	Memory Allocation
Mandatory/Optional	Mandatory
Description	Verify that memory range reported under Core PRM settings is the same and is marked as reserved
Objective	Verify the allocated memory for SGX
Procedure	<ol style="list-style-type: none"> Boot to UEFI shell Run memmap Check that the range reported in the MSR is marked as reserved/hardware reserved. Compare the reserved range from the memmap log to the reported range in the SgxBIOSInfoToolOutput.txt file under "Core PRM Settings"
Test Pass/Fail Criteria	The result is 'pass', if the range reported is marked and correct.

Test ID	SGX_005
Test Case Title	SGX Functionality
Mandatory/Optional	Mandatory
Description	Perform sanity test of Intel® SGX functionality to verify the system configuration and OS/SW build is SGX compatible.



Objective	Perform sanity test of
Procedure	<ol style="list-style-type: none">1. Set SGX as enabled in BIOS2. Install the SGX SW (if not already installed, can be found on VIP)3. Install the full MEI SW package. (if not already installed, can be found on VIP)4. Open new CMD as Administrator (Do not use a pre opened CMD). Change directory to SGX Functional Validation tool. Run command "SGXFunctionalValidationTool.exe -v -l" the tool requires going through several power states for testing and it is necessary to run the command several times5. Check the SgxFunctionalValidationToolOutput.txt for failures
Test Pass/Fail Criteria	SgxFunctionalValidationToolOutput.txt should give a 'pass/fail/' result.

Figure 23-1. Intel® SGX Functional Validation Tool Pass Result Example

<p>Test Summary:</p> <p>SUCCESS: Get platform service capabilities SUCCESS: Load the validation enclave in debug mode SUCCESS: Check SE_SVN and SGX Locked for Production Mode MSR's. SUCCESS: Verify the Provisioning enclave ISV_SVN version SUCCESS: Check if SGX is in debug mode SUCCESS: Load whitelisted enclave SKIPPED: Tried to EPID Provision the system under test (Note: Intern SKIPPED: Tried to Provision the PSE in the system under test (Note: SUCCESS: Test sealing and unsealing data across S3 boundary SUCCESS: Test sealing and unsealing data across S4 boundary SUCCESS: Test sealing and unsealing data across S5 reboot boundary SUCCESS: Test sealing and unsealing data across S5 shutdown boundary</p> <p>SGX functionality has been verified.</p> <p>-----</p>
--

Test ID	SGX_006
Test Case Title	EPID/PSE Provisioning
Mandatory/Optional	Mandatory
Description	Perform EPID and PSE provisioning status
Objective	Perform sanity test of
Procedure	<ol style="list-style-type: none">1. Set SGX as enabled in BIOS2. Connect platform to the Internet via LAN/Wi-Fi3. Open new CMD as Administrator (Do not use a pre opened CMD). Change directory to SGX Functional Validation tool. Run command "SGXFunctionalValidationTool.exe -v -l -skip_power_tests -prov_epid -prov_pse".4. Check the CMD for failures
Test Pass/Fail Criteria	SgxFunctionalValidationToolOutput.txt should give a 'pass/fail/' result.

**Figure 23-2. Functional Validation Tool Provisioning Pass Result Example**

```
Administrator: C:\Windows\system32\cmd.exe
Manual inspection of SVN values required to verify they are loaded/set correctly.
Currently installed SGX Provisioning Enclave ISV_SVN: 0x0004
Successfully tested SGX Locked for Production Mode.
Successfully loaded the whitelisted enclave.
Starting EPID provisioning...
SGX is currently configured to use the production provisioning server.
Provisioning to this server will only succeed if using a production CPU.

Successfully EPID provisioned the platform. EPID Group: 0x00000ae3

Starting PSE provisioning.....
Successfully completed PSE provisioning.

Test Summary:

SUCCESS: Get platform service capabilities
SUCCESS: Load the validation enclave in debug mode
SUCCESS: Check SE_SVN and SGX Locked for Production Mode MSR's.
SUCCESS: Verify the Provisioning enclave ISV_SVN version
SUCCESS: Check if SGX is in debug mode
SUCCESS: Load whitelisted enclave
SUCCESS: Tried to EPID Provision the system under test (Note: Internet connectivity is required for this test)
SUCCESS: Tried to Provision the PSE in the system under test (Note: Internet connectivity is required for this test)
SKIPPED: Test sealing and unsealing data across S3 boundary
SKIPPED: Test sealing and unsealing data across S4 boundary
SKIPPED: Test sealing and unsealing data across S5 reboot boundary
SKIPPED: Test sealing and unsealing data across S5 shutdown boundary

SGX functionality has been verified.
-----
```

§ §



24 Intel® System Security Report (Nifty Rock) Compliance

24.1 Introduction

The purpose of this document is to provide OEMs guidance on the steps necessary to successfully validate **Intel® System Security Report (Nifty Rock)** technology on Intel client (desktop and mobile) platforms. This document defines the purpose and value of each validation aspect in the validation process. The intent of this document is to outline the ideal validation sequence for **Intel® System Security Report (Nifty Rock)** in this platform and provide an overview of the collateral that is available to provide OEMs the framework to define their own validation strategy.

This document is not a technology. **The readers are expected to be familiar with Intel® Hardware Shield (Intel® Trusted Execution Technology, Intel® Runtime BIOS Resilience Technology, Intel® System Security Report (Nifty Rock) and Devil's Gate Rock technology) to use this document as a validation supplement to develop their own Nifty Rock validation plan.** For Nifty Rock collaterals refer [Section 24.1.4](#).

Devil's Gate Rock (DGR) is the collection of techniques and code within the BIOS used to create and enforce HW access policy for the SMI handler. It consists of a collection of policy mechanisms that are configured by POST before the SMI handler is locked down. Once the SMI handler is locked all accesses into the system must be compliant with the policy established during POST.

Intel® Runtime BIOS Resilience is a subset of DGR covering SMM memory policy only. Intel® Runtime BIOS Resilience Protection hardens the SMI handler via hardware enforced BIOS policy regarding SMI handler access to memory using an enhanced paging policy. This paging policy covers SMI handler access to both BIOS and MLE resources. Intel® Runtime BIOS Resilience Protection is extended using a technology code named **Intel® System Security Report (Nifty Rock)**.

The Platform Properties Assessment Module (PPAM) is the primary component of **Intel® System Security Report (Nifty Rock)** and is used to **collect and report information about platform SMM implementation and configuration**, in order to provide trustworthy attestation of the resulting SMI memory policy regarding SMM secure configuration and access to MLE owned memory. **Intel® System Security Report (Nifty Rock)** is used to create a trustworthy report describing the SMM policy

24.1.1 Platforms Applicable

This validation guide is applicable to the following Client vPro platforms

**Table 24-1. List of Applicable Platforms**

Platform Name
Alder Lake
Comet Lake U
Tiger Lake
Comet Lake H
Comet Lake S
Whiskey Lake U
Coffee Lake S 8+2
Coffee Lake H 8+2

24.1.2 Terminology

Term	Description
Intel® TXT	Intel® Trusted Execution Technology
IRBR	Intel® Runtime BIOS Resilience Technology
DGR	Devil's Gate Rock
Intel® Hardware Shield	Intel® Trusted Execution Technology, Intel® Runtime BIOS Resilience Technology, Devil's Gate Rock, Intel® System Security Report (also Nifty Rock)

24.1.3 Nifty Rock Prerequisites

Applicable platforms are listed in Section 26.1.1

- Verify chipset is Intel® TXT capable
- Processor should support Intel® TXT and have it enabled in BIOS, it should be Intel® vPro® QDF as well.
- Incorporate the PPAM binaries provided as part of the PPAM kit into the BIOS as recommended in the BIOS Writer's guide. Refer next Section.
- Install the tools provided along with the PPAM kit posted on VIP on the system. Run the tools from UEFI shell root directory

BIOS Setting

1. Intel Advanced Menu > CPU Configuration > Intel® TXT<Enabled>

Note:

For enabling Intel® TXT and more details, refer [Chapter 12](#), "Intel® Trusted Execution Technology (Intel® TXT)".



24.1.4 Reference Documents

Table 2. Intel® TXT

Intel® TXT Software Development Guide: Measured Launch Environment Developers Guide	https://www.intel.com/content/dam/www/public/us/en/documents/guides/intel-txt-software-development-guide.pdf
Intel® TXT BIOS Specification	# 572782
Intel® Trusted Execution Technology ACM Kit	Refer VIP portal for the latest kit
Intel® TXT TPM Provisioning Toolkit	Refer VIP portal for the latest kit
Intel® TXT Client Debug Toolkit	Refer VIP portal for the latest kit
Intel® Trusted Execution Technology (Intel® TXT) TBoot information	https://sourceforge.net/p/tboot/wiki/Home/
Intel® Trusted Execution Technology (Intel® TXT) STM Guide	# 596559
Intel® Management Engine (Intel® ME) and Intel® Sensor Solution Consumer/Corporate Compliance Guide	Chapter 13, "Intel® Trusted Execution Technology (Intel® TXT)"

Table 3. Copper Point

Intel® Runtime BIOS Resilience Architecture Guide Overview 0.8	# 576872
Core and Uncore BIOS Specification	# 550049

Table 4. Nifty Rock

Intel® Platform Properties Assessment Module (PPAM) 1.0 Operating System User Guide	# 602426
Intel® Platform Properties Assessment Module (PPAM) 1.0 OS Diagnostic User Guide	# 609184
Intel® Platform Properties Assessment Module (PPAM) 1.1 User Guide	# 604868
Intel® Platform Properties Assessment Module (PPAM) 1.1 Diagnostic User Guide	# 609181
Nifty Rock Technology BIOS specifications	# 601824
Platform Intel® Properties Assessment Module (PPAM) Kit	Refer VIP portal for the latest kit
Intel® CSME 15 and Intel® Sensor Solution Corporate Compliance Guide	Chapter 24

24.1.5 Validation Tools

Refer following commands to run from UEFI shell to collect entire report on platform capability and resources through the PPAM.

1. Load PpamService.efi
2. FrmLoaderApp.efi Frm.efi <SINIT_ACM.bin>
3. PpamTestApp.efi
4. TxtDumpLogApp.efi
5. PpamManifestDumpApp.efi.



Note: SINIT_ACM.bin needs to be passed on Intel® TXT-enabled platform

- **Load PpamService.efi**
 - Produces the PPAM launch protocol which are used by Frm.efi
- **FrmLoaderApp.efi Frm.efi <SINIT_ACM.bin>**
 - Establishes VMX root mode
- **PpamTestApp.efi**
 - It dumps the PPAM report
- **TxtDumpLogApp.efi**
 - It dumps the ACM event log
- **PpamManifestDumpApp.efi**
 - It dumps the PPAM manifest.

24.2 Nifty Rock Test

This section describes the test plan used to verify Nifty Rock functionality on systems enabling the feature.

Test ID	Test Case Title	PETS/Manual	Mandatory/Optional
NR_TC01	Check PPAM binaries are successfully loaded	Manual	Mandatory
NR_TC02	Check "CapabilityPhysicalResourceBitmap" value returned indicates PPAM physical resource	Manual	Mandatory
NR_TC03	Check "PPAM_RSC_VALID_INDICATOR" value for resource list validity and every APICID should be valid	Manual	Mandatory
NR_TC04	Check "PPAM_META_PROPERTY_BITMAP" meta resources BIOS SMM properties and lock setting are asserted correctly	Manual	Mandatory
NR_TC05	Check the PPAM memory range attributes are set correctly	Manual	Mandatory
NR_TC06	Verify PPAM hash matches PpamManifest hash	Manual	Mandatory
NR_TC07	Check all PPAM resources are returned as part of PPAM_GET_RESOURCES_VMCALL	Manual	Mandatory

Note: Make sure to cover the prerequisites in [Section 24.1.3](#) before running any of the tests below.



24.3 NR_TC01

Test ID	NR_TC01
Test Case Title:	Check PPAM binaries are successfully loaded
Mandatory/Optional:	Mandatory
Description:	Validate no errors are reported in PPAMTestApp log
Objective:	Check PPAM is successfully loaded
Procedure:	<ol style="list-style-type: none">1. Boot to EFI-Shell and run step 2 from root directory2. Load PpamService.efi FrmLoaderApp.efi Frm.efi <SINIT_ACM.bin> PpamTestApp.efi;3. Obtain PpamTestApp log by running PpamTestApp.efi result in step 24. Make sure GetResource value for each CPU is 0x0 under PPAM_GET_RESOURCES_VMCALL and also flag bit zero, is set for all APICID's in PPAM_RSC_VALID_INDICATOR corresponding to CPU threads in GetResource. <p>Note: If "FrmLoaderApp.efi Frm.efi <SINIT_ACM>" does not complete correctly. Run the test again with the command "FrmLoaderApp.efi Frm.efi -notxt "to check PPAM is integrated correctly irrespective of TXT. In this case PpamTestApp log obtained, will indicate it is running outside of TXT and would not report resources under PPAM_GET_RESOURCES_VMCALL i.e ResourceSize is 0x0</p>
Test Pass/Fail Criteria	Test passes, if no error is reported in GetResource value for each CPU and there is no missing corresponding APICID in PPAM_RSC_VALID_INDICATOR

24.4 NR_TC02

Test ID	NR_TC02
Test Case Title:	Check "CapabilityPhysicalResourceBitmap" value returned indicates PPAM physical resource
Mandatory/Optional:	Mandatory
Description:	Identify PPAM implementation of physical resources reported by the platform
Objective:	Validate CapabilityPhysicalResourceBitmap value returned is correct
Procedure:	<ol style="list-style-type: none">1. Boot to EFI-Shell and run step 2 from root directory2. Load PpamService.efi FrmLoaderApp.efi Frm.efi <SINIT_ACM.bin> PpamTestApp.efi;3. Obtain PpamTestApp log by running PpamTestApp.efi result in step 24. For NR1.0 PPAM10 and lower: Verify "CapabilityPhysicalResourceBitmap" returned under PPAM_GET_CAPABILITY_VMCALL: should match 0x0000000000000001. For NR 1.1 PPAM 11: Verify "CapabilityPhysicalResourceBitmap" returned under PPAM_GET_CAPABILITY_VMCALL: should match 0x0000000000000057
Test Pass/Fail Criteria	Test passes if CapabilityPhysicalResourceBitmap is 0x0000000000000001 for NR1.0 PPAM10 and lower and For NR1.1 and PPAM 11: Test passes if CapabilityPhysicalResourceBitmap is 0x0000000000000057



24.5 NR_TC03

Test ID	NR_TC03
Test Case Title:	Check "PPAM_RSC_VALID_INDICATOR" value for resource list validity for every APICID
Mandatory/Optional:	Mandatory
Description:	PPAM resources are defined properly
Objective:	Testing configuration of the platform
Procedure:	<ol style="list-style-type: none"> 1. Boot to EFI-Shell and run step 2 from root directory 2. Load PpamService.efi FrmLoaderApp.efi Frm.efi <SINIT_ACM.bin> PpamTestApp.efi; 3. Obtain PpamTestApp log by running PpamTestApp.efi result in step 2 4. Check "RscType" value and "RscLength" under PPAM_RSC_VALID_INDICATOR. "RscType" should be 0x 00000001 and 'RscLength' should be 0x0010
Test Pass/Fail Criteria	Test passes, if log contains the below values under "PPAM_RSC_VALID_INDICATOR" RscType: 00000001 RscLength: 0010

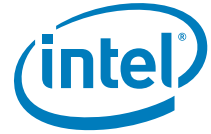
24.6 NR_TC04

Test ID	NR_TC04
Test Case Title:	Check "PPAM_META_PROPERTY_BITMAP" meta resources BIOS SMM properties and lock setting are asserted correctly
Mandatory/Optional:	Mandatory
Description:	PPAM meta properties are asserted correctly
Objective:	Check meta properties; BIOS SMM properties and lock setting are asserted correctly in the platform
Procedure:	<ol style="list-style-type: none"> 1. Boot to EFI-Shell and run step 2 from root directory 2. Load PpamService.efi FrmLoaderApp.efi Frm.efi <SINIT_ACM.bin>; PpamTestApp.efi; 3. Obatin PpamTestApp log by running PpamTestApp.efi result in step 2 4. Check "CapabilityMetaResourceBitmap" value from PPAM_GET_CAPABILITY_VMCALL. 5. Check "Properties" value under PPAM_META_PROPERTY_BITMAP 6. If "CapabilityMetaResourceBitmap" value is equal to "Properties" value under PPAM_META_PROPERTY_BITMAP, meta properties are set correctly
Test Pass/Fail Criteria	PASS, if CapabilityMetaResourceBitmap value is equal to Properties value under PPAM_META_PROPERTY_BITMAP (000000000000000007)



24.7 NR_TC05

Test ID	NR_TC05
Test Case Title:	Check PPAM memory range attributes are not executable
Mandatory/Optional:	Mandatory
Description:	PPAM memory range attributes are correctly set
Objective:	Check memory range attributes are not executable
Procedure:	<ol style="list-style-type: none">1. Boot to EFI-Shell and run step 2 from root directory2. Load PpamService.efi FrmLoaderApp.efi Frm.efi <SINIT_ACM.bin>; PpamTestApp.efi;3. Obtain PpamTestApp log by running PpamTestApp.efi result in step 24. Check "RWXAttributes" value under PPAM_PHYS_MEM_RANGE returned is not 00000007
Test Pass/Fail Criteria	PASS, if for all memory ranges log does not have RWX Attributes equal to 00000007



24.8 NR_TC06

Test ID	NR_TC06
Test Case Title:	Verify PPAM hash matches PpamManifest hash
Mandatory/Optional:	Mandatory
Description:	PPAM Manifest contains digital signature of PPAM binary. This test is to make sure that the hash of the PPAM matches STM hash in the TXTdump log, TPM dynamic event log
Objective:	Verify PPAM Manifest is correctly loaded
Procedure:	<ol style="list-style-type: none"> 1. Boot to EFI-Shell and run step 2 from root directory 2. Load PpamService.efi FrmLoaderApp.efi Frm.efi <SINIT_ACM.bin>; PpamTestApp.efi; TXTDumpLogApp.efi; PpamManifestDumpApp.efi 3. Obtain PPAM Manifest log generated by running PpamManifestDumpApp.efi in step 2 4. Get PPAM Manifest SHA value that contains the hash (a non-zero value) 5. Obtain TXT log generated by running TXTDumpLogApp.efi in step 2 6. Get Digest(0) value from under PCRIndex - 17, EventType - 0x0000040E (STM_HASH) 7. Compare PPAM SHA value to the digest value from txt log
Test Pass/Fail Criteria	PASS, if PPAM SHA value matches the digest value

24.9 NR_TC07

Test ID	NR_TC07
Test Case Title:	Check all PPAM resources are returned as part of PPAM_GET_RESOURCES_VMCALL
Mandatory/Optional:	Mandatory
Description:	All PPAM resources should be reported



Test ID	NR_TC07
Objective:	Verify HW access policy is enforced for SMM besides SMM memory policy for maximum security
Procedure:	<p>1. Boot to EFI-Shell</p> <p>2. Load PpamService.efi FrmLoaderApp.efi Frm.efi <SINIT_ACM>; PpamTestApp.efi;</p> <p>3. Obtain PPAM Test App log generated by running PpamTestApp.efi in step2</p> <p>4. Check resources under "PPAM_GET_RESOURCES_VMCALL"</p> <p>5. For NR1.0 PPAM 10 and lower: Make sure all below resources are listed in PpamTestApp log</p> <ul style="list-style-type: none">> PPAM_SCRATCH_RESOURCE> PPAM_PHYS_MEM_RANGE> PPAM_META_PROPERTY_BITMAP> PPAM_RSC_VALID_INDICATOR> PPAM_META_DIAGNOSTIC (Note: This resource is displayed, if a diagnostic error occurs)> PPAM_END_OF_RESOURCES <p>For NR1.1 PPAM 11: Make sure all below resources are listed in PpamTestApp log</p> <ul style="list-style-type: none">> PPAM_SCRATCH_RESOURCE> PPAM_PHYS_MEM_RANGE> PHYS_IO_RANGE> PHYS_MSR> PHYS_CPU_STATE_SAVE_REG> PHYS_CPU_OTHER_REG> PPAM_META_PROPERTY_BITMAP> PPAM_RSC_VALID_INDICATOR> PPAM_META_DIAGNOSTIC (Note: This resource is displayed, if a diagnostic error occurs)> PPAM_END_OF_RESOURCES
Test Pass/Fail Criteria	PASS if no resource is missing from the above listed resources under PPAM_GET_RESOURCES_VMCALLSS

§ §



25 Intel® Trusted Device Setup

25.1 Introduction

Intel® Trusted Device Setup (Intel® TDS) provides a tampering detection mechanism that enables IT to trust the automated device enrollment solutions.

- Devices are sealed and locked with platform measurements data on manufacturing line.
- Detection of tampering attempts after Seal applied.
- Device attestation during end user boot (3rd party solution).
- Automated provisioning based on the attestation result.

25.2 Solution Prerequisites

- Windows* 10 Intel® MEI Driver with Intel® TDS support.
- Windows* PE* on a bootable media (Example: PXE, HDD) with configuration and tools.
- Intel® IFWI with BIOS Extension and Intel® TDS configuration enabled on CSME FW.
- Bootguard profile 5 with startup locality 3.
- HW TPM 2.0 Intel® Boot Guard or equivalent.
- OPAL v2 or Pyrite (v1 or v2) - compliant NVMe* Self Encrypting Drive (SED), unlocked and not activated.

25.3 Terminology

Terms	Description
Intel® TDS	Intel® Trusted Device Setup
Intel® PMT	Intel® Platform Measurements Tool
PBA	Pre-boot application (BIOS Extension)

25.4 Tools for Testing

Tool Name	New For Intel® TDS	Description
Intel® Platform Measurements Tool (Intel® PMT)	Yes	Collects platform measurements and signs them, produces a signed Platform Measurement File (PMF).
Intel® MEInfo	No	Provides information about the status of the platform, and notifies the user whether Intel® TDS is enabled.
Intel® TDS Sealing Tool	Yes	Seals, unseals, and reseals a device on the manufacturing line.
Intel® TDS Seal Validation Tool	Yes	Intel® Trusted Device Setup Seal Validation Tool allows to perform a local attestation of Intel® TDS system components for functional validation purposes. Note: This tool can run only on Windows* 10.
TBSLogGenerator	External Tool	Dumps PCR values and TCG log in a human-readable format for the boot session when TBSLogGenerator.exe gets run.

25.5 Process Prerequisites

Use the below commands to generate certificates needed for the E2E flow (Refer www.openssl.org to get the tool):




- **Generate the private key and certificate**

```
openssl.exe req -x509 -newkey rsa:2048 -keyout pmt_private.pem -out pmt_certificate.bin -days 365 -nodes -outform DER -subj "/C=US/ST=Oregon//C=US/ST=Oregon/L=Portland/O=INTEL/OU=SSG/CN=PMF/O=INTEL/OU=SSG/CN=PMF pseudo-signing certificate"
```

- **Extract public key from private key**

```
openssl.exe rsa -in pmt_private.pem -outform PEM -pubout -out pmt_public.pem
```

These commands will generate the following files:

 pmt_certificate.bin
 pmt_private.pem
 pmt_public.pem

- Copy these files to the PMT folder



25.6 Intel® TDS Solution Compliance Test Coverage Summary

A= Automated, M= Manual, S= Semi-automated

Test ID	Test Case Title	How	Test Type
TDS_01	FW image Intel® TDS capable	A	Compliance
TDS_02	Intel® Boot Guard enabled	A	Compliance
TDS_03	Platform prerequisites	A	Compliance
TDS_04	Seal device in collection mode	A	Compliance
TDS_05	BIOS configuration lock	S	Compliance
TDS_06	Chassis intrusion lock	S	Compliance
TDS_07	SED lock	S	Compliance
TDS_08	Opt-out	S	Compliance
TDS_09	Dropship boot unseal check	S	Compliance



25.7 Intel® TDS Tests

25.7.1 TDS_01

Test ID:	TDS_01
Test Case Title:	FW Image Intel® TDS Capable
Mandatory/Optional	Mandatory
Test type:	Prerequisite
Description:	Check if the image has Intel® TDS enabled
Objective:	Ensures the image on the platform is TDS capable.
Procedure:	<p>Run Intel® MEInfo and verify that Intel® Trusted Device Setup shows Present/Enabled:</p> <p>FW Capabilities 0x7FF6D645</p> <p>Intel(R) Active Management Technology - PRESENT/ENABLED Protect Audio Video Path - PRESENT/ENABLED Intel(R) Dynamic Application Loader - PRESENT/ENABLED Service Advertisement & Discovery - PRESENT/ENABLED Intel(R) Platform Trust Technology - PRESENT/ENABLED Persistent RTC and Memory - PRESENT/ENABLED Intel(R) Trusted Device Setup - PRESENT/ENABLED</p>
Test Pass/Fail Criteria:	Test passes when Intel® Trusted Device Setup shows Present/Enabled.

25.7.2 TDS_02

Test ID:	TDS_02																																										
Test Case Title:	Intel® Boot Guard enabled																																										
Mandatory/ Optional	Mandatory																																										
Test Type:	Prerequisite																																										
Description:	Check that Intel® Boot Guard profile 5 is enabled, and startup from locality 3.																																										
Objective:	Ensures the boot flow is with secure and measured boot.																																										
Procedure:	<div>1. To check Intel® Boot Guard Profile, run Intel® MEInfo with -fwstatus flag.</div> <div>2. Parse Fwstatus6, if FACB[bit=0] == 1, PBE[bit=3] == 1, VB[bit=9] ==1, MB[bit=8] == 1 and ENF[bit=6:7] == 3, then it's Boot Guard profile 5 (According to the below table)</div> <div><div>BTG PROFILES</div><table><thead><tr><th>Profile</th><th>FACB</th><th>PBE</th><th>VB</th><th>MB</th><th>ENF</th><th>Comments</th></tr></thead><tbody><tr><td>0</td><td>0</td><td>0</td><td>0</td><td>0</td><td>0</td><td>BTG disabled</td></tr><tr><td>3</td><td>0</td><td>1</td><td>1</td><td>1</td><td>0</td><td>Debug profile</td></tr><tr><td>4</td><td>1</td><td>1</td><td>1</td><td>0</td><td>3</td><td>Strict profile</td></tr><tr><td>5</td><td>1</td><td>1</td><td>1</td><td>1</td><td>3</td><td>Strict profile + measured boot</td></tr><tr><td>6</td><td>1</td><td>1</td><td>1</td><td>0</td><td>0</td><td>Available in SPS only</td></tr></tbody></table></div> <div>3. To calculate Locality 3:<div>a. Reboot and Run TBSLogGenerator >log.txt</div><div>b. In log.txt, search for the event that includes a line with this format: PCR[00]= "Number" and the event does not have EV_NO_ACTION.</div></div> <div>Example:</div> <div><pre>****ID0001**0x0084-0x00d0***** Event 01: EV_S_CRTM_CONTENTS (0x00000007), 77 bytes for PCR[00] DIGEST = 812397d3441823ccc6fe375871159d47b769b5f82f1a26b66c6cb55d1e854e15 PCR[00] = 72fc9a838d68ad233649aea9f31c7568e69e2717f068ee392c6e593abca60b3d EventData (27 bytes): 00000000 42 6f 6f 74 20 47 75 61-72 64 20 4d 65 61 73 75 Boot Guard Measu 00000010 72 65 64 20 53 2d 43 52-54 4d 00 red S-CRTM ****ID0002**0x00d1-0x0104*****</pre></div> <div>4. Validate the following (DIGEST can be found in the same event of PCR[00]):hash256((0003 DIGEST) == PCR[00]</div> <div>(It is obtained from TBSLogGenerator. It is a Microsoft* tool that is released with the HLK)</div>	Profile	FACB	PBE	VB	MB	ENF	Comments	0	0	0	0	0	0	BTG disabled	3	0	1	1	1	0	Debug profile	4	1	1	1	0	3	Strict profile	5	1	1	1	1	3	Strict profile + measured boot	6	1	1	1	0	0	Available in SPS only
Profile	FACB	PBE	VB	MB	ENF	Comments																																					
0	0	0	0	0	0	BTG disabled																																					
3	0	1	1	1	0	Debug profile																																					
4	1	1	1	0	3	Strict profile																																					
5	1	1	1	1	3	Strict profile + measured boot																																					
6	1	1	1	0	0	Available in SPS only																																					
Test Pass/Fail Criteria:	Test passes when BtG profile is enabled and locality is 3.																																										

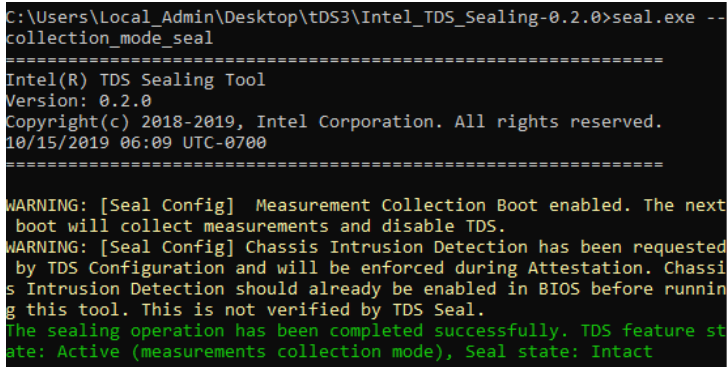
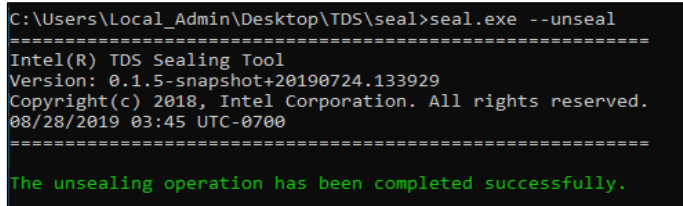


25.7.3 TDS_03

Test ID:	TDS_03
Test Case Title:	Platform prerequisites
Mandatory/Optional	Mandatory
Test Type:	Prerequisite
Description:	Checks that the platform prerequisites for Intel® TDS all apply to SUT: <ul style="list-style-type: none">• Platform is an Intel® vPro® machine• Platform contains SPI TPM 2.0 module
Objective:	To determine if the SUT has the prerequisites necessary for Intel® TDS.
Procedure:	<ol style="list-style-type: none">1. Check that platform is Intel® AMT capable by running Intel® MEInfo and seeing Intel® AMT is in the output (Disabled or Enabled).2. Open TPM.msc and check that Intel® PTT's state is "Ready for use".
Test Pass/Fail Criteria:	Test passes when Intel® MEInfo shows Intel® Active Management Technology – Present, and Intel® PTT state is "Ready for use".



25.7.4 TDS_04

Test ID:	TDS_04
Test Case Title:	Seal device in collection mode
Mandatory/Optional	Mandatory
Test Type:	Compliance
Description:	Prepare device for measurement collection by running the Seal in collection mode command.
Objective:	The device can be prepared for measurement collection
Procedure:	<ol style="list-style-type: none"> Run sealing tool in collection mode: Seal.exe --collection_mode_seal -c seal.ini Run unseal command: Seal.exe --unseal
Test Pass/Fail Criteria:	<ol style="list-style-type: none"> For step 1, the green color message indicates the test pass as "The sealing operation has been completed successfully. TDS feature state: Active (measurements collection mode), Seal state: Intact".  <pre> C:\Users\Local_Admin\Desktop\TDS3\Intel_TDS_Sealing-0.2.0>seal.exe --collection_mode_seal ===== Intel(R) TDS Sealing Tool Version: 0.2.0 Copyright(c) 2018-2019, Intel Corporation. All rights reserved. 10/15/2019 06:09 UTC-0700 ===== WARNING: [Seal Config] Measurement Collection Boot enabled. The next boot will collect measurements and disable TDS. WARNING: [Seal Config] Chassis Intrusion Detection has been requested by TDS Configuration and will be enforced during Attestation. Chassis Intrusion Detection should already be enabled in BIOS before running this tool. This is not verified by TDS Seal. The sealing operation has been completed successfully. TDS feature state: Active (measurements collection mode), Seal state: Intact </pre> For step 2, the following message appears:  <pre> C:\Users\Local_Admin\Desktop\TDS\seal>seal.exe --unseal ===== Intel(R) TDS Sealing Tool Version: 0.1.5-snapshot+20190724.133929 Copyright(c) 2018, Intel Corporation. All rights reserved. 08/28/2019 03:45 UTC-0700 ===== The unsealing operation has been completed successfully. </pre>



25.7.5 TDS_05

Test ID:	TDS_05
Test Case Title:	BIOS configuration lock
Mandatory/Optional	Mandatory
Test Type:	Compliance
Description:	On a platform with Intel® TDS enabled and set, check if BIOS configuration is locked and try accessing BIOS.
Objective:	To check if BIOS configuration lock is set on Intel® TDS enabled platforms, and that the lock works in protecting the BIOS from changes.
Procedure:	<ol style="list-style-type: none">1. In seal.ini, PlatformMeasurements.ini and svt.ini change set the following configurations: BIOSLockEnabled = 1 ChassisIntrusionEnabled= 0 SEDLockEnabled = 02. Run sealing flow from Section 25.8.1 (Full E2E Sealing) and validate the pass criteria is met.3. Reboot and try to access BIOS menus through the OEM specific key before OS loads. (By using Intel® IFWI, access to BIOS menu can be done by pressing F2 key during boot.)4. Access must be blocked.5. Run unseal command: Seal.exe --unseal
Test Pass/Fail Criteria:	<ol style="list-style-type: none">1. Test fails if Step 2 fails or BIOS is not locked and hence will be able to open BIOS menus.2. Step 5 output is as follows: <pre>C:\Users\Local_Admin\Desktop\TDS\seal>seal.exe --unseal ===== Intel(R) TDS Sealing Tool Version: 0.1.5-snapshot+20190724.133929 Copyright(c) 2018, Intel Corporation. All rights reserved. 08/28/2019 03:45 UTC-0700 ===== The unsealing operation has been completed successfully.</pre>



25.7.6 TDS_06

Test ID:	TDS_06
Test Case Title:	Chassis intrusion lock
Mandatory/Optional	Mandatory
Test Type:	Compliance (If chassis intrusion enabled in solution)
Description:	On platform with Intel® TDS enabled and set, check if chassis intrusion detection is working
Objective:	To check if chassis tampering detection is working when set in TDS
Procedure:	<ol style="list-style-type: none"> 1. In seal.ini, PlatformMeasurements.ini and svt.ini change set the following configurations: BIOSLockEnabled = 0 ChassisIntrusionEnabled = 1 SEDLockEnabled = 0 2. Run sealing flow from Section 25.8.1 (Full E2E Sealing) and validate the pass criteria is met. 3. Shut down. 4. Open the chassis 5. Power up and run get state using sealing tool: Seal.exe --get_state Output will include the Seal is broken, and the reason is Chassis intrusion detected. 6. Run unseal command: Seal.exe --unseal
Test Pass/Fail Criteria:	<ol style="list-style-type: none"> 1. Test pass if the output of step #5 contains the Seal state: broken and the string "Reason #2: 'Chassis Intrusion Detected'". 2. Step 6 output is as follows: <div data-bbox="760 1161 1336 1354" data-label="Text"> <pre> C:\Users\Local_Admin\Desktop\TDS\seal>seal.exe --unseal ===== Intel(R) TDS Sealing Tool Version: 0.1.5-snapshot+20190724.133929 Copyright(c) 2018, Intel Corporation. All rights reserved 08/28/2019 03:45 UTC-0700 ===== The unsealing operation has been completed successfully </pre> </div>



25.7.7 TDS_07

Test ID:	TDS_07
Test Case Title:	SED lock
Mandatory/Optional	Mandatory
Test Type:	Compliance
Description:	On a platform with Intel® TDS enabled and set, check if SED is locked
Objective:	To check if SED is locked when applying the seal
Procedure:	<ol style="list-style-type: none">1. In seal.ini, PlatformMeasurements.ini and svt.ini change set the following configurations: BIOSLockEnabled = 0 ChassisIntrusionEnabled= 0 SEDLockEnabled = 12. Run sealing flow from Section 25.8.1 (Full E2E Sealing) until step #9.3. Shut down.4. Replace the disk.5. Power up and run get state using sealing tool: Seal.exe --get_state Output will include the Seal is broken due to disk tampering.6. Run unseal command: Seal.exe --unseal
Test Pass/Fail Criteria:	<ol style="list-style-type: none">1. Test pass if the output of step #5 contains the Seal state: broken and the string "Reason #4: 'Disk Measurement Failed'".2. Step 6 output is as follows: <pre>C:\Users\Local_Admin\Desktop\TDS\seal>seal.exe --unseal ===== Intel(R) TDS Sealing Tool Version: 0.1.5-snapshot+20190724.133929 Copyright(c) 2018, Intel Corporation. All rights reserved. 08/28/2019 03:45 UTC-0700 ===== The unsealing operation has been completed successfully.</pre>



25.7.8 TDS_08

Test ID:	TDS_08
Test Case Title:	Opt-Out
Mandatory/Optional	Mandatory
Test Type:	Compliance
Description:	On a platform with Intel® TDS enabled and active: 1. Use a default opt out hotkey to opt out of Intel® TDS flow 2. Use a configured opt out key to opt out of Intel® TDS flow
Objective:	To check if opt out feature works, customizable opt out key works, and that once the opt-out is performed, the BIOS is no longer locked.
Procedure:	<ol style="list-style-type: none"> Run test TDS_05 steps 1-4 and validate it passes. Reboot and wait for PBA screen and enter default opt out keys {CTRL+ALT+o, CTRL+ALT+p, CTRL+ALT+t, CTRL+ALT+o}. To check opt out screen: Select "Yes" <div data-bbox="771 840 1421 1018" data-label="Image"> </div> <ol style="list-style-type: none"> On OS, Run seal.exe --get_state Seal state must be broken. Run unseal command: Seal.exe --unseal Repeat steps above and use the configured opt out keys. <p>Note: To change default, opt out keys, Open seal.ini file from Seal tool kit. Change CustomOptOutEnabled to 1 and change the OptOutHotKey to any optout keys that are not default (Allowed values are described in Section 4.8. "Opt-out hotkey" of the Intel® TDS_Sealing_Readme.txt file.</p>
Test Pass/Fail Criteria:	<p>Test passes if default opt-out keys work, and custom opt-out keys works. Sealing tool get state will show Seal state is Broken and the reason is "Reason #1: 'Aborted by the user - BIOS lock removed'":</p> <div data-bbox="678 1444 1421 1549" data-label="Text"> <pre>Seal log contains 3 events: - 10/15/2019 06:25 UTC-0700 - Seal Configured (Seal Instance ID: 3938101247) - 10/15/2019 06:25 UTC-0700 - Seal Enabled - 10/15/2019 06:40 UTC-0700 - Seal Broken (Boot Counter: 4, TDS Execution Counter: 4, Reason #1: 'Aborted by the user - BIOS Lock removed')</pre> </div>



25.7.9 TDS_09

Test ID:	TDS_09
Test Case Title:	Dropship boot unseal check
Mandatory/Optional	Mandatory
Test Type:	Compliance
Description:	Check if unseal works properly.
Objective:	To check the initial step by the end user, operates as expected.
Procedure:	<ol style="list-style-type: none">1. Apply seal if not applied (Using TDS_05 until step 4)2. Using Sealing tool to unseal the device with the following command: Seal.exe --unseal The following message appears: <pre>C:\Users\Local_Admin\Desktop\TDS\seal>seal.exe --unseal ===== Intel(R) TDS Sealing Tool Version: 0.1.5-snapshot+20190724.133929 Copyright(c) 2018, Intel Corporation. All rights reserved. 08/28/2019 03:45 UTC-0700 ===== The unsealing operation has been completed successfully.</pre>3. Run seal.exe --get_state Output will include "TDS feature state: Inactive, Seal state: Disabled".
Test Pass/Fail Criteria:	<p>Test passes when:</p> <ol style="list-style-type: none">1. Step 2 ends with the message "The unsealing operation has been completed successfully".2. Step 3 ends with the output "Intel® TDS feature state: Inactive, Seal state: Disabled".



25.8 Backup

25.8.1 Full E2E Sealing

Title	Full E2E Sealing
<p>Procedure:</p>	<ol style="list-style-type: none"> 1. Run sealing tool in collection mode: Seal.exe --collection_mode_seal -c seal.ini 2. Shutdown the machine using the command: shutdown /t 0 /f /s Then power on and wait for OS 3. In PMT tool folder, open PlatformMeasurements.ini and do the following: <ol style="list-style-type: none"> a. Validate the field ExpiryDate=YYYY-MM-DD has future date b. Assert [Seal Configuration] in seal.ini in Seal tool folder matches the configuration in the PlatformMeasurements.ini file in PMT folder c. Save file and exit. 4. Open CMD with Admin privileges and run the following command to generate the measurements file PlatformMeasurements.bin: Intel_TDS_PMTx64.exe GENPLATMSRFULL. 5. To Sign the PMF, Run the following command: Intel_TDS_PMTx64.exe GENSIGNEDBIN -fl signedBin.bin 6. This command will generate a signed PMF binary file signedBin.bin. Copy signedBin.bin to sealing tool folder 7. Seal the machine with the following command: Seal.exe --seal -g signedBin.bin 8. The message "machine sealed successfully" is outputted. 9. Shut down the machine. 10. Boot the machine and observe the PBA screen is seen instead of BIOS: <div data-bbox="803 1045 1396 1213" data-label="Image"> </div> <ol style="list-style-type: none"> 11. On OS, run sealing tool with the command: seal.exe --get_state The output will include "Intel® TDS feature state: Active, Seal State: Intact". 12. Copy TDS_TL3_Seal_Identity_File_***.csv from seal folder to SVT folder. 13. Run svt.exe --validate and make sure the tests are passed.
<p>Test Pass/Fail Criteria:</p>	<p>Test passes when the following applies:</p> <ol style="list-style-type: none"> 1. PBA screen seen on boot in step 10. 2. Step 11 output is "Intel® TDS feature state: active, Seal State: Intact". 3. Step 13 tests are passed.

§ §



A Appendix A — Intel® Trusted Execution Technology (Intel® TXT)

A.1 Provisioning Trusted Platform Module (TPM) for Intel® Trusted Execution Technology (Intel® TXT)

A.1.1 TPM 1.2 Background

Intel® TXT relies on three indices created in the TPM NVRAM area for operation:

1. AUX INDEX—This is an architectural index used by the ACMS.
2. PS (Platform Supplier) INDEX—This is a LCP (launch control policy) index intended to be used by the PS (OEM/ODM) to define default launch policy for the platform. Intel also uses this area in this index to define basic security policy (for example, SINIT revocation, NPW ACM restriction)
3. PO (Platform Owner) INDEX—This is LCP index intended to be used by the PO (IT, System Integrator, End User) to define launch control policy appropriate for the deployed environment.

Because the AUX and PS indices are used by Intel® TXT for basic operation, these indices must be properly defined, provisioned and protected before shipment to ensure proper Intel® TXT operation. Since the PO index is intended to be used in the deployed environment, this index should not be defined by platform suppliers in shipping systems.

A.1.2 TPM 1.2 Minimum Requirements

OEM/ODM need to make sure that following TPM provisioning steps are done prior to shipping the Intel® TXT enabled platform.

1. Define Auxiliary index
2. Define Platform Supplier index
3. Provision the Platform Supplier index as specified in the ACM distribution (ALLOW ANY policy with the desired SINIT revocation counter)
4. Lock the AUX and PS indices in the TPM NV area to prevent corruption (required for production signed ACM 1.0 and higher)

A.1.3 TPM 1.2 Intel Provided Development Tools

To enable BIOS testing and facilitate TPM provisioning tool development, Intel has provided the following:

ACM Packages/Bin—The Bin directory in the ACM packages contain provisioning scripts that are appropriate for the ACM being used. Because these provisioning scripts may change with the ACM releases, BIOS evaluators are encouraged to use the scripts that come with each ACM release.



Intel® TPM BDK (Intel® TPM BIOS Development Kit) – This kit contains scripts and reference code that can be used by the TPM vendor or OEM tool teams to create EFI based provisioning scripts appropriate for their manufacturing process. This kit provides the IBV/OEM with EFI based sample code and executable that provision a TPM for use with Intel® TXT. This tool kit contains documentation and build instructions that the user can use to create their own tools.

Note: These kits are for **reference only** and the example scripts should NOT be used to provision the TPM for BIOS testing or production provisioning.

The following sections describe the correct sequence to provision the TPM using the DOS scripts provided with ACM packages. The first section describes the required provisioning for SUT (system under test) based on ES (Engineering Sample) and debugged signed ACM (typically rev 0.5 to 0.9). The final section describes the required provisioning for SUT based on QS (Qual Samples) and production signed ACM (these are 0.9 NPW and 1.0+ releases).

A.1.4 TPM 1.2 Provisioning for Debug Signed ACM

A.1.4.1 Required Provisioning for Debugged Signed ACM

With the debugged signed ACM the provisioning steps below are required for Intel® TXT operation. These steps are applicable to ACM releases from 0.5 to 0.9 that are debugged signed.

1. **AUX2_DEF.BAT**—To define the AUX index space
2. **PS_DEF.BAT**—To define the PS index space
3. **PS_ANY.BAT**—To provision the PS as required by the ACM

A.1.4.2 Optional Provisioning for Debugged Signed ACM

If test plan includes test cases for PO (platform owner) policies, following scripts can be used to facilitate the PO provision process. These scripts are not provided with ACM package and are available upon request.

1. **EK.BAT**—If TPM does not provide default EK
2. **TAKE_OWN.BAT**—Ownership is required for PO definition
3. **POA_DEF.BAT**—To define the PO index space
4. **Install the test PO policy**—The POA_ANY.BAT can be modified to make the policy appropriate for testing SW

A.1.5 TPM 1.2 Provisioning for Production Signed ACM

A.1.5.1 Required Provisioning for Production Signed ACM

Production signed ACM requires that the NV indices be locked. The exception to this lock requirement are the ACM that has been tagged as NPW (non-production worthy). For NPW production signed ACM, the NV indices do not have to be locked however the PS index needs to be provisioned to allow NPW ACM execution. The appropriate PS provisioning scripts are distributed with the ACM.



For production signed ACM the provisioning steps are listed below. These ACMs typically are releases 1.0 and higher or 0.9 releases that are tagged NPW. The steps are similar to debug signed ACM with the additional locking requirement or the PS provision for NPW ACM execution

1. **AUX2_DEF.BAT**—To define the AUX index space
2. **PS_DEF.BAT**—To define the PS index space
3. **PS_ANY.BAT** or **PS_NPW.BAT**— To provision the PS as required by the ACM. NPW ACM (.9x production signed) and production ACM (1.x production signed) have different scripts; make sure you're running the one that comes with ACM.

Required—For ACM 1.0 and higher

4. **NV_LOCK.BAT**—This locks the indices in the TPM NVRAM

Note: This locking is permanent on most TPM. Some TPM do provide a RevokeTrust mechanism that would clear the lock.

Strong Recommendation—In addition to the required steps listed above, the following write protection of the PS index is strongly recommended to maintain index integrity.

5. **PS_WP.BAT**—Write protects the PS index.

Note: This is not required for basic operation however Intel recommends write protecting the PS on production platforms.

A.1.5.2 TPM 1.2 Optional Provisioning for Production Signed ACM

Similar to optional provisioning for the debug signed ACM above. If test plan includes test cases for PO (platform owner) policies, following scripts can be used to facilitate the PO provision process. These scripts are not provided with ACM package and are available upon request.

1. **EK.BAT**—If TPM does not provide default EK
2. **TAKE_OWN.BAT**—Ownership is required for PO definition
3. **PO_DEF.BAT**—To define the PO index space
4. **Install the test PO policy**—The PO_ANY.BAT can be modified to make the policy appropriate for testing SW

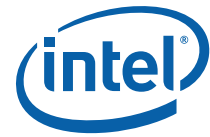
A.1.6 TPM 2.0 Background

Intel® TXT relies on TPM capability and requirements are defined by the Trusted Computer Group (TCG), an industry initiative “formed to develop, define and promote open, vendor-neutral, industry standards for trusted computing building blocks and software interfaces across multiple platforms.

The chipset and TPM together provide a certain level of ‘protection’. Both platform and TPM hardware enforce the rules, which are different for different localities as follows:

There are five localities (0 – 4), each locality is mapped to a 4K address range in the Intel Trusted Execution Technology (Intel TXT) configuration space starting at 0FED4_0000.

Locality 0: 0FED4_0XXX - General Locality (Can always be accessed)



Locality 1: 0FED4_1XXX - Not defined/reserved for use by any OS
Locality 2: 0FED4_2XXX - available to the MLE, only after a measured launch
Locality 3: 0FED4_3XXX - only accessible by Intel ACM code after authentication
Locality 4: 0FED4_4XXX - only accessible by the hardware (processor microcode)

Note: BIOS and provisioning tools only use Locality 0

Here are some new TPM Concepts:

- Hierarchies (specifically Platform Hierarchy)
- Command and Response
- Additional hashing and encryption algorithms
- Algorithm Agility
- Authorizations and Enhanced Authorization
- Policy Sessions
- Parameter encryption
- TPM Non-Volatile memory (NVRAM) Operations

Platform Hierarchy:

Unlike TPM 1.2 family where the OEM had to create TPM objects (for example, AUX and PS Policy NVRAM Indexes) and then lock the TPM preventing anyone from deleting or modifying their definitions, TPM 2.0 defines 3 hierarchies that are independent of each other. These are the Platform Hierarchy, Storage Hierarchy, and Endorsement Hierarchy.

The Platform Hierarchy is dedicated for the platform vendor while the Storage Hierarchy and Endorsement Hierarchy are dedicated for the platform owner. This document only deals with the Platform Hierarchy (PH). Each hierarchy has its own authorization value (AuthValue) and authorization policy (authPolicy). More on authorization policies later, but authPolicy is an alternative way to demonstrate authorization to use the PH.

This means that there is no longer the notion of a LOCKED TPM and the OEM now be able to add, delete, and provision its TPM objects at any time. Unlike the other hierarchies, which have persistent authorization values, the PH authValue and authPolicy are cleared each time the platform resets. It is the BIOS responsibility to establish the PH authValue (and optionally the PH authPolicy) on each platform reset.

The notion is that BIOS set PH authValue to a random value, use that value if it needs to perform any operations that require PH authorization and then flush that value from memory (or store it in a protected location) before any executing any untrusted code (option ROMs, boot code, and so forth.).

A.1.7 TPM 2.0 Minimum Requirements

The OEM must provision the TPM before the platform is put into use. This may be done before the TPM is attached to the platform, during the platform manufacturing/testing process, or automatically the first time the platform boots. At a minimum this requires:

1. Creating the AUX Index and PS Index
2. Writing the PS index with a valid TXT Policy



Furthermore, the OEM must select an authPolicy for the PS index that allows only the OEM to write the PS index. Typically this policy also allows the OEM to delete the index. The OEM must protect against unauthorized modification or deletion of the index – this includes guarding the passwords, authorization values, and keys required to modify or delete the index.

A.1.8 TPM 2.0 Intel Provided Development Tools

To enable BIOS testing and facilitate TPM provisioning tool development, Intel has provided the following:

ACM Packages—The root directory in the ACM packages contain provisioning script(TPM2Prov.efi) that is appropriate for the ACM being used. Because the provisioning script may change with the ACM releases, BIOS evaluators are encouraged to use the script that come with each ACM release.

Intel® TPM BDK (Intel® TPM BIOS Development Kit) – This kit contains scripts and reference code that can be used by the TPM vendor or OEM tool teams to create EFI based provisioning scripts appropriate for their manufacturing process. This kit provides the IBV/OEM with EFI based sample code and executable that provision a TPM for use with Intel® TXT. This tool kit contains documentation and build instructions that the user can use to create their own tools. (**TPM2prov.efi**).

Note: These kits are for **reference only** and the example scripts should NOT be used to provision the TPM for BIOS testing or production provisioning.

A.1.9 TPM 2.0 Provisioning for Debug Signed ACM

A.1.9.1 Required Provisioning for Debugged Signed ACM

With the debugged signed ACM the provisioning steps below are required for Intel® TXT operation. These steps are applicable to ACM releases from 0.5 to 0.9 that are debugged signed.

Once you download the ACM kit user need to complete the following two steps.

1. **Define_AUX.nsh** —To define the AUX index space
2. **Define_PS.nsh** —To define the PS index space

Below is a sample output observed on execution of TPM provisioning commands:

1. Define_AUX.nsh

```
Define_AUX.nsh
2.0 FS0:\TPM2ProvTool\> echo -off
Creating Aux Index.
Clearing AUXDeletionControl flag in PS Policy
Start Policy Session
Policy OR (Branch A, Branch B, Branch C)
Writing PS Policy to clear AUXDeletionControl flag
Flush Session 0
AUX Define
```

2. Define_PS.nsh

```
Define_PS.nsh
```




```
2.0 FS0:\TPM2ProvTool\> echo -off
Start Policy Session
Policy Command Code (0, TPM_CC_NV_UndefineSpaceSpecial)
Policy OR (Branch A, Branch B, Branch C)
UndefineSpecial PS_Def.iDef
PS Define
Flush Session 0
Writing PS Policy
Start Policy Session
Policy OR (Branch A, Branch B, Branch C)
Writing NV Data
Flush Session 0
```

A.1.10 TPM 2.0 Provisioning for Production Signed ACM

A.1.10.1 Required Provisioning for Production Signed ACM

Tool for TPM 2.0 Provisioning for Production Signed ACM is released at the Production Candidate (PC) milestone of Broadwell Platform.

A.1.11 TPM 2.0 WinPE Based TPM Provisioning

Similar to TPM1.2 WinPE based provisioning tool as described in Section B.1.6, Intel provides WinPE4.0 based TPM 2.0 Provisioning at the Broadwell Beta milestone. This tool is supported on Microsoft* WinPE or Windows* 8/8.1 Administrative command prompt.

A.2 Intel® TXT Trusted Boot (Tboot) Usage

Intel Corporation has submitted TXT reference code (Tboot) to sourceforge which enables Xen* and Linux* to use Intel® TXT for verified launch to build an Intel® TXT MLE. An Intel® TXT MLE (Tboot launched Xen* or Linux*) is an excellent tool for Intel® TXT checkout.

In addition to verifying that the processor, chipset, TPM and AC modules can collaborate do a measured launch, tboot has a descriptive serial output that can help root cause Intel® TXT measured launch issues.

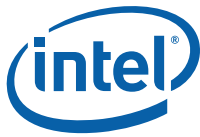
This section describes how to use tboot-linux and tboot-xen for Intel® TXT checkout.

A.2.1 Available Tboot Test Images

A.2.1.1 Pre-Built Tboot-Linux* Live Image

To facilitate Intel® TXT evaluation, Intel has provided a Tboot evaluation kit, *Intel® Trusted Execution Technology Evaluation Kit—Trusted Boot (tboot) Usage Image*. This kit contains an ISO image of a bootable Tboot-Linux* environment using Fedora 19. This ISO image can be used to create a bootable MLE on a USB Drive or DVD.

For complete instruction on how build a Tboot-Linux* image refer the README file located at the Mercurial Repo (<http://www.bughost.org/repos.hg/tboot.hg/file/9c733d6c3f40/README>).



A.2.2 Invoking Tboot

With a bootable tboot image prepared either through using the Live Image or by building it from the reference code, invoking tboot is just a matter of selecting the tboot option from the grub menu. Below are the typical steps needed to launch tboot:

1. Verify that platform is ready for Intel® TXT measured launch
2. Enable all the required settings in the BIOS: TPM, Intel® VT, Intel® VT-d, Intel® TXT
3. Boot the system and select the tboot entry from grub menu.

A.2.3 Verifying Tboot Launch

A.2.3.1 Using txt-stat

If the tboot launch completed into either Linux* or Xen*, the Linux* executable **txt-stat** can be used to verify a successful launch. **txt-stat** is included in the tboot package. It distributed with the Tboot-Linux* Live Image, refer the package instruction for details. **txt-stat** is also compiled by default if the tboot package was compiled at the root level.

To run **txt-stat**:

1. Login to MLE as root
2. Open a shell
3. Change to the directory that contains **txt-stat**
4. Invoke **txt-stat** from the command line using

```
shell> txt-stat
```

The **txt-stat** command reports the current status of TXT environment. You may also access the txt-stat 'log' if you use LiveUSB for launching the Tboot LiveImage. Log file is stored on USB flash drive under root/logs folder.

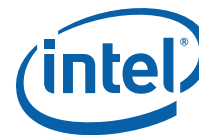
To confirm successful execution, look for the following entry in **txt-stat** output:

```
*****
      TXT measured launch: TRUE
      secrets flag set: TRUE
*****
```

A.2.3.2 Sample txt-stat Output

Intel(r) TXT Configuration Registers:

```
STS: 0x00018091
    sender_done: TRUE
    sexit_done: FALSE
    mem_unlock: TRUE
    mem_config_lock: FALSE
    private_open: TRUE
    mem_config_ok: FALSE
ESTS: 0x00
    txt_reset: FALSE
    txt_wake_error: FALSE
```



```

E2STS: 0x0000000000000006
  slp_entry_error: FALSE
  secrets: TRUE
  block_mem: TRUE
  reset: FALSE
ERRORCODE: 0x00000000
DIDVID: 0x00000001b0018086
  vendor_id: 0x8086
  device_id: 0xb001
  revision_id: 0x1
SINIT.BASE: 0xaaaf00000
SINIT.SIZE: 131072B (0x20000)
HEAP.BASE: 0xaaaf20000
HEAP.SIZE: 917504B (0xe0000)
DPR: 0x00000000ab000041
  lock: TRUE
  top: 0xab000000
  size: 4MB (4194304B)
*****
TXT measured launch: TRUE
secrets flag set: TRUE
*****
ERROR: reading TXT heap failed by read()
TBOOT log:
  max_size=7fe4
  curr_pos=4d51
  buf:
TBOOT: ***** TBOOT *****
TBOOT: 2013-11-21 22:24 -0400 206:9c733d6c3f40
TBOOT: *****
TBOOT: command line: boot=linux logging=vga,serial,memory
TBOOT: BSP is cpu 0
TBOOT: original e820 map:
TBOOT: 0000000000000000 - 000000000009bc00 (1)
TBOOT: 000000000009bc00 - 00000000000a0000 (2)
TBOOT: 00000000000a0000 - 0000000000010000 (2)
TBOOT: 0000000000010000 - 00000000aa90d000 (1)
TBOOT: 00000000aa90d000 - 00000000aa9e7000 (2)
TBOOT: 00000000aa9e7000 - 00000000aabe7000 (4)
TBOOT: 00000000aabe7000 - 00000000aabff000 (3)
TBOOT: 00000000aabff000 - 00000000aac00000 (1)
TBOOT: 0000000100000000 - 000000014e000000 (1)
TBOOT: 00000000aac00000 - 00000000b0000000 (2)
TBOOT: 00000000f8000000 - 00000000fc000000 (2)
TBOOT: 00000000fec00000 - 00000000fec01000 (2)
TBOOT: 00000000fed10000 - 00000000fed14000 (2)
TBOOT: 00000000fed18000 - 00000000fed1a000 (2)
TBOOT: 00000000fed1c000 - 00000000fed20000 (2)
TBOOT: 00000000fee00000 - 00000000fee01000 (2)
TBOOT: 00000000ff980000 - 00000000ffc00000 (2)
TBOOT: 00000000ffd80000 - 0000000100000000 (2)
TBOOT: TPM is ready

```



```
...  
txt-stat message deleted for clarity.  
...  
BOOT: VMXOFF done for cpu 6  
TBOOT: cpu 6 waking up, SIPI vector=10000  
TBOOT: VMXOFF done for cpu 1  
TBOOT: cpu 1 waking up, SIPI vector=10000  
TBOOT: VMXOFF done for cpu 3  
TBOOT: cpu 3 waking up, SIPI vector=10000  
TBOOT: VMXOFF done for cpu 5  
TBOOT: cpu 5 waking up, SIPI vector=10000  
TBOOT: VMXOFF done for cpu 7  
TBOOT: cpu 7 waking up, SIPI vector=10000
```

A.2.3.3 Using Serial Port

The best method to verify a tboot launch is to view the serial output. With serial connection connected to the SUT with baud rate at 115200, the tboot log entry can view to confirm successful measured launching.

Note: While ACM serial out debug message requires BIOS to explicitly use 0x3F8 port for capturing the log, Tboot LiveImage serial can be captured using any available/connect serial (COM) port on the platform.

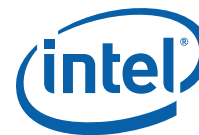
Key entries to verify from the serial output are:

1. Confirmation from tboot that HW and SW components are ready for Intel® TXT measured launch recognized. These component confirmations are as follow:
 - i. TBOOT: TPM is ready
 - ii. TBOOT: TXT chipset and all needed capabilities present
 - iii. TBOOT: CPU is ready for SENTER
 - iv. TBOOT: SINIT matches platform
2. Confirmation that tboot is executing a measured launch using GETSEC[SENDER]. The message to verify this is:
 - i. TBOOT: executing GETSEC[SENDER]...
3. The next entries to look for are confirmations that measured launch have completed successfully. The messages to verify this are:
 - i. TBOOT: measured launch succeeded
 - ii. TBOOT: set LT.CMD.SECRETS flag
4. Last step is confirmation that tboot has successful transferred control to MLE. Below are examples of transfer messages to Linux* and Xen*.
 - i. TBOOT: transferring control to kernel @0x00c00000...
 - ii. TBOOT: transferring control to xen @0x00100000...

A.2.3.4 Sample Serial Output Tboot Linux

Below is a sample serial port output captured from an Intel® TXT Tboot-Linux* measured boot.

This log may be different from the log in validation environment due to differences in system configuration, BIOS implementation and Intel® TXT patch version applied.



```

TBOOT: ***** TBOOT *****
TBOOT:      2013-11-21 22:24 -0400 206:9c733d6c3f40
TBOOT: *****
TBOOT: command line: boot=linux logging=vga,serial,memory
TBOOT: BSP is cpu 0
TBOOT: original e820 map:
TBOOT: 0000000000000000 - 0000000000009bc00 (1)
TBOOT: 0000000000009bc00 - 000000000000a0000 (2)
TBOOT: 000000000000e0000 - 00000000000100000 (2)
TBOOT: 00000000000100000 - 00000000aa90d000 (1)
TBOOT: 00000000aa90d000 - 00000000aa9e7000 (2)
TBOOT: 00000000aa9e7000 - 00000000aabe7000 (4)
TBOOT: 00000000aabe7000 - 00000000aabff000 (3)
TBOOT: 00000000aabff000 - 00000000aac00000 (1)
TBOOT: 0000000100000000 - 000000014e000000 (1)
TBOOT: 00000000aac00000 - 00000000b0000000 (2)
TBOOT: 00000000f8000000 - 00000000fc000000 (2)
TBOOT: 00000000fec00000 - 00000000fec01000 (2)
TBOOT: 00000000fed10000 - 00000000fed14000 (2)
TBOOT: 00000000fed18000 - 00000000fed1a000 (2)
TBOOT: 00000000fed1c000 - 00000000fed20000 (2)
TBOOT: 00000000fee00000 - 00000000fee01000 (2)
TBOOT: 00000000ff980000 - 00000000ffc00000 (2)
TBOOT: 00000000ffd80000 - 0000000100000000 (2)
TBOOT: TPM is ready
TBOOT: TPM nv_locked: FALSE
TBOOT: TPM timeout values: A: 0, B: 0, C: 10, D: 10
TBOOT: TPM: tpm_get_nvindex_size() response size incorrect
TBOOT: failed to get actual policy size in TPM NV
TBOOT: failed to read policy from TPM NV, using default
TBOOT: policy:
TBOOT:   version: 2
TBOOT:   policy_type: TB_POLTYPE_CONT_NON_FATAL
TBOOT:   hash_alg: TB_HALG_SHA1
TBOOT:   policy_control: 00000001 (EXTEND_PCR17)
TBOOT:   num_entries: 2
TBOOT:   policy entry[0]:
TBOOT:     mod_num: 0
TBOOT:     pcr: none
TBOOT:     hash_type: TB_HTYPE_ANY
TBOOT:     num_hashes: 0
TBOOT:   policy entry[1]:
TBOOT:     mod_num: any
TBOOT:     pcr: 19
TBOOT:     hash_type: TB_HTYPE_ANY
TBOOT:     num_hashes: 0
TBOOT: TPM: write nv 20000002, offset 00000000, 00000004 bytes, return =
00000000
2
TBOOT: Error: write TPM error: 0x2.
TBOOT: no policy in TPM NV.

```



```
TBOOT: IA32_FEATURE_CONTROL_MSR: 0000ff07
TBOOT: CPU is SMX-capable
TBOOT: CPU is VMX-capable
TBOOT: SMX is enabled
TBOOT: TXT chipset and all needed capabilities present
TBOOT: TXT.ERRORCODE=0
TBOOT: LT.ESTS=0
TBOOT: IA32_FEATURE_CONTROL_MSR: 0000ff07
TBOOT: CPU is SMX-capable
TBOOT: CPU is VMX-capable
TBOOT: SMX is enabled
TBOOT: TXT chipset and all needed capabilities present
TBOOT: bios_data (@aaf20008, 2c):
TBOOT:  version: 3
TBOOT:  bios_sinit_size: 0x0 (0)
TBOOT:  lcp_pd_base: 0x0
TBOOT:  lcp_pd_size: 0x0 (0)
TBOOT:  num_logical_procs: 8
TBOOT:  flags: 0x00000000
TBOOT: CR0 and EFLAGS OK
TBOOT: supports preserving machine check errors
TBOOT: CPU is ready for SENTER
TBOOT: checking previous errors on the last boot.
      TPM: read nv index 20000002 offset 00000000, return value = 00000002
TBOOT: Error: read TPM error: 0x2.
TBOOT: last boot has no error.
TBOOT: chipset ids: vendor: 0x8086, device: 0xb001, revision: 0x1
TBOOT: chipset production fused: 0
TBOOT: checking if module SNB_SINIT_20100502_debug.bin is an SINIT for
this platform...
TBOOT:  2 ACM chipset id entries:
TBOOT:      vendor: 0x8086, device: 0xb001, flags: 0x1, revision: 0x1,
extended
: 0x1
TBOOT: SINIT matches platform
TBOOT: copied SINIT (size=b000) to aaf00000
TBOOT: AC mod base alignment OK
TBOOT: AC mod size OK
TBOOT: AC module header dump for SINIT:
TBOOT:  type: 0x2 (ACM_TYPE_CHIPSET)
TBOOT:  length: 0xa1 (161)
TBOOT:  version: 0
TBOOT:  chipset_id: 0xb001
TBOOT:  flags: 0x8000
TBOOT:  pre_production: 0
TBOOT:  debug_signed: 1
TBOOT:  vendor: 0x8086
TBOOT:  date: 0x20100502
TBOOT:  size*4: 0xb000 (45056)
TBOOT:  code_control: 0x0
TBOOT:  entry point: 0x00000008:00003094
TBOOT:  scratch_size: 0x8f (143)
```



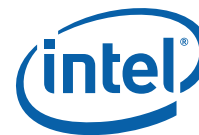
```

TBOOT:  info_table:
TBOOT:  uuid: {0x7fc03aaa, 0x46a7, 0x18db, 0xac2e,
             {0x69, 0x8f, 0x8d, 0x41, 0x7f, 0x5a}}
TBOOT:      ACM_UUID_V3
TBOOT:  chipset_acm_type: 0x1 (SINIT)
TBOOT:  version: 3
TBOOT:  length: 0x28 (40)
TBOOT:  chipset_id_list: 0x4e8
TBOOT:  os_sinit_data_ver: 0x5
TBOOT:  min_mle_hdr_ver: 0x00020000
TBOOT:  capabilities: 0x0000000e
TBOOT:      rlp_wake_getsec: 0
TBOOT:      rlp_wake_monitor: 1
TBOOT:      ecx_pgtbl: 1
TBOOT:  acm_ver: 16
TBOOT:  chipset list:
TBOOT:  count: 2
TBOOT:  entry 0:
TBOOT:      flags: 0x1
TBOOT:      vendor_id: 0x8086
TBOOT:      device_id: 0xb001
TBOOT:      revision_id: 0x1
TBOOT:      extended_id: 0x1
TBOOT:  entry 1:
TBOOT:      flags: 0xb0008086
TBOOT:      vendor_id: 0x1
TBOOT:      device_id: 0x0
TBOOT:      revision_id: 0x0
TBOOT:      extended_id: 0x0
TBOOT:  file addresses:
TBOOT:  &_start=00803000
TBOOT:  &_end=0087ccb4
TBOOT:  &_mle_start=00803000
TBOOT:  &_mle_end=00821000
TBOOT:  &_post_launch_entry=00803020
TBOOT:  &_txt_wakeup=008031f0
TBOOT:  &g_mle_hdr=008175c0
TBOOT:  MLE header:
TBOOT:  uuid={0x9082ac5a, 0x476f, 0x74a7, 0x5c0f,
           {0x55, 0xa2, 0xcb, 0x51, 0xb6, 0x42}}
TBOOT:  length=34
TBOOT:  version=00020001
TBOOT:  entry_point=00000020
TBOOT:  first_valid_page=00000000
TBOOT:  mle_start_off=0
TBOOT:  mle_end_off=1e000
TBOOT:  capabilities: 0x00000007
TBOOT:      rlp_wake_getsec: 1
TBOOT:      rlp_wake_monitor: 1
TBOOT:      ecx_pgtbl: 1
TBOOT:  MLE start=803000, end=821000, size=1e000
TBOOT:  ptab_size=3000, ptab_base=00800000

```



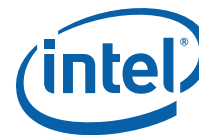
```
TBOOT: bios_data (@aaf20008, 2c):
TBOOT: version: 3
TBOOT: bios_sinit_size: 0x0 (0)
TBOOT: lcp_pd_base: 0x0
TBOOT: lcp_pd_size: 0x0 (0)
TBOOT: num_logical_procs: 8
TBOOT: flags: 0x00000000
TBOOT: discarding RAM above reserved regions: 0xaabff000 - 0xaac00000
TBOOT: min_lo_ram: 0x0, max_lo_ram: 0xaa90d000
TBOOT: min_hi_ram: 0x100000000, max_hi_ram: 0x14e000000
TBOOT: no LCP module found
TBOOT: os_sinit_data (@aaf30154, 64):
TBOOT: version: 5
TBOOT: mle_ptab: 0x800000
TBOOT: mle_size: 0x1e000 (122880)
TBOOT: mle_hdr_base: 0x145c0
TBOOT: vtd_pmr_lo_base: 0x0
TBOOT: vtd_pmr_lo_size: 0xaa800000
TBOOT: vtd_pmr_hi_base: 0x100000000
TBOOT: vtd_pmr_hi_size: 0x4e000000
TBOOT: lcp_po_base: 0x0
TBOOT: lcp_po_size: 0x0 (0)
TBOOT: capabilities: 0x00000002
TBOOT: rlp_wake_getsec: 0
TBOOT: rlp_wake_monitor: 1
TBOOT: ecx_pgtbl: 0
TBOOT: efi_rsdtd_ptr: 0x0
TBOOT: setting MTRRs for acmod: base=aaf00000, size=b000, num_pages=11
TBOOT: executing GETSEC[SENTER]...
TBOOT: ***** TBOOT *****
TBOOT: 2010-06-21 22:24 -0400 206:9c733d6c3f40
TBOOT: *****
TBOOT: command line: boot=linux logging=vga,serial,memory
TBOOT: BSP is cpu 0
TBOOT: original e820 map:
TBOOT: 0000000000000000 - 000000000009bc00 (1)
TBOOT: 000000000009bc00 - 00000000000a0000 (2)
TBOOT: 00000000000a0000 - 0000000000100000 (2)
TBOOT: 0000000000100000 - 00000000aa90d000 (1)
TBOOT: 00000000aa90d000 - 00000000aa9e7000 (2)
TBOOT: 00000000aa9e7000 - 00000000aabe7000 (4)
TBOOT: 00000000aabe7000 - 00000000aabff000 (3)
TBOOT: 00000000aabff000 - 00000000aac00000 (1)
TBOOT: 00000000aac00000 - 0000000014e00000 (1)
TBOOT: 0000000014e00000 - 00000000b0000000 (2)
TBOOT: 00000000b0000000 - 00000000fc000000 (2)
TBOOT: 00000000fc000000 - 00000000fec01000 (2)
TBOOT: 00000000fec01000 - 00000000fed14000 (2)
TBOOT: 00000000fed14000 - 00000000fed1a000 (2)
TBOOT: 00000000fed1a000 - 00000000fed20000 (2)
TBOOT: 00000000fed20000 - 00000000fee01000 (2)
TBOOT: 00000000fee01000 - 00000000ff980000 (2)
TBOOT: 00000000ff980000 - 00000000ffc00000 (2)
```

```
TBOOT: 00000000ffd80000 - 0000000100000000 (2)
TBOOT: TPM is ready
TBOOT: TPM nv_locked: FALSE
TBOOT: TPM timeout values: A: 0, B: 0, C: 10, D: 10
TBOOT: TPM: tpm_get_nvindex_size() response size incorrect
TBOOT: failed to get actual policy size in TPM NV
TBOOT: failed to read policy from TPM NV, using default
TBOOT: policy:
TBOOT:  version: 2
TBOOT:  policy_type: TB_POLTYPE_CONT_NON_FATAL
TBOOT:  hash_alg: TB_HALG_SHA1
TBOOT:  policy_control: 00000001 (EXTEND_PCR17)
TBOOT:  num_entries: 2
TBOOT:  policy entry[0]:
TBOOT:  mod_num: 0
TBOOT:  pcr: none
TBOOT:  hash_type: TB_HTYPE_ANY
TBOOT:  num_hashes: 0
TBOOT:  policy entry[1]:
TBOOT:  mod_num: any
TBOOT:  pcr: 19
TBOOT:  hash_type: TB_HTYPE_ANY
TBOOT:  num_hashes: 0
TBOOT: TPM: write nv 20000002, offset 00000000, 00000004 bytes, return =
00000000
2
TBOOT: Error: write TPM error: 0x2.
TBOOT: no policy in TPM NV.
TBOOT: IA32_FEATURE_CONTROL_MSR: 0000ff07
TBOOT: CPU is SMX-capable
TBOOT: CPU is VMX-capable
TBOOT: SMX is enabled
TBOOT: TXT chipset and all needed capabilities present
TBOOT: TXT.ERRORCODE=c0000001
TBOOT: AC module error: acm_type=1, progress=00, error=0
TBOOT: LT.ESTS=0
TBOOT: IA32_FEATURE_CONTROL_MSR: 0000ff07
TBOOT: CPU is SMX-capable
TBOOT: CPU is VMX-capable
TBOOT: SMX is enabled
TBOOT: TXT chipset and all needed capabilities present
TBOOT: bios_data (@aaf20008, 2c):
TBOOT:  version: 3
TBOOT:  bios_sinit_size: 0x0 (0)
TBOOT:  lcp_pd_base: 0x0
TBOOT:  lcp_pd_size: 0x0 (0)
TBOOT:  num_logical_procs: 8
TBOOT:  flags: 0x00000000
TBOOT: measured launch succeeded
TBOOT: bios_data (@aaf20008, 2c):
TBOOT:  version: 3
TBOOT:  bios_sinit_size: 0x0 (0)
```



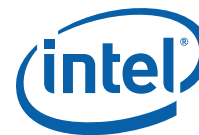
```
TBOOT: lcp_pd_base: 0x0
TBOOT: lcp_pd_size: 0x0 (0)
TBOOT: num_logical_procs: 8
TBOOT: flags: 0x00000000
TBOOT: os_mle_data (@aaf20034, 10120):
TBOOT: version: 2
TBOOT: mbi: 0x000101b0
TBOOT: os_sinit_data (@aaf30154, 64):
TBOOT: version: 5
TBOOT: mle_ptab: 0x800000
TBOOT: mle_size: 0x1e000 (122880)
TBOOT: mle_hdr_base: 0x145c0
TBOOT: vtd_pmr_lo_base: 0x0
TBOOT: vtd_pmr_lo_size: 0xaa800000
TBOOT: vtd_pmr_hi_base: 0x100000000
TBOOT: vtd_pmr_hi_size: 0x4e000000
TBOOT: lcp_po_base: 0x0
TBOOT: lcp_po_size: 0x0 (0)
TBOOT: capabilities: 0x00000002
TBOOT:     rlp_wake_getsec: 0
TBOOT:     rlp_wake_monitor: 1
TBOOT:     ecx_pgtbl: 0
TBOOT: efi_rsdt_ptr: 0x0
TBOOT: sinit_mle_data (@aaf301b8, 22c):
TBOOT: version: 8
TBOOT: bios_acm_id:
      80 00 00 00 20 10 05 02 80 00 b0 01 ff ff ff ff ff ff ff ff
TBOOT: edx_senter_flags: 0x00000000
TBOOT: mseg_valid: 0x0
TBOOT: sinit_hash:
      d1 b1 1d 67 4e e0 9d 61 f0 67 36 08 5c 2c 1e bc ea a5 07 77
TBOOT: mle_hash:
      00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
TBOOT: stm_hash:
      00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
TBOOT: lcp_policy_hash:
      00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
TBOOT: lcp_policy_control: 0x00000002
TBOOT: rlp_wakeup_addr: 0xaaaf018a0
TBOOT: num_mdrs: 7
TBOOT: mdrs_off: 0x9c
TBOOT: num_vtd_dmars: 232
TBOOT: vtd_dmars_off: 0x144
TBOOT: sinit_mdrs:
TBOOT: 0000000000000000 - 00000000000a0000 (GOOD)
TBOOT: 0000000000100000 - 0000000000f00000 (GOOD)
TBOOT: 0000000001000000 - 00000000aaaf0000 (GOOD)
TBOOT: 0000000100000000 - 000000014e000000 (GOOD)
TBOOT: 0000004000000000 - 0000005380000000 (GOOD)
TBOOT: 0000000ab0000000 - 0000000ab8000000 (SMRAM NON-OVERLAY)
TBOOT: 0000000000000cfc - 000000000100cfc (PCIE EXTENDED CONFIG)
TBOOT: proc_scrtm_status: 0x00000000
```



```
TBOOT: RSDP (v002 INTEL) @ 0x000f0410
TBOOT: Seek in XSDT...
TBOOT: entry[0] sig = FACP @ 0xaab85d98
TBOOT: entry[1] sig = APIC @ 0xaabfcf18
TBOOT: acpi_table_ioapic @ aabfcfc4,.address = fec00000
TBOOT: RSDP (v002 INTEL) @ 0x000f0410
TBOOT: Seek in XSDT...
TBOOT: entry[0] sig = FACP @ 0xaab85d98
TBOOT: entry[1] sig = APIC @ 0xaabfcf18
TBOOT: entry[2] sig = TCPA @ 0xaaba4d18
TBOOT: entry[3] sig = MCFG @ 0xaaba4c98
TBOOT: acpi_table_mcfg @ aaba4c98,.base_address = f8000000
TBOOT: mtrr_def_type: e = 1, fe = 1, type = 0
TBOOT: mtrrs:
TBOOT: basemasktypev
TBOOT: 000000f800000061
TBOOT: 080000fe00000061
TBOOT: 0a0000ff80000061
TBOOT: 0a8000ffe0000061
TBOOT: 0aa000fff0000061
TBOOT: 0aac00fffc000001
TBOOT: 100000fc00000061
TBOOT: 140000ff00000061
TBOOT: 14e000ffe0000001
TBOOT: 0000000000000000
TBOOT: discarding RAM above reserved regions: 0xaabff000 - 0xaac00000
TBOOT: reserving 0xaa800000 - 0xaa90d000, which was truncated for VT-d
TBOOT: min_lo_ram: 0x0, max_lo_ram: 0xaa90d000
TBOOT: min_hi_ram: 0x100000000, max_hi_ram: 0x14e000000
TBOOT: MSR for SMM monitor control on BSP is 0x0.
TBOOT: verifying ILP is opt-out or has the same MSEG header with
TXT.MSEG.BASE
    opt-out
TBOOT: succeeded.
TBOOT: enabling SMIs on BSP
TBOOT: mle_join.entry_point = 8031f0
TBOOT: mle_join.seg_sel = 8
TBOOT: mle_join.gdt_base = 804000
TBOOT: mle_join.gdt_limit = 3f
TBOOT: joining RLPs to MLE with MONITOR wakeup
TBOOT: rlp_wakeup_addr = 0xaaf018a0
TBOOT: cpu 7 waking up from TXT sleep
TBOOT: waiting for all APs (7) to enter wait-for-sipi...
TBOOT: MSR for SMM monitor control on cpu 7 is 0x0
TBOOT: verifying ILP's MSR_IA32_SMM_MONITOR_CTL with cpu 7
    : succeeded.
TBOOT: enabling SMIs on cpu 7
TBOOT:.VMXON done for cpu 7
TBOOT:
TBOOT: launching mini-guest for cpu 7
TBOOT: cpu 6 waking up from TXT sleep
TBOOT: MSR for SMM monitor control on cpu 6 is 0x0
```



```
TBOOT: verifying ILP's MSR_IA32_SMM_MONITOR_CTL with cpu 6
: succeeded.
TBOOT: enabling SMIs on cpu 6
TBOOT: VMXON done for cpu 6
TBOOT: launching mini-guest for cpu 6
TBOOT: cpu 3 waking up from TXT sleep
TBOOT: MSR for SMM monitor control on cpu 3 is 0x0
TBOOT: verifying ILP's MSR_IA32_SMM_MONITOR_CTL with cpu 3
: succeeded.
TBOOT: enabling SMIs on cpu 3
TBOOT: VMXON done for cpu 3
TBOOT: launching mini-guest for cpu 3
TBOOT: cpu 5 waking up from TXT sleep
TBOOT: MSR for SMM monitor control on cpu 5 is 0x0
TBOOT: verifying ILP's MSR_IA32_SMM_MONITOR_CTL with cpu 5
: succeeded.
TBOOT: enabling SMIs on cpu 5
TBOOT: VMXON done for cpu 5
TBOOT: cpu 2 waking up from TXT sleep
TBOOT: launching mini-guest for cpu 5
TBOOT: MSR for SMM monitor control on cpu 2 is 0x0
TBOOT: verifying ILP's MSR_IA32_SMM_MONITOR_CTL with cpu 2
: succeeded.
TBOOT: enabling SMIs on cpu 2
TBOOT: VMXON done for cpu 2
TBOOT: launching mini-guest for cpu 2
TBOOT: cpu 4 waking up from TXT sleep
TBOOT: MSR for SMM monitor control on cpu 4 is 0x0
TBOOT: verifying ILP's MSR_IA32_SMM_MONITOR_CTL with cpu 4
: succeeded.
TBOOT: enabling SMIs on cpu 4
TBOOT: VMXON done for cpu 4
TBOOT: launching mini-guest for cpu 4
TBOOT: cpu 1 waking up from TXT sleep
TBOOT: MSR for SMM monitor control on cpu 1 is 0x0
TBOOT: verifying ILP's MSR_IA32_SMM_MONITOR_CTL with cpu 1
.: succeeded.
TBOOT: enabling SMIs on cpu 1
TBOOT: VMXON done for cpu 1
TBOOT: launching mini-guest for cpu 1
TBOOT:
TBOOT: all APs in wait-for-sipi
TBOOT: saved IA32_MISC_ENABLE = 0x00850089
TBOOT: set LT.CMD.SECRETS flag
TBOOT: opened TPM locality 1
TBOOT: RSDP (v002 INTEL) @ 0x000f0410
TBOOT: Seek in XSDT...
TBOOT: entry[0] sig = FACP @ 0xaab85d98
TBOOT: entry[1] sig = APIC @ 0xaabfcf18
TBOOT: entry[2] sig = TCPA @ 0xaaba4d18
TBOOT: entry[3] sig = MCFG @ 0xaaba4c98
TBOOT: entry[4] sig = HPET @ 0xaaba4c18
```



```

TBOOT: entry[5] sig = SSDT @ 0xaab86018
TBOOT: entry[6] sig = SSDT @ 0xaab87c18
TBOOT: entry[7] sig = BOOT @ 0xaaba4b98
TBOOT: entry[8] sig = SSDT @ 0xaab84018
TBOOT: entry[9] sig = SSDT @ 0xaab83018
TBOOT: entry[10] sig = DMAR @ 0xaab85c18
TBOOT: DMAR table @ 0xaab85c18 saved.
TBOOT: no LCP module found
TBOOT: verifying module 0 of mbi (87e000 - bd28bf) in e820 table
      (range from 000000000087e000 to 0000000000bd28c0 is in E820_RAM)
TBOOT: succeeded.
TBOOT: verifying module 1 of mbi (bd3000 - 2545bff) in e820 table
      (range from 0000000000bd3000 to 00000000002545c00 is in E820_RAM)
TBOOT: succeeded.
TBOOT: protecting TXT heap (aaf20000 - aaffffff) in e820 table
TBOOT: protecting SINIT (aaf00000 - aaf1ffff) in e820 table
TBOOT: protecting TXT Private Space (fed20000 - fed2ffff) in e820 table
TBOOT: verifying e820 table against SINIT MDRs: verification succeeded.
TBOOT: verifying tboot and its page table (800000 - 87ccb3) in e820 table
      (range from 0000000000800000 to 000000000087ccb4 is in E820_RAM)
TBOOT: succeeded.
TBOOT: Error: ELF magic number is not matched.
TBOOT: protecting tboot (800000 - 87cfff) in e820 table
TBOOT: reserving tboot memory log (60000 - 67fff) in e820 table
TBOOT: adjusted e820 map:
TBOOT: 0000000000000000 - 0000000000060000 (1)
TBOOT: 0000000000060000 - 0000000000068000 (2)
TBOOT: 0000000000068000 - 000000000009bc00 (1)
TBOOT: 000000000009bc00 - 00000000000a0000 (2)
TBOOT: 00000000000a0000 - 0000000000010000 (2)
TBOOT: 0000000000010000 - 0000000000080000 (1)
TBOOT: 0000000000080000 - 0000000000087d00 (2)
TBOOT: 0000000000087d00 - 00000000000f0000 (1)
TBOOT: 00000000000f0000 - 00000000000100000 (2)
TBOOT: 00000000000100000 - 0000000000aa80000 (1)
TBOOT: 00000000aa80000 - 00000000aa90d00 (2)
TBOOT: 00000000aa90d00 - 00000000aa9e7000 (2)
TBOOT: 00000000aa9e7000 - 00000000aabe7000 (4)
TBOOT: 00000000aabe7000 - 00000000aabff000 (3)
TBOOT: 00000000aabff000 - 00000000aac00000 (2)
TBOOT: 00000000aac00000 - 00000000aaf00000 (2)
TBOOT: 00000000aaf00000 - 00000000aaf20000 (2)
TBOOT: 00000000aaf20000 - 00000000ab000000 (2)
TBOOT: 00000000ab000000 - 00000000b0000000 (2)
TBOOT: 00000000b0000000 - 00000000fc000000 (2)
TBOOT: 00000000fec00000 - 00000000fec01000 (2)
TBOOT: 00000000fed10000 - 00000000fed14000 (2)
TBOOT: 00000000fed18000 - 00000000fed1a000 (2)
TBOOT: 00000000fed1c000 - 00000000fed20000 (2)
TBOOT: 00000000fed20000 - 00000000fed30000 (2)
TBOOT: 00000000fee00000 - 00000000fee01000 (2)
TBOOT: 00000000ff980000 - 00000000ffc00000 (2)

```



```
TBOOT: 00000000ffd80000 - 00000000100000000 (2)
TBOOT: 00000000100000000 - 0000000014e000000 (1)
TBOOT: verifying module "vmlinuz0 root=LABEL=LIVE rootfstype=auto ro
liveimg ver
bose console=tty0 console=ttyS0,115200 iommu=on vga=no OK: af 47 51 f8 48
2c
53 f8 cb 80 ea 58 94 07 62 19 60 6f 15 3b
TBOOT: verifying module "initrd0.img "...
TBOOT: OK: d1 4a 4b 3a 52 bd fb 3a 8c a5 96 51 2e 42 26 fb 09 94 ba 00
TBOOT: all modules are verified
TBOOT: pre_k_s3_state:
TBOOT: vtd_pmr_lo_base: 0x0
TBOOT: vtd_pmr_lo_size: 0xaa800000
TBOOT: vtd_pmr_hi_base: 0x100000000
TBOOT: vtd_pmr_hi_size: 0x4e000000
TBOOT: pol_hash: ab 41 62 4e 7d 71 f0 68 d4 8e 1c 2f 43 e6 16 bf 40 67 1c
39
TBOOT: VL measurements:
TBOOT: PCR 17: 97 04 35 36 30 67 4b fe 21 b8 6b 64 a7 b0 f9 9c 29 7c f9
02
TBOOT: PCR 18: af 47 51 f8 48 2c 53 f8 cb 80 ea 58 94 07 62 19 60 6f 15
3b
TBOOT: PCR 19: d1 4a 4b 3a 52 bd fb 3a 8c a5 96 51 2e 42 26 fb 09 94 ba
00
TBOOT: TPM: start OSAP, return value = 00000012
TBOOT: failed to seal data
TBOOT: PCRs before extending:
TBOOT: PCR 17: 1e 87 57 4e 91 2d f6 82 bc 88 57 db d2 58 eb 21 33 3e 96
e2
TBOOT: PCR 18: b8 0d e5 d1 38 75 85 41 c5 f0 52 65 ad 14 4a b9 fa 86 d1
db
TBOOT: PCRs after extending:
TBOOT: PCR 17: 08 76 e7 39 23 4f b4 90 28 e5 36 af 27 4f e7 8a b1 1f 2a
11
TBOOT: PCR 18: 98 6f 5b 8e bb 75 e6 e6 dc 33 b0 e6 6e 68 a8 3b 6b 9d b0
2e
TBOOT: creation or verification of S3 measurements failed.
TBOOT: tboot_shared data:
TBOOT: version: 5
TBOOT: log_addr: 0x00060000
TBOOT: shutdown_entry: 0x008031b0
TBOOT: shutdown_type: 0
TBOOT: tboot_base: 0x00803000
TBOOT: tboot_size: 0x79cb4
TBOOT: num_in_wfs: 7
TBOOT: no LCP module found
TBOOT: Error: ELF magic number is not matched.
TBOOT: assuming kernel is Linux format
TBOOT: Initrd from 0x7e68d000 to 0x7ffffc00
TBOOT: Kernel (protected mode) from 0xc00000 to 0xf512c0
TBOOT: Kernel (real mode) from 0x90000 to 0x93600
TBOOT: transferring control to kernel @0x00c00000...
Initializing cgroup subsys cpuset
```



Initializing cgroup subsys cpu

§ §



B Appendix B — Intel® CSME Firmware Corporate Power Management in WoWLAN Coexistence Mode

This chapter provides detailed tests for Intel® Manageability Engine (Intel® ME) Firmware Power Management in WoWLAN Coexistence Mode.

For details on WoWLAN Coexistence and WoWLAN Coexistence Mode, including feature availability, review the *Intel® AMT and Wake On Wireless LAN Coexistence* feature overview found in CDI/IBL Document Number: 546827.

Warning: In order to fully implement Wake on Wireless LAN (WoWLAN) in Sx states, the host BIOS must set HOST_WLAN_PP_EN. For more further details, refer the PCH *External Design Specification (EDS)* and the PCH *Platform Design Guide (PDG)*. Failure to properly set the HOST_WLAN_PP_EN bit may result in failures for the tests described herein.

Test Environment setup for this section:

- System Under Test (SUT) can be configured in either manual configuration mode or using enterprise provisioning mode.
- IP address can be selected as static/DHCP (IPv4 or IPv6)
- Select manageability mode as **Intel® AMT**
- Intel® Platform Enablement Test Suite should be installed on the management console.
- Install all platform drivers (Chipset, Graphics, LAN, WLAN, Intel® MEI, LMS_SOL)
- Client platform OS can be Windows* 10
- For wired LAN network use a hub/switch and network cables.
- Wireless setup:
 - Wireless card should be installed.
 - Setup an active wireless profile.
- LAN and WLAN interfaces IPs should be setup on different subnets.

Tools for Testing:

Intel® Platform Enablement Test Suite—Latest version of the tool from the Intel® CSME Compliancy kit release. Refer the Intel® Platform Enablement Test Suite user guide available in the Intel Compliancy kit for exact instructions on how to load and setup the Intel® Platform Enablement Test Suite software.

Note: The following tests can be run by means of Intel® Platform Enablement Test Suite or Manually by following the test procedure step by step.



B.1 Intel® Management Engine (Intel® ME) Power Management Test Coverage Summary

Test ID	Test Case Title	PETS/Manual	Network Factor
ME_PM_1	S0/M0 to S3/M-Off (Mandatory)	PETS - Package Names: Compliance_Power_G3-S5_WoWLAN.xml	LAN+WLAN; WLAN only
ME_PM_2	S3/M-Off to S0/M0 (Mandatory)	PETS - Package Names: Compliance_Power_G3-S5_WoWLAN.xml	LAN+WLAN; WLAN only
ME_PM_3	S0/M0 to S3/M3 (Mandatory)	PETS - Package Names: Compliance_Power_G3-S5_WoWLAN.xml	LAN+WLAN; WLAN only
ME_PM_4	S3/M3 to S0/M0 (Mandatory)	PETS - Package Names: Compliance_Power_G3-S5_WoWLAN.xml	LAN+WLAN; WLAN only
ME_PM_5	S3/M3 to S3/M-Off (Mandatory)	PETS - Package Names: Compliance_Power_G3-S5_WoWLAN.xml	LAN+WLAN; WLAN only
ME_PM_6	S3/M3 to S3/M-Off (with Intel® ME Wake) (Mandatory)	PETS - Package Names: Compliance_Power_G3-S5_WoWLAN.xml	LAN+WLAN; WLAN only
ME_PM_7	S3/M-Off to S3/M3 (Mandatory)	PETS - Package Names: Compliance_Power_G3-S5_WoWLAN.xml	LAN+WLAN; WLAN only
ME_PM_17	Host Power-Cycle Reset also known as cold reset (mandatory)	PETS - Package Names: Compliance_Power_G3-S5_WoWLAN.xml	LAN+WLAN; WLAN only
ME_PM_19	Straight-to-S5, ME Power Policy is S0-Only (Power Button Override) (BIOS: S5 after exit G3. Host WOL: Off) (Mandatory)	PETS - Package Names: Compliance_Power_G3-S5_WoWLAN.xml	LAN+WLAN; WLAN only
ME_PM_20	Straight-to-S5, ME Power Policy Calls for Sx Operation (Mandatory)	PETS - Package Names: Compliance_Power_G3-S5_WoWLAN.xml	LAN+WLAN; WLAN only
ME_PM_21	S0/M0 to S3/M-Off (without Intel® ME Wake) to S3/M-Off (with Intel® ME Wake) (Mandatory)	PETS - Package Names: Compliance_Power_G3-S5_WoWLAN.xml	LAN+WLAN
ME_PM_22	S3/M-Off (with Intel® ME Wake) to S3/M-Off (without Intel® ME Wake) (Mandatory)	PETS - Package Names: Compliance_Power_G3-S5_WoWLAN.xml	LAN+WLAN

Note: All the tests which use wake on LAN (WOL) as a trigger require SUSPEND well (SUS well) to be powered-up. Hence platforms which implement and support DeepSx cannot run WOL tests.

B.2 AME_PM_1: S0/M0 to S3/M-Off

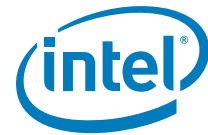
Test ID:	ME_PM_1.1a
Test Case Title:	S0/M0 to S3/M-Off in WoWLAN Coexistence Mode
Mandatory/Optional:	Mandatory
Description:	Original Power State: S0/M0; Target power state - S3/M-Off; LAN Power Policy - Power Policy #1, WLAN Link Policy - '#3: Enabled in S0, Sx/AC'; power source - DC; Trigger: Host go S3
Objective:	This test checks for the system power flow S0/M0 to S3/M-Off



Test ID:	ME_PM_1.1a
Procedure:	<ol style="list-style-type: none">1. Configure BIOS to keep the system in S5 after exiting G32. If the SUT has WLAN support, enable the host WoWLAN driver setting.3. Set the Original Power Policy to #1: ON in S04. Set Wireless Link Policy '#3: Enabled in S0, Sx/AC'. <p>Note: This is required only when wireless is used.</p> <ol style="list-style-type: none">5. Set the power source to DC.6. Boot the system to S0/M0 that is, make sure OS is up7. Verify that Intel® ME is on (Intel® AMT answers ping by means of the LAN/WLAN interface)8. Put host into standby.9. Verify test pass/fail criteria10. FWSTS: N/A
Test Pass/Fail Criteria:	Host goes to S3 state. Intel® ME becomes M-Off. This can be done by checking SLP_A# signal, that should be asserted, indicating Intel® ME is in M-Off.

Test ID:	ME_PM_1.2a
Test Case Title:	S0/M0 to S3/M-Off in WoWLAN Coexistence Mode
Mandatory/Optional:	Mandatory
Description:	Original Power State: S0/M0; Target power state - S3/M-Off; LAN Power Policy - Power Policy #1, WLAN Link Policy - '#3: Enabled in S0, Sx/AC'; power source - ACDC; Trigger: Host goes to S3
Objective:	This test checks for the system power flow S0/M0 to S3/M-Off
Procedure:	<ol style="list-style-type: none">1. Configure BIOS to keep the system in S5 after exiting G32. If the SUT has WLAN support, enable the host WoWLAN driver setting.3. Set the Original Power Policy to #1: ON in S04. Set Wireless Link Policy '#3: Enabled in S0, Sx/AC'. <p>Note: This is required only when wireless is used.</p> <ol style="list-style-type: none">5. Set the power source to AC+DC.6. Boot the system to S0/M0 that is, make sure OS is up7. Verify that Intel® ME is on (Intel® AMT answers ping by means of the LAN/WLAN interface)8. Put host into standby.9. Verify test pass/fail criteria.10. FWSTS: N/A
Test Pass/Fail Criteria:	Host goes to S3 state. Intel® ME become M-Off. This can be done by checking SLP_A# signal, that should be asserted, indicating Intel® ME is in M-Off.

Test ID:	ME_PM_1.3a
Test Case Title:	S0/M0 to S3/M-Off in WoWLAN Coexistence Mode
Mandatory/Optional:	Mandatory
Description:	Original Power State: S0/M0; Target power state - S3/M-Off; LAN Power Policy - Power Policy #2, WLAN Link Policy - '#3: Enabled in S0, Sx/AC'; power source - DC; Trigger: Host goes to S3
Objective:	This test checks for the system power flow S0/M0 to S3/M-Off



Test ID:	ME_PM_1.3a
Procedure:	<ol style="list-style-type: none"> 1. Configure BIOS to keep the system in S5 after exiting G3 2. If the SUT has WLAN support, enable the host WoWLAN driver setting. 3. Set the Original Power Policy to #2: ON in S0, Intel® ME Wake in S3/AC, S4-S5/AC 4. Set the wireless management link policy to '#3: Enabled in S0, Sx/AC' 5. Set the power source to DC. 6. Boot the system to S0/M0 that is, make sure OS is up 7. Verify that Intel® ME is on (Intel® AMT answers ping by means of the LAN/WLAN interface) 8. Put host into standby 9. Verify test pass/fail criteria. 10. FWSTS: N/A
Test Pass/Fail Criteria:	Host goes to S3 state. Intel® ME become M-Off. This can be done by checking SLP_A# signal, that should be asserted, indicating Intel® ME is in M-Off.

B.3 ME_PM_2: S3/M-Off to S0/M0

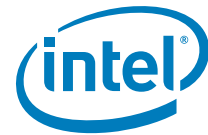
Test ID:	ME_PM_2.2a
Test Case Title:	S3/M-Off to S0/M0 in WoWLAN Coexistence Mode
Mandatory/Optional:	Mandatory
Description:	Original Power State: S3/M-Off; Target power state - S0/M0; LAN Power Policy - Power Policy #1, WLAN Link Policy - '#3: Enabled in S0, Sx/AC'; power source - DC; Trigger: PWR button
Objective:	This test checks for the system power flow S3/M-Off to S0/M0
Procedure:	<ol style="list-style-type: none"> 1. Configure BIOS to keep the system in S5 after exiting G3 2. If the SUT has WLAN support, enable the host WoWLAN driver setting. 3. Set the Original Power Policy to #1: ON in S0 4. Set Wireless Link Policy '#3: Enabled in S0, Sx/AC'. <p>Note: This is required only when wireless is used.</p> <ol style="list-style-type: none"> 5. Set the power source to DC. 6. Boot the system to S0/M0 that is, make sure OS is up 7. Check Windows last boot time 8. Verify that Intel® ME is on (Intel® AMT answers ping by means of the LAN/WLAN interface) 9. Ensure that yellow bang is not seen on Drivers in Device Manager 10. Put host into standby 11. Verify that Intel® ME is in M-Off state. This can be done by checking SLP_A# signal, that should be asserted, indicating Intel® ME is in M-Off. 12. Put the system back to S0 by pressing the power button shortly (make sure OS is up) 13. Ping Intel® AMT IP address with both wired and WLAN interface and Verify Test Pass/Fail Criteria 14. Confirm that the system is in S0/M0 state and the second bit of the FWSTS 2 register should have a value 0x60002306 15. Ensure that yellow bang is not seen on Drivers in Device Manager
Test Pass/Fail Criteria:	Intel® AMT answers ping by means of the LAN/WLAN interface. Host goes to S0 state. Intel® ME becomes M0. Verify Windows last boot time has not changed.

Test ID:	ME_PM_2.3a
Test Case Title:	S3/M-Off to S0/M0 in WoWLAN Coexistence Mode
Mandatory/Optional:	Mandatory



Test ID:	ME_PM_2.3a
Description:	Original Power State: S3/M-Off; Target power state - S0/M0; LAN Power Policy - Power Policy #1, WLAN Link Policy - '#3: Enabled in S0, Sx/AC'; power source - ACDC; Trigger: PWR button
Objective:	This test checks for the system power flow S3/M-Off to S0/M0
Procedure:	<ol style="list-style-type: none">1. Configure BIOS to keep the system in S5 after exiting G32. If the SUT has WLAN support, enable the host WoWLAN driver setting.3. Set the Original Power Policy to #1: ON in S04. Set Wireless Link Policy '#3: Enabled in S0, Sx/AC'. <p>Note: This is required only when wireless is used.</p> <ol style="list-style-type: none">5. Set the power source to AC+DC.6. Boot the system to S0/M0 that is, make sure OS is up7. Check Windows last boot time8. Verify that Intel® ME is on (Intel® AMT answers ping by means of the LAN/WLAN interface)9. Ensure that yellow bang is not seen on Drivers in Device Manager10. Put host into standby11. Verify that Intel® ME is in M-Off state. This can be done by checking SLP_A# signal, that should be asserted, indicating Intel® ME is in M-Off.12. Put the system back to S0 by pressing the power button. Make sure OS is up13. Ping Intel® AMT IP address with both wired and WLAN interface14. Verify Test Pass/Fail Criteria15. Confirm that the system is in S0/M0 state and the second bit of the FWSTS 2 register should have a value 0x6000230616. Ensure that yellow bang is not seen on Drivers in Device Manager
Test Pass/Fail Criteria:	Host goes to S0 state. Intel® ME becomes M0. Intel® AMT answers ping by means of the LAN/WLAN interface. Verify Windows last boot time has not changed.

Test ID:	ME_PM_2.4a
Test Case Title:	S3/M-Off to S0/M0 in WoWLAN Coexistence Mode
Mandatory/Optional:	Mandatory
Description:	Original Power State: S3/M-Off; Target power state - S0/M0; LAN Power Policy - Power Policy #2, WLAN Link Policy - '#3: Enabled in S0, Sx/AC'; power source - ACDC; Trigger: host wake on magic packet
Objective:	This test checks for the system power flow S3/M-Off to S0/M0



Test ID:	ME_PM_2.4a
Procedure:	<ol style="list-style-type: none"> 1. Configure BIOS to keep the system in S5 after exiting G3 2. Enable host WOL 3. If the SUT has WLAN support and the magic packet is to be sent by means of the LAN interface, enable the host WoWLAN driver setting. 4. Enable Host LAN device to wake from off states by Magic Packet only. 5. Set the Original Power Policy to #2: ON in S0, Intel® ME Wake in S3/AC, S4-S5/AC 6. Set Wireless Link Policy '#3: Enabled in S0, Sx/AC'. <p>Note: This is required only when wireless is used.</p> <ol style="list-style-type: none"> 7. Set the power source to AC+DC 8. Configure idle timeout value in Intel® MEBX to 1 9. Boot the system to S0/M0 that is, make sure OS is up 10. Check Windows last boot time 11. Verify that Intel® ME is on (Intel® AMT answers ping by means of the LAN/WLAN interface) 12. Ensure that yellow bang is not seen on Drivers in Device Manager 13. Put host into standby 14. Wait for idle timeout expiry for Intel® ME to enter M-Off (To make sure Intel® ME enters M-Off, check SLP_A# status) 15. Wake the host by sending magic packets by means of the LAN/WLAN device. Make sure OS is up 16. Ping Intel® AMT IP address with both wired and WLAN interface. 17. Verify Test Pass/Fail Criteria 18. Confirm that the system is in S0/M0 state and the second bit of the FWSTS 2 register should have a value 0x60002306 19. Ensure that yellow bang is not seen on Drivers in Device Manager
Test Pass/Fail Criteria:	Host wakes to S0 state, Intel® ME becomes M0. Intel® AMT answers ping by means of the LAN/WLAN interface. Verify Windows last boot time has not changed.

Test ID:	ME_PM_2.5a
Test Case Title:	S3/M-Off to S0/M0 in WoWLAN Coexistence Mode
Mandatory/Optional:	Mandatory
Description:	Original Power State: S3/M-Off; Target power state - S0/M0; LAN Power Policy - Power Policy #2, WLAN Link Policy - '#3: Enabled in S0, Sx/AC'; power source - DC; Trigger: PWR button
Objective:	This test checks for the system power flow S3/M-Off to S0/M0
Procedure:	<ol style="list-style-type: none"> 1. Configure BIOS to keep the system in S5 after exiting G3. 2. If the SUT has WLAN support, enable the host WoWLAN driver setting. 3. Set the Original Power Policy to #2: ON in S0, Intel® ME Wake in S3/AC, S4-S5/AC 4. Set Wireless Link Policy '#3: Enabled in S0, Sx/AC'. <p>Note: This is required only when wireless is used.</p> <ol style="list-style-type: none"> 5. Set the power source to DC. 6. Boot the system to S0/M0 that is, make sure OS is up 7. Check Windows last boot time 8. Verify that Intel® ME is on (Intel® AMT answers ping by means of the LAN/WLAN interface) 9. Ensure that yellow bang is not seen on Drivers in Device Manager 10. Put host into standby 11. Verify that Intel® ME is in M-Off state. This can be done by checking SLP_A# signal, that should be asserted, indicating Intel® ME is in M-Off. 12. Put the system back to S0 by pressing the power button. Make sure OS is up 13. Ping Intel® AMT IP address with both wired and WLAN interface 14. Verify Test Pass/Fail Criteria 15. Confirm that the system is in S0/M0 state and the second bit of the FWSTS 2 register should have a value 0x60002306 16. Ensure that yellow bang is not seen on Drivers in Device Manager



Test ID:	ME_PM_2.5a
Test Pass/Fail Criteria:	Host wakes to S0 state, Intel® ME becomes M0. Intel® AMT answers ping by means of the LAN/WLAN interface. Verify Windows last boot time has not changed.

Test ID:	ME_PM_2.6a
Test Case Title:	S3/M-Off to S0/M0 in WoWLAN Coexistence Mode
Mandatory/Optional:	Mandatory
Description:	Original Power State: S3/M-Off; Target power state - S0/M0; LAN Power Policy - Power Policy #2, WLAN Link Policy - #3: Enabled in S0, Sx/AC; power source - ACDC; Trigger: PWR button
Objective:	This test checks for the system power flow S3/M-Off to S0/M0
Procedure:	<ol style="list-style-type: none">1. Configure BIOS to keep the system in S5 after exiting G3.2. If the SUT has WLAN support, enable the host WoWLAN driver setting.3. Set the Original Power Policy to #2: ON in S0, Intel® ME Wake in S3/AC, S4-S5/AC4. Set Wireless Link Policy #3: Enabled in S0, Sx/AC. <p>Note: This is required only when wireless is used.</p> <ol style="list-style-type: none">5. Set the power source to AC+DC.6. Configure idle timeout value in Intel® MEBX to 17. Boot the system to S0/M0 that is, make sure OS is up8. Check Windows last boot time9. Verify that Intel® ME is on (Intel® AMT answers ping by means of the LAN/WLAN interface)10. Ensure that yellow bang is not seen on Drivers in Device Manager11. Put host into standby12. Verify that Intel® ME is on (This can be done by checking SLP_A# signal, that should be de-asserted, indicating Intel® ME is in M3.)13. Wait for idle timeout expiry for Intel® ME to enter M-Off (To make sure Intel® ME enters M-Off, check SLP_A# status)14. Put the system back to S0 by pressing the power button shortly. Make sure OS is up15. Ping Intel® AMT IP address with both wired and WLAN interface16. Verify Test Pass/Fail Criteria17. Confirm that the system is in S0/M0 state and the second bit of the FWSTS 2 register should have a value 0x6000230618. Ensure that yellow bang is not seen on Drivers in Device Manager
Test Pass/Fail Criteria:	Host wakes to S0 state, Intel® ME becomes M0. Intel® AMT answers ping by means of the LAN/WLAN interface. Verify Windows last boot time has not changed.

B.4 ME_PM_3: S0/M0 to S3/M3 to S0/M0

Test ID:	ME_PM_3.1a
Test Case Title:	S0/M0 to S3/M3 to S0/M0 in WoWLAN Coexistence Mode
Mandatory/Optional:	Mandatory
Description:	Original Power State: S0/M0; Target power state - S3/M3; LAN Power Policy - Power Policy #2, WLAN Link Policy - #3: Enabled in S0, Sx/AC; power source - ACDC; Trigger: WS-MAN frame sent to the WLAN interface
Objective:	This test checks for the system power flow S0/M0 to S3/M3 to S0/M0



Test ID:	ME_PM_3.1a
Procedure:	<ol style="list-style-type: none"> 1. Configure BIOS to keep the system in S5 after exiting G3 2. If the SUT has WLAN support, enable the host WoWLAN driver setting. 3. Set the Original Power Policy to #2: ON in S0, Intel® ME Wake in S3/AC, S4-S5/AC 4. Set Wireless Link Policy '#3: Enabled in S0, Sx/AC'. <p>Note: This is required only when wireless is used.</p> <ol style="list-style-type: none"> 5. Set the power source to AC+DC 6. Boot the system to S0/M0 that is, make sure OS is up 7. Check Windows last boot time. 8. Verify that Intel® ME is on (Intel® AMT answers ping by means of the LAN/WLAN interface). 9. Ensure that yellow bang is not seen on Drivers in Device Manager 10. Put host into standby. 11. Verify that Intel® ME is on (This can be done by checking SLP_A# signal, that should be de-asserted, indicating Intel® ME is in M3.) 12. Ping Intel® AMT IP address by means of WS-MAN protocol by means of the LAN and WLAN interfaces. 13. Verify Test Pass/Fail Criteria 14. Confirm that the system is in S0/M0 state and the second bit of the FWSTS 2 register should have a value 0x68002306 15. Ensure that yellow bang is not seen on Drivers in Device Manager
Test Pass/Fail Criteria:	Host wakes to S0 state, Intel® ME becomes M0. Intel® AMT answers ping by means of the LAN/WLAN interface. Verify Windows last boot time has not changed.

Test ID:	ME_PM_3.21a
Test Case Title:	S0/M0 to S3/M3 to S0/M0 in WoWLAN Coexistence Mode
Mandatory/Optional:	Mandatory
Description:	Original Power State: S0/M0; Target power state - S3/M3; LAN Power Policy - Power Policy #2, WLAN Link Policy - #2: Enabled in S0 only; power source - ACDC; Trigger: WS-MAN frame sent to the WLAN interface
Objective:	This test checks for the system power flow S0/M0 to S3/M3 to S0/M0
Procedure:	<ol style="list-style-type: none"> 1. Configure BIOS to keep the system in S5 after exiting G3 2. If the SUT has WLAN support, enable the host WoWLAN driver setting. 3. Set the Original Power Policy to #2: ON in S0, Intel® ME Wake in S3/AC, S4-S5/AC 4. Set Wireless Link Policy '#2: Enabled in S0 only'. <p>Note: This is required only when wireless is used.</p> <ol style="list-style-type: none"> 5. Set the power source to AC+DC. 6. Boot the system to S0/M0 that is, make sure OS is up. 7. Check Windows last boot time. 8. Verify that Intel® ME is on (Intel® AMT answers ping by means of the LAN/WLAN interface). 9. Ensure that yellow bang is not seen on Drivers in Device Manager 10. Put host into standby 11. Verify that Intel® ME is on (This can be done by checking SLP_A# signal, that should be de-asserted, indicating Intel® ME is in M3.) 12. Ping Intel® AMT IP address by means of WS-MAN protocol by means of the LAN and WLAN interfaces. 13. Verify Test Pass/Fail Criteria 14. Confirm that the system is in S0/M0 state and the second bit of the FWSTS 2 register should have a value 0x68002306 15. Ensure that yellow bang is not seen on Drivers in Device Manager
Test Pass/Fail Criteria:	Host wakes to S0 state, Intel® ME becomes M0. Intel® AMT answers ping by means of the LAN/WLAN interface. Verify Windows last boot time has not changed.



B.5 ME_PM_4: S3/M3 to S0/M0

Test ID:	ME_PM_4.1a
Test Case Title:	S3/M3 to S0/M0 in WoWLAN Coexistence Mode
Mandatory/Optional:	Mandatory
Description:	Original Power State: S3/M3; Target power state - S0/M0; LAN Power Policy - Power Policy #2, WLAN Link Policy - #3: Enabled in S0, Sx/AC; power source - ACDC; Trigger: Host wake on magic packet
Objective:	This test checks for the system power flow S3/M3 to S0/M0
Procedure:	<ol style="list-style-type: none">1. Configure BIOS to keep the system in S5 after exiting G32. Enable host WOL3. If the SUT has WLAN support and the magic packet is to be sent by means of the LAN interface, enable the host WoWLAN driver setting.4. Enable Host LAN/WLAN device to wake from off states by Magic Packet only.5. Set the Original Power Policy to #2: ON in S0, Intel® ME Wake in S3/AC, S4-S5/AC6. Set Wireless Link Policy #3: Enabled in S0, Sx/AC. <p>Note: This is required only when wireless is used.</p> <ol style="list-style-type: none">7. Set the power source to AC+DC8. Boot the system to S0/M0 that is, make sure OS is up9. Check Windows last boot time10. Verify that Intel® ME is on (Intel® AMT answers ping by means of the LAN/WLAN interface)11. Ensure that yellow bang is not seen on Drivers in Device Manager12. Put host into standby13. Verify that Intel® ME is on (This can be done by checking SLP_A# signal, that should be de-asserted, indicating Intel® ME is in M3.)14. Wake up the host by sending magic packets by means of the LAN/WLAN device.15. Ping Intel® AMT IP address by means of the LAN and WLAN interface and Verify Test Pass/Fail Criteria16. Confirm that the system is in S0/M0 state and the second bit of the FWSTS 2 register should have a value 0x6800230617. Ensure that yellow bang is not seen on Drivers in Device Manager
Test Pass/Fail Criteria:	Host goes to S0 state. Intel® ME becomes M0. Intel® AMT answers ping by means of the LAN/WLAN interface. Verify Windows last boot time has not changed.

Test ID:	ME_PM_4.2a
Test Case Title:	S3/M3 to S0/M0 in WoWLAN Coexistence Mode
Mandatory/Optional:	Mandatory
Description:	Original Power State: S3/M3; Target power state - S0/M0; LAN Power Policy - Power Policy #2, WLAN Link Policy - #3: Enabled in S0, Sx/AC; power source - ACDC; Trigger: Power button
Objective:	This test checks for the system power flow S3/M3 to S0/M0



Test ID:	ME_PM_4.2a
Procedure:	<ol style="list-style-type: none"> 1. Configure BIOS to keep the system in S5 after exiting G3 2. If the SUT has WLAN support, enable the host WoWLAN driver setting. 3. Set the Original Power Policy to #2: ON in S0, Intel® ME Wake in S3/AC, S4-S5/AC 4. Set Wireless Link Policy '#3: Enabled in S0, Sx/AC'. <p>Note: This is required only when wireless is used.</p> <ol style="list-style-type: none"> 5. Set the power source to AC + DC 6. Boot the system to S0/M0 that is, make sure OS is up 7. Check Windows last boot time 8. Verify that Intel® ME is on (Intel® AMT answers ping by means of the LAN/WLAN interface) 9. Ensure that yellow bang is not seen on Drivers in Device Manager 10. Put host into standby 11. Verify that Intel® ME is on (This can be done by checking SLP_A# signal, that should be de-asserted, indicating Intel® ME is in M3.) 12. Wake the host by pressing power button 13. Ping Intel® AMT IP address by means of the LAN/WLAN interface and Verify Test Pass/Fail Criteria 14. Confirm that the system is in S0/M0 state and the second bit of the FWSTS 2 register should have a value 0x68002306 15. Ensure that yellow bang is not seen on Drivers in Device Manager
Test Pass/Fail Criteria:	Host returns to S0. Intel® ME becomes M0. Intel® AMT is reachable by means of the LAN and WLAN interface. Verify Windows last boot time has not changed.

Test ID:	ME_PM_4.21a
Test Case Title:	S3/M3 to S0/M0 in WoWLAN Coexistence Mode
Mandatory/Optional:	Mandatory
Description:	Original Power State: S3/M3; Target power state - S0/M0; LAN Power Policy - Power Policy #2, WLAN Link Policy - #2: Enabled in S0 only; power source - ACDC; Trigger: Host wake on magic packet
Objective:	This test checks for the system power flow S3/M3 to S0/M0
Procedure:	<ol style="list-style-type: none"> 1. Configure BIOS to keep the system in S5 after exiting G3 2. Enable host WOL 3. If the SUT has WLAN support and the magic packet is to be sent by means of the LAN interface, enable the host WoWLAN driver setting. 4. Enable Host LAN/WLAN device to wake from off states by Magic Packet only. 5. Set the Original Power Policy to #2: ON in S0, Intel® ME Wake in S3/AC, S4-S5/AC 6. Set Wireless Link Policy '#2: Enabled in S0 only'. <p>Note: This is required only when wireless is used.</p> <ol style="list-style-type: none"> 7. Set the power source to AC+DC 8. Boot the system to S0/M0 that is, make sure OS is up 9. Check Windows last boot time 10. Verify that Intel® ME is on (Intel® AMT answers ping by means of the LAN/WLAN interface) 11. Ensure that yellow bang is not seen on Drivers in Device Manager 12. Put host into standby 13. Verify that Intel® ME is on (This can be done by checking SLP_A# signal, that should be de-asserted, indicating Intel® ME is in M3.) 14. Wake up the host by sending magic packets by means of the LAN/WLAN device. 15. Ping Intel® AMT IP address by means of the LAN and WLAN interface and Verify Test Pass/Fail Criteria 16. Confirm that the system is in S0/M0 state and the second bit of the FWSTS 2 register should have a value 0x68002306 17. Ensure that yellow bang is not seen on Drivers in Device Manager



Test ID:	ME_PM_4.21a
Test Pass/Fail Criteria:	Host goes to S0 state. Intel® ME becomes M0. Intel® AMT answers ping by means of the LAN and WLAN interface. Verify Windows last boot time has not changed.

Test ID:	ME_PM_4.22a
Test Case Title:	S3/M3 to S0/M0 in WoWLAN Coexistence Mode
Mandatory/Optional:	Mandatory
Description:	Original Power State: S3/M3; Target power state - S0/M0; LAN Power Policy - Power Policy #2, WLAN Link Policy - '#2: Enabled in S0 only'; power source - ACDC; Trigger: Power button
Objective:	This test checks for the system power flow S3/M3 to S0/M0
Procedure:	<ol style="list-style-type: none">1. Configure BIOS to keep the system in S5 after exiting G32. If the SUT has WLAN support, enable the host WoWLAN driver setting.3. Set the Original Power Policy to #2: ON in S0, Intel® ME Wake in S3/AC, S4-S5/AC4. Set Wireless Link Policy '#2: Enabled in S0 only'. <p>Note: This is required only when wireless is used.</p> <ol style="list-style-type: none">5. Set the power source to AC + DC6. Boot the system to S0/M0 that is, make sure OS is up7. Check Windows last boot time8. Verify that Intel® ME is on (Intel® AMT answers ping by means of the LAN/WLAN interface)9. Ensure that yellow bang is not seen on Drivers in Device Manager10. Put host into standby11. Verify that Intel® ME is on (This can be done by checking SLP_A# signal, that should be de-asserted, indicating Intel® ME is in M3.)12. Wake the host by pressing power button13. Ping Intel® AMT IP address by means of the LAN/WLAN interface only and Verify Test Pass/Fail Criteria14. Confirm that the system is in S0/M0 state and the second bit of the FWSTS 2 register should have a value 0x6800230615. Ensure that yellow bang is not seen on Drivers in Device Manager
Test Pass/Fail Criteria:	Host returns to S0. Intel® ME becomes M0. Intel® AMT answers ping by means of the LAN/WLAN interface only. Verify Windows last boot time has not changed.

B.6 ME_PM_5: S3/M3 to S3/M-Off (Without Intel® ME Wake)

Test ID:	ME_PM_5.1a
Test Case Title:	S3/M3 to S3/M-Off (without Intel® ME Wake) in WoWLAN Coexistence Mode
Mandatory/Optional:	Mandatory Exemptions <input checked="" type="checkbox"/> Non-Mobile (AC-only) Systems
Description:	Original Power State: S3/M3; Target power state - S3/M-Off; LAN Power Policy - Power Policy #2, WLAN Link Policy - '#3: Enabled in S0, Sx/AC'; power source - ACDC; Trigger: ACDC->DC
Objective:	This test checks for the system power flow S3/M3 to S3/M-Off (without Intel® ME Wake)



Test ID:	ME_PM_5.1a
Procedure:	<ol style="list-style-type: none"> 1. Configure BIOS to keep the system in S5 after exiting G3 2. If the SUT has WLAN support, enable the host WoWLAN driver setting. 3. Set the Original Power Policy to #2: ON in S0, Intel® ME Wake in S3/AC, S4-S5/AC 4. Set Wireless Link Policy '#3: Enabled in S0, Sx/AC'. <p>Note: This is required only when wireless is used.</p> <ol style="list-style-type: none"> 5. Set the power source to AC+DC 6. Boot the system to S0/M0 that is, make sure OS is up 7. Verify that Intel® ME is on (Intel® AMT answers ping by means of the LAN/WLAN interface) 8. Put host into standby 9. Verify that Intel® ME is on (This can be done by checking SLP_A# signal, that should be de-asserted, indicating Intel® ME is in M3.) 10. Disconnect AC power cord 11. Verify Test Pass/Fail Criteria 12. FWSTS: N/A
Test Pass/Fail Criteria:	Host stays in S3 state. Intel® ME stays off. This can be done by checking SLP_A# signal, that should be asserted, indicating Intel® ME is in M-Off.

Test ID:	ME_PM_5.21a
Test Case Title:	S3/M3 to S3/M-Off (without Intel® ME Wake) in WoWLAN Coexistence Mode
Mandatory/Optional:	Mandatory Exemptions <input checked="" type="checkbox"/> Non-Mobile (AC-only) Systems
Description:	Original Power State: S3/M3; Target power state - S3/M-Off; LAN Power Policy - Power Policy #2, WLAN Link Policy - '#2: Enabled in S0 only'; power source - ACDC; Trigger: ACDC->DC
Objective:	This test checks for the system power flow S3/M3 to S3/M-Off (without Intel® ME Wake)
Procedure:	<ol style="list-style-type: none"> 1. Configure BIOS to keep the system in S5 after exiting G3 2. If the SUT has WLAN support, enable the host WoWLAN driver setting. 3. Set the Original Power Policy to #2: ON in S0, Intel® ME Wake in S3/AC, S4-S5/AC 4. Set Wireless Link Policy '#2: Enabled in S0 only'. <p>Note: This is required only when wireless is used.</p> <ol style="list-style-type: none"> 5. Set the power source to AC + DC 6. Boot the system to S0/M0 that is, make sure OS is up 7. Verify that Intel® ME is on (Intel® AMT answers ping by means of the LAN/WLAN interface) 8. Put host into standby 9. Verify that Intel® ME is on (This can be done by checking SLP_A# signal, that should be de-asserted, indicating Intel® ME is in M3.) 10. Disconnect AC power cord 11. Verify Test Pass/Fail Criteria 12. FWSTS: N/A
Test Pass/Fail Criteria:	Host stays in S3 state. Intel® ME becomes M-Off. This can be done by checking SLP_A# signal, that should be asserted, indicating Intel® ME is in M-Off.

B.7 ME_PM_6: S3/M3 to S3/M-Off (With Intel® ME Wake)

Test ID:	ME_PM_6.1a
Test Case Title:	S3/M3 to S3/M-Off (with Intel® ME Wake) in WoWLAN Coexistence Mode



Test ID:	ME_PM_6.1a
Mandatory/Optional:	Mandatory
Description:	Original Power State: S3/M3; Target power state - S3/M-Off; LAN Power Policy - Power Policy #2, WLAN Link Policy `#3: Enabled in S0, Sx/AC'; power source - ACDC; Trigger: Wait idle time.
Objective:	This test checks for the system power flow S3/M3 to S3/M-Off (with Intel® ME Wake)
Procedure:	<ol style="list-style-type: none">1. Configure BIOS to keep the system in S5 after exiting G32. If the SUT has WLAN support, enable the host WoWLAN driver setting.3. Set the Original Power Policy to #2: ON in S0, Intel® ME Wake in S3/AC, S4-S5/AC4. Set Wireless Link Policy `#3: Enabled in S0, Sx/AC'. <p>Note: This is required only when wireless is used.</p> <ol style="list-style-type: none">5. Set the power source to AC + DC6. Configure idle timeout value in Intel® MEBX to 17. Boot the system to S0/M0 that is, make sure OS is up8. Verify that Intel® ME is on (Intel® AMT answers ping by means of the LAN/WLAN interface)9. Put host into standby10. Verify that Intel® ME is on (This can be done by checking SLP_A# signal, that should be de-asserted, indicating Intel® ME is in M3.)11. Wait for idle timeout expiry for ME to enter M-Off (To make sure Intel® ME enters M-Off by checking that SLP_A# should be asserted)12. Verify Test Pass/Fail Criteria13. FWSTS: N/A
Test Pass/Fail Criteria:	Host stays in S3 state. Verify that Intel® ME became M-Off by checking that SLP_A# signal is asserted,

Test ID:	ME_PM_6.21a
Test Case Title:	S3/M3 to S3/M-Off (with Intel® ME Wake) in WoWLAN Coexistence Mode
Mandatory/Optional:	Mandatory
Description:	Original Power State: S3/M3; Target power state - S3/M-Off; LAN Power Policy - Power Policy #2, WLAN Link Policy `#2: Enabled in S0 only'; power source - ACDC; Trigger: Wait idle time.
Objective:	This test checks for the system power flow S3/M3 to S3/M-Off (with Intel® ME Wake)
Procedure:	<ol style="list-style-type: none">1. Configure BIOS to keep the system in S5 after exiting G32. If the SUT has WLAN support, enable the host WoWLAN driver setting.3. Set the Original Power Policy to #2: ON in S0, Intel® ME Wake in S3/AC, S4-S5/AC4. Set Wireless Link Policy `#2: Enabled in S0 only'. <p>Note: This is required only when wireless is used.</p> <ol style="list-style-type: none">5. Set the power source to AC + DC6. Configure idle timeout value in Intel® MEBX to 17. Boot the system to S0/M0 that is, make sure OS is up8. Verify that Intel® ME is on (Intel® AMT answers ping by means of the LAN/WLAN interface)9. Put host into standby10. Verify that Intel® ME is on (This can be done by checking SLP_A# signal, that should be de-asserted, indicating Intel® ME is in M3.)11. Wait for idle timeout expiry for ME to enter M-Off (To make sure Intel® ME enters M-Off check SLP_A# status)12. Verify Test Pass/Fail Criteria13. FWSTS: N/A
Test Pass/Fail Criteria:	Host stays in S3 state. Verify that Intel® ME became M-Off by checking that SLP_A# signal is asserted,



B.8 ME_PM_7: S3/M-Off to S3/M3 (to S0/M0)

Test ID:	ME_PM_7.1a
Test Case Title:	S3/M-Off to S3/M3 in WoWLAN Coexistence Mode
Mandatory/Optional:	Mandatory
Wireless Only:	No
Description:	Original Power State: S3/M-Off; Target power state - S3/M3; LAN Power Policy - Power Policy #2, WLAN Link Policy - '#3: Enabled in S0, Sx/AC'; power source - ACDC; Trigger: Wake ME by means of the LAN ping.
Objective:	This test checks for the system power flow S3/M-Off to S3/M3
Procedure:	<ol style="list-style-type: none"> 1. Configure BIOS to keep the system in S5 after exiting G3 2. If the SUT has WLAN support, enable the host WoWLAN driver setting. 3. Set the Original Power Policy to #2: ON in S0, Intel® ME Wake in S3/AC, S4-S5/AC 4. Set Wireless Link Policy '#3: Enabled in S0, Sx/AC'. <p>Note: This is required only when wireless is used.</p> <ol style="list-style-type: none"> 5. Set the power source to AC + DC 6. Configure idle timeout value in Intel® MEBX to 1 7. Boot the system to S0/M0 that is, make sure OS is up 8. Verify that Intel® ME is on (Intel® AMT answers ping by means of the LAN/WLAN interface) 9. Put the system into standby 10. Verify that Intel® ME is on (This can be done by checking SLP_A# signal, that should be de-asserted, indicating Intel® ME is in M3.) 11. Wait for idle timeout expiry for Intel® ME to enter M-Off (To make sure Intel® ME enters M-Off check SLP_A# status) 12. Wake up Intel® ME by means of the Intel® ME version query over the LAN interface. 13. Verify Test Pass/Fail Criteria 14. FWSTS: N/A
Test Pass/Fail Criteria:	Intel® AMT answers ping by means of the LAN interface. Host stays in S3 state. Intel® ME becomes M3.

Test ID:	ME_PM_7.2a
Test Case Title:	S3/M-Off to S3/M3 to S0/M0 in WoWLAN Coexistence Mode
Mandatory/Optional:	Mandatory
Description:	Original Power State: S3/M-Off; Target power state - S3/M3; LAN Power Policy - Power Policy #2, WLAN Link Policy - '#3: Enabled in S0, Sx/AC'; power source - DC; Trigger: WS-MAN frame sent to the WLAN interface
Objective:	This test checks for the system power flow S3/M-Off to S3/M3 to S0/M0



Test ID:	ME_PM_7.2a
Procedure:	<ol style="list-style-type: none">1. Configure BIOS to keep the system in S5 after exiting G32. If the SUT has WLAN support, enable the host WoWLAN driver setting.3. Set the Original Power Policy to #2: ON in S0, Intel® ME Wake in S3/AC, S4-S5/AC4. Set Wireless Link Policy '#3: Enabled in S0, Sx/AC'. <p>Note: This is required only when wireless is used.</p> <ol style="list-style-type: none">5. Set the power source to DC6. Boot the system to S0/M0 that is, make sure OS is up7. Check Windows last boot time.8. Verify that Intel® ME is on (Intel® AMT answers ping by means of the LAN/WLAN interface)9. Ensure that yellow bang is not seen on Drivers in Device Manager10. Put host into standby11. Verify that ME is in M-Off state. This can be done by checking SLP_A# signal, that should be asserted, indicating Intel® ME is in M-Off.12. Reconnect AC power cord13. Ping Intel® AMT IP address by means of WS-MAN protocol by means of the LAN and WLAN interfaces.14. Verify Test Pass/Fail Criteria15. Confirm that the system is in S0/M0 state and the second bit of the FWSTS 2 register should have a value 0x6800230616. Ensure that yellow bang is not seen on Drivers in Device Manager
Test Pass/Fail Criteria:	Host wakes to S0 state, Intel® ME becomes M0. Intel® AMT answers ping by means of the LAN/WLAN interface. Verify Windows last boot time has not changed.

Test ID:	ME_PM_7.3a
Test Case Title:	S3/M-Off to S3/M3 to S0/M0 in WoWLAN Coexistence Mode
Mandatory/Optional:	Mandatory
Description:	Original Power State: S3/M-Off; Target power state - S3/M3; LAN Power Policy - Power Policy #2, WLAN Link Policy - '#3: Enabled in S0, Sx/AC'; power source - ACDC; Trigger: WS-MAN frame sent to the WLAN interface
Objective:	This test checks for the system power flow S3/M-Off to S3/M3 to S0/M0
Procedure:	<ol style="list-style-type: none">1. Configure BIOS to keep the system in S5 after exiting G32. If the SUT has WLAN support, enable the host WoWLAN driver setting.3. Set the Original Power Policy to #2: ON in S0, Intel® ME Wake in S3/AC, S4-S5/AC4. Set Wireless Link Policy '#3: Enabled in S0, Sx/AC'. <p>Note: This is required only when wireless is used.</p> <ol style="list-style-type: none">5. Set the power source to AC + DC6. Configure idle timeout value in Intel® MEBX to 17. Boot the system to S0/M0 that is, make sure OS is up8. Check Windows last boot time.9. Verify that Intel® ME is on (Intel® AMT answers ping by means of the LAN/WLAN interface)10. Ensure that yellow bang is not seen on Drivers in Device Manager11. Put the system into standby12. Verify that Intel® ME is on (This can be done by checking SLP_A# signal, that should be de-asserted, indicating Intel® ME is in M3.)13. Wait for idle timeout expiry for Intel® ME to enter M-Off (To make sure Intel® ME enters M-Off check SLP_A# status)14. Wake up Intel® ME and the system by means of the Intel® ME version query over the WLAN interface.15. Verify Test Pass/Fail Criteria16. Confirm that the system is in S0/M0 state and the second bit of the FWSTS 2 register should have a value 0x6000230617. Ensure that yellow bang is not seen on Drivers in Device Manager



Test ID:	ME_PM_7.3a
Test Pass/Fail Criteria:	Host wakes to S0 state, Intel® ME becomes M0. Intel® AMT answers ping by means of the LAN/WLAN interface. Verify Windows last boot time has not changed. Note: It could take about ~30-40 seconds for the firmware to start responding to pings by means of the WLAN interface.

Test ID:	ME_PM_7.21a
Test Case Title:	S3/M-Off to S3/M3 in WoWLAN Coexistence Mode
Mandatory/Optional:	Mandatory
Wireless Only:	No
Description:	Original Power State: S3/M-Off; Target power state - S3/M3; LAN Power Policy - Power Policy #2, WLAN Link Policy - '#2: Enabled in S0 only'; power source - ACDC; Trigger: Wake ME by means of the LAN ping.
Objective:	This test checks for the system power flow S3/M-Off to S3/M3
Procedure:	<ol style="list-style-type: none"> 1. Configure BIOS to keep the system in S5 after exiting G3 2. If the SUT has WLAN support, enable the host WoWLAN driver setting. 3. Set the Original Power Policy to #2: ON in S0, Intel® ME Wake in S3/AC, S4-S5/AC 4. Set Wireless Link Policy '#2: Enabled in S0 only'. 5. This is required only when wireless is used. 6. Set the power source to AC+DC. 7. Configure idle timeout value in Intel® MEBX to 1. 8. Boot the system to S0/M0 that is, make sure OS is up. 9. Verify that Intel® ME is on (Intel® AMT answers ping by means of the LAN/WLAN interface) 10. Put the system into standby 11. Verify that Intel® ME is on (This can be done by checking SLP_A# signal, that should be de-asserted, indicating Intel® ME is in M3.) 12. Wait for idle timeout expiry for Intel® ME to enter M-Off (To make sure Intel® ME enters M-Off check SLP_A# status) 13. Wake up Intel® ME by means of the Intel® ME version query over the LAN interface. 14. Verify Test Pass/Fail Criteria 15. FWSTS: N/A
Test Pass/Fail Criteria:	Intel® AMT answers ping by means of the LAN interface. Host stays in S3 state. Intel® ME becomes M3.

Test ID:	ME_PM_7.22a
Test Case Title:	S3/M-Off to S3/M3 in WoWLAN Coexistence Mode
Mandatory/Optional:	Mandatory
Wireless Only:	No
Description:	Original Power State: S3/M-Off; Target power state - S3/M3; LAN Power Policy - Power Policy #2, WLAN Link Policy - '#2: Enabled in S0 only'; power source - DC; Trigger: DC->ACDC.
Objective:	This test checks for the system power flow S3/M-Off to S3/M3



Test ID:	ME_PM_7.22a
Procedure:	<ol style="list-style-type: none">1. Configure BIOS to keep the system in S5 after exiting G32. If the SUT has WLAN support, enable the host WoWLAN driver setting.3. Set the Original Power Policy to #2: ON in S0, Intel® ME Wake in S3/AC, S4-S5/AC4. Set Wireless Link Policy '#2: Enabled in S0 only'. <p>Note: This is required only when wireless is used.</p> <ol style="list-style-type: none">5. Set the power source to DC6. Boot the system to S0/M0 that is, make sure OS is up7. Verify that Intel® ME is on (Intel® AMT answers ping by means of the LAN/WLAN interface)8. Put host into standby9. Verify that ME is in M-Off state. This can be done by checking SLP_A# signal, that should be asserted, indicating Intel® ME is in M-Off.10. Reconnect AC power cord11. Ping Intel® AMT IP address by means of the LAN interface only12. Verify Test Pass/Fail Criteria13. FWSTS: N/A
Test Pass/Fail Criteria:	Intel® AMT is reachable by means of the LAN interface only. Host stays in S3 state. Intel® ME becomes M3.

B.9 ME_PM_17: Host Power-Cycle Reset—Cold Reset

Test ID:	ME_PM_17.5a
Test Case Title:	S3/M3 to S0/M0 (Host Power-Cycle Reset) in WoWLAN Coexistence Mode
Mandatory/Optional:	Mandatory
Description:	This test checks for the system power flow of host power-cycle from S3/M3 to S0/M0 by means of the S5; LAN Power Policy - Power Policy #2, WLAN Link Policy '#3: Enabled in S0, Sx/AC'; power source - ACDC; Trigger: RCO power-cycle.
Objective:	This test checks for the system power flow of host power-cycle from S3/M3 to S0/M0 by means of the S5.
Procedure:	<ol style="list-style-type: none">1. Configure BIOS to keep the system in S5 after exiting G32. If the SUT has WLAN support, enable the host WoWLAN driver setting.3. Set the Original Power Policy to #2: ON in S0, Intel® ME Wake in S3/AC, S4-S5/AC4. Set Wireless Link Policy '#3: Enabled in S0, Sx/AC'. <p>Note: This is required only when wireless is used.</p> <ol style="list-style-type: none">5. Set the power source to AC + DC6. Boot the system to S0/M0 that is, make sure OS is up7. Verify that Intel® ME is on (Intel® AMT answers ping by means of the LAN/WLAN interface)8. Ensure that yellow bang is not seen on Drivers in Device Manager9. Put the system into S3/M3.10. Verify that Intel® ME is on (This can be done by checking SLP_A# signal, that should be de-asserted, indicating Intel® ME is in M3.)11. Send the Remote Control Power-Cycle command12. Verify Test Pass/Fail Criteria13. Confirm that the system is in S0/M0 state and the second bit of the FWSTS 2 register should have a value 0x6800230614. Ensure that yellow bang is not seen on Drivers in Device Manager
Test Pass/Fail Criteria:	Host performs power-cycle by means of the S5 to S0 state with OS up and running. Ensure SLP_S3#, SLP_S4# and SLP_S5# are asserted during the transition. Intel® ME stays M0. Intel® AMT answers ping by means of the LAN/WLAN interface.



Test ID:	ME_PM_17.25a
Test Case Title:	S3/M3 to S0/M0 (Host Power-Cycle Reset) in WoWLAN Coexistence Mode
Mandatory/Optional:	Mandatory
Description:	This test checks for the system power flow of host power-cycle from S3/M3 to S0/M0 by means of the S5; LAN Power Policy - Power Policy #2, WLAN Link Policy `#2: Enabled in S0 only'; power source - ACDC; Trigger: RCO power-cycle.
Objective:	This test checks for the system power flow of host power-cycle from S3/M3 to S0/M0 by means of the S5.
Procedure:	<ol style="list-style-type: none"> 1. Configure BIOS to keep the system in S5 after exiting G3 2. If the SUT has WLAN support, enable the host WoWLAN driver setting. 3. Set the Original Power Policy to #2: ON in S0, Intel® ME Wake in S3/AC, S4-S5/AC 4. Set Wireless Link Policy `#2: Enabled in S0 only'. <p>Note: This is required only when wireless is used.</p> <ol style="list-style-type: none"> 5. Set the power source to AC + DC 6. Boot the system to S0/M0 that is, make sure OS is up 7. Verify that Intel® ME is on (Intel® AMT answers ping by means of the LAN/WLAN interface) 8. Ensure that yellow bang is not seen on Drivers in Device Manager 9. Put the system into S3/M3. 10. Verify that Intel® ME is on (This can be done by checking SLP_A# signal, that should be de-asserted, indicating Intel® ME is in M3.) 11. Send the Remote Control Power-Cycle command 12. Verify Test Pass/Fail Criteria. 13. Confirm that the system is in S0/M0 state and the second bit of the FWSTS 2 register should have a value 0x68002306 14. Ensure that yellow bang is not seen on Drivers in Device Manager
Test Pass/Fail Criteria:	Host performs power-cycle by means of the S5 to S0 state with OS up and running. Ensure SLP_S3#, SLP_S4# and SLP_S5# are asserted during the transition. Intel® ME stays M0. Intel® AMT answers ping by means of the LAN/WLAN interface.

B.10 Straight-to-S5, Intel® Management Engine (Intel® ME) Power Policy is S0 Only

Test ID:	ME_PM_19.3a
Test Case Title:	S3/M-Off to S5/M-Off in WoWLAN Coexistence Mode
Mandatory/Optional:	Mandatory
Description:	<p>This test checks for S3/M-Off to S5/M-Off flow; LAN Power Policy - Power Policy #1, WLAN Link Policy `#3: Enabled in S0, Sx/AC'; power source - DC; trigger: PWR button override.</p> <p>Note: If Deep S4/S5 state is enabled on the platform under test, make sure Deep S4/S5 global parameters are configured in PETS:</p> <ol style="list-style-type: none"> 1. "Deep S4/S5 enabled" should be set to TRUE 2. "Deep S4/S5 Policy" should be configured to the policy chosen in BIOS.
Objective:	This test checks for S3/M-Off to S5/M-Off flow



Test ID:	ME_PM_19.3a
Procedure:	<ol style="list-style-type: none">1. Configure BIOS to keep the system in S5 after exiting G3 (Intel® ME available)2. If the SUT has WLAN support, enable the host WoWLAN driver setting.3. Set the Original Power Policy to #1: ON in S04. Set Wireless Link Policy '#3: Enabled in S0, Sx/AC'. <p>Note: This is required only when wireless is used.</p> <ol style="list-style-type: none">5. Set the power source to DC.6. Boot the system to S0/M0 that is, make sure OS is up7. Verify that Intel® ME is on (Intel® AMT answers ping by means of the LAN/WLAN interface).8. Move host into Standby (S3).9. Verify that Intel® ME is off (Intel® AMT does not answer ping by means of the LAN/WLAN interface)10. Press PWR button for more than 5 seconds (power button override).11. If Deep S4/S5 is enabled and configuration policy matches the target power state, check for Deep S4/S5 signal. (For details on Deep S4/S5 policies, refer to Table 12-1 the beginning of this chapter)12. Verify that ME is in M-Off state. This can be done by checking SLP_A# signal, that should be asserted, indicating Intel® ME is in M-Off.13. Verify Test Pass/Fail Criteria14. FWSTS: N/A
Test Pass/Fail Criteria:	<p>System goes to S0/M0 and then to S5/M-Off.</p> <p>Note: Depending on OEM implementation system may directly go to G3 after power button override event.</p> <p>If Deep S4/S5 is enabled and configuration policy matches the target power state, platform should be in Deep S4/S5 state.</p>

Test ID:	ME_PM_19.4a
Test Case Title:	S3/M-Off to S5/M-Off in WoWLAN Coexistence Mode
Mandatory/Optional:	Mandatory
Description:	<p>This test checks for S3/M-Off to S5/M-Off flow; LAN Power Policy - Power Policy #1, WLAN Link Policy '#3: Enabled in S0, Sx/AC'; power source - ACDC; trigger: PWR button override</p> <p>Notes:</p> <p>If Deep S4/S5 state is enabled on the platform under test, make sure Deep S4/S5 global parameters are configured in PETS:</p> <ol style="list-style-type: none">1. "Deep S4/S5 enabled" should be set to TRUE2. "Deep S4/S5 Policy" should be configured to the policy chosen in BIOS.
Objective:	This test checks for S3/M-Off to S5/M-Off flow



Test ID:	ME_PM_19.4a
Procedure:	<ol style="list-style-type: none"> 1. Configure BIOS to keep the system in S5 after exiting G3 (Intel® ME available) 2. If the SUT has WLAN support, enable the host WoWLAN driver setting. 3. Set the Original Power Policy to #1: ON in S0 4. Set Wireless Link Policy '#3: Enabled in S0, Sx/AC'. Note: This is required only when wireless is used. 5. Set the power source to AC+DC 6. Boot the system to S0/M0 that is, make sure OS is up 7. Verify that Intel® ME is on (Intel® AMT answers ping by means of the LAN/WLAN interface) 8. Move host to standby (S3) 9. Verify that Intel® ME is off (Intel® AMT does not answer ping by means of the LAN/WLAN interface) 10. Press PWR button for more than 5 seconds (power button override) 11. If Deep S4/S5 is enabled and configuration policy matches the target power state, check for Deep S4/S5 signal. (For details on Deep S4/S5 policies, refer Table 12-1 in the beginning of this chapter) 12. Verify that ME is in M-Off state. This can be done by checking SLP_A# signal, that should be asserted, indicating Intel® ME is in M-Off. 13. Verify Test Pass/Fail Criteria 14. FWSTS: N/A
Test Pass/Fail Criteria:	<p>System goes to S0/M0 and then to S5/M-Off.</p> <p>Note: Depending on OEM implementation system may directly go to G3 after power button override event.</p> <p>If Deep S4/S5 is enabled and configuration policy matches the target power state, platform should be in Deep S4/S5 state.</p>

B.11 Straight-to-S5, Intel® ME Power Policy Calls for Sx Operation

Test ID:	ME_PM_20.3a
Test Case Title:	S3/M3 to S5/M3 in WoWLAN Coexistence Mode
Mandatory/Optional:	Mandatory
Description:	This test checks for S3/M3 to S5/M3 flow; LAN Power Policy - Power Policy #2, WLAN Link Policy '#3: Enabled in S0, Sx/AC'; power source - ACDC; trigger: Power Button Override
Objective:	This test checks for S3/M3 to S5/M3 flow
Procedure:	<ol style="list-style-type: none"> 1. Configure BIOS to keep the system in S5 after exiting G3 (Intel® ME available) 2. If the SUT has WLAN support, enable the host WoWLAN driver setting. 3. Set the Original Power Policy to #2: ON in S0, Intel® ME Wake in S3/AC, S4-S5/AC 4. Set Wireless Link Policy '#3: Enabled in S0, Sx/AC'. Note: This is required only when wireless is used. 5. Set the power source to AC+DC 6. Boot the system to S0/M0 that is, make sure OS is up 7. Verify that Intel® ME is on (Intel® AMT answers ping by means of the LAN/WLAN interface) 8. Move host to Standby (S3) 9. Verify that Intel® ME is on (This can be done by checking SLP_A# signal, that should be de-asserted, indicating Intel® ME is in M3.) 10. Press PWR button for more than 5 seconds (power button override) 11. Verify Test Pass/Fail Criteria 12. FWSTS: N/A
Test Pass/Fail Criteria:	System goes to S0/M0 to S5/M-Off and then to S5/M3 after ~ 4-5 seconds.



Test ID:	ME_PM_20.4a
Test Case Title:	S3/M-Off to S5/M3 in WoWLAN Coexistence Mode
Mandatory/Optional:	Mandatory
Description:	This test checks for S3/M-Off to S5/M3 flow; LAN Power Policy - Power Policy #2, WLAN Link Policy `#3: Enabled in S0, Sx/AC'; power source - ACDC; trigger: Power Button Override
Objective:	This test checks for S3/M-Off to S5/M3 flow
Procedure:	<ol style="list-style-type: none">1. Configure BIOS to keep the system in S5 after exiting G3 (Intel® ME available)2. If the SUT has WLAN support, enable the host WoWLAN driver setting.3. Configure idle timeout value in Intel® MEBX to 14. Set the Original Power Policy to #2: ON in S0, Intel® ME Wake in S3/AC, S4-S5/AC5. Set Wireless Link Policy `#3: Enabled in S0, Sx/AC'. <p>Note: This is required only when wireless is used.</p> <ol style="list-style-type: none">6. Set the power source to AC+DC7. Boot the system to S0/M0 that is, make sure OS is up8. Verify that Intel® ME is on (Intel® AMT answers ping by means of the LAN/WLAN interface)9. Move host into Standby (S3)10. Verify that Intel® ME is on (This can be done by checking SLP_A# signal, that should be de-asserted, indicating Intel® ME is in M3.)11. Wait for idle timeout expiry for ME to enter M-Off (To make sure ME enters M-Off check SLP_A# status)12. Press PWR button for more than 5 seconds (power button override)13. Verify Test Pass/Fail Criteria14. FWSTS: N/A
Test Pass/Fail Criteria:	System goes to S0/M0 to S5/M-Off and then to S5/M3 after ~ 4-5 seconds.

Test ID:	ME_PM_20.9a
Test Case Title:	S3/M-Off to S5/M-Off in WoWLAN Coexistence Mode
Mandatory/Optional:	Mandatory
Description:	<p>This test checks for S3/M-Off to S5/M3 flow; LAN Power Policy - Power Policy #2, WLAN Link Policy `#3: Enabled in S0, Sx/AC'; power source - DC; trigger: Power Button Override</p> <p>Notes:</p> <p>If Deep S4/S5 state is enabled on the platform under test, make sure Deep S4/S5 global parameters are configured in PETS:</p> <ol style="list-style-type: none">1. "Deep S4/S5 enabled" should be set to TRUE2. "Deep S4/S5 Policy" should be configured to the policy chosen in BIOS.
Objective:	This test checks for S3/M-Off to S5/M-Off flow



Test ID:	ME_PM_20.9a
Procedure:	<ol style="list-style-type: none"> 1. Configure BIOS to keep the system in S5 after exiting G3 (Intel® ME available) 2. If the SUT has WLAN support, enable the host WoWLAN driver setting. 3. Set the Original Power Policy to #2: ON in S0, Intel® ME Wake in S3/AC, S4-S5/AC 4. Set Wireless Link Policy '#3: Enabled in S0, Sx/AC'. <p>Note: This is required only when wireless is used.</p> <ol style="list-style-type: none"> 5. Set the power source to DC 6. Boot the system to S0/M0 that is, make sure OS is up 7. Verify that Intel® ME is on (Intel® AMT answers ping by means of the LAN/WLAN interface) 8. Move host to Standby (S3) 9. Verify that Intel® ME is off (Intel® AMT does not answer ping by means of the LAN/WLAN interface) 10. Press PWR button for more than 5 seconds (power button override) 11. If Deep S4/S5 is enabled and configuration policy matches the original power state of this test, check for Deep S4/S5 signal. (For details on Deep S4/S5 policies, refer Table 12-1 in the beginning of this chapter) 12. Verify Test Pass/Fail Criteria. 13. FWSTS: N/A
Test Pass/Fail Criteria:	<p>Host goes to S5 by means of the S0 and stays in S5. Intel® ME goes to M-Off. Intel® AMT is not reachable by means of the LAN/WLAN interface.</p> <p>Note: Depending on OEM implementation system may directly go to G3 after power button override event instead of going to S5.</p> <p>If Deep S4/S5 is enabled and configuration policy matches the target power state, platform should be in Deep S4/S5 state.</p>

Test ID:	ME_PM_20.22a
Test Case Title:	S3/M3 to S5/M3 in WoWLAN Coexistence Mode
Mandatory/Optional:	Mandatory
Description:	This test checks for S3/M3 to S5/M3 flow; LAN Power Policy - Power Policy #2, WLAN Link Policy '#2: Enabled in S0 only'; power source - ACDC; trigger: Power Button Override
Objective:	This test checks for S3/M3 to S5/M3 flow.
Procedure:	<ol style="list-style-type: none"> 1. Configure BIOS to keep the system in S5 after exiting G3 (Intel® ME available) 2. If the SUT has WLAN support, enable the host WoWLAN driver setting. 3. Set the Original Power Policy to #2: ON in S0, Intel® ME Wake in S3/AC, S4-S5/AC 4. Set Wireless Link Policy '#2: Enabled in S0 only'. <p>Note: This is required only when wireless is used.</p> <ol style="list-style-type: none"> 5. Set the power source to AC+DC 6. Boot the system to S0/M0 that is, make sure OS is up 7. Verify that Intel® ME is on (Intel® AMT answers ping by means of the LAN/WLAN interface) 8. Move host to Standby (S3) 9. Verify that Intel® ME is on (This can be done by checking SLP_A# signal, that should be de-asserted, indicating Intel® ME is in M3.) 10. Press PWR button for more than 5 seconds (power button override) 11. After 4-5 seconds Verify that Intel® ME is on (This can be done by checking SLP_A# signal, that should be de-asserted, indicating Intel® ME is in M3.) 12. Verify Test Pass/Fail Criteria 13. FWSTS: N/A
Test Pass/Fail Criteria:	System goes to S0/M0 to S5/M-Off and then to S5/M3 after ~ 4-5 seconds. Intel® AMT answers ping by means of the LAN interface only.



Test ID:	ME_PM_20.23a
Test Case Title:	S3/M-Off to S5/M3 in WoWLAN Coexistence Mode
Mandatory/Optional:	Mandatory
Description:	This test checks for S3/M-Off to S5/M3 flow; LAN Power Policy - Power Policy #2, WLAN Link Policy `#2: Enabled in S0 only'; power source - ACDC; trigger: Power Button Override
Objective:	This test checks for S3/M-Off to S5/M3 flow
Procedure:	<ol style="list-style-type: none">1. Configure BIOS to keep the system in S5 after exiting G3 (Intel® ME available)2. If the SUT has WLAN support, enable the host WoWLAN driver setting.3. Configure idle timeout value in Intel® MEBX to 14. Set the Original Power Policy to #2: ON in S0, Intel® ME Wake in S3/AC, S4-S5/AC5. Set Wireless Link Policy `#2: Enabled in S0 only'. <p>Note: This is required only when wireless is used.</p> <ol style="list-style-type: none">6. Set the power source to AC+DC7. Boot the system to S0/M0 that is, make sure OS is up8. Verify that Intel® ME is on (Intel® AMT answers ping by means of the LAN/WLAN interface)9. Move host into Standby (S3)10. Verify that Intel® ME is on (This can be done by checking SLP_A# signal, that should be de-asserted, indicating Intel® ME is in M3.)11. Wait for idle timeout expiry for ME to enter M-Off (To make sure ME enters M-Off check SLP_A# status)12. Press PWR button for more than 5 seconds (power button override)13. After 4-5 seconds Verify that Intel® ME is on (This can be done by checking SLP_A# signal, that should be de-asserted, indicating Intel® ME is in M3.)14. Verify Test Pass/Fail Criteria15. FWSTS: N/A
Test Pass/Fail Criteria:	System goes to S0/M0 to S5/M-Off and then to S5/M3 after ~ 4-5 seconds. Intel® AMT answers ping by means of the LAN interface only

B.12 S0/M0 to S3/M-Off (Without Intel® ME Wake) to S3/M-Off (with Intel® ME Wake)

Test ID:	ME_PM_21.1a
Test Case Title:	S0/M0 to S3/M-Off (without Intel® ME Wake) to S3/M-Off (with Intel® ME Wake) in WoWLAN Coexistence Mode
Mandatory/Optional:	Mandatory Exemptions <input checked="" type="checkbox"/> Non-Mobile (AC-only) Systems
Wireless Only:	No
Description:	This test checks for S0/M0 to S3/M-Off (without Intel® ME Wake) to S3/M-Off (with Intel® ME Wake) flow; This test checks for S3/M-Off to S3/M-Off flow; LAN Power Policy - Power Policy #2;; power source - DC; trigger: DC->ACDC + Wait Idle Time



Test ID:	ME_PM_21.1a
Objective:	This test checks for S0/M0 to S3/M-Off (without Intel® ME Wake) to S3/M-Off (with Intel® ME Wake) flow
Procedure:	<ol style="list-style-type: none"> 1. Configure BIOS to keep the system in S5 after exiting G3 (Intel® ME available) 2. If the SUT has WLAN support, enable the host WoWLAN driver setting. 3. Set the idle timeout value in Intel® MEBX to 1 4. Set the Original Power Policy to #2: ON in S0, Intel® ME Wake in S3/AC, S4-S5/AC 5. Set the power source to DC 6. Boot the system to S0/M0 (that is, make sure OS is up) 7. Verify that Intel® ME is on (Intel® AMT answers ping by means of the LAN interface) 8. Move host to standby (S3) 9. Verify that ME is in M-Off state. This can be done by checking SLP_A# signal, that should be asserted, indicating Intel® ME is in M-Off. 10. Reconnect AC power cord. 11. Verify that Intel® ME is on (This can be done by checking SLP_A# signal, that should be de-asserted, indicating Intel® ME is in M3.) 12. Wait for IdleTimeout expiration to enter M-Off State (To confirm Intel® ME enters M-Off status check SLP_A# status) 13. Verify Test Pass/Fail Criteria 14. FWSTS: N/A
Test Pass/Fail Criteria:	Intel® AMT answers ping by means of the LAN interface. Host stays in S3 state. Intel® ME becomes M3. After Idle timeout expires Intel® ME turns off.

B.13 S0/M0 to S3/M-Off (with Intel® ME Wake) to S3/M-Off (Without Intel® ME Wake)

Test ID:	ME_PM_22.1a
Test Case Title:	S3/M-Off (with Intel® ME Wake) to S3/M-Off (without Intel® ME Wake) in WoWLAN Coexistence Mode
Mandatory/Optional:	Mandatory Exemptions <input checked="" type="checkbox"/> Non-Mobile (AC-only) Systems
Wireless Only:	No
Description:	This test checks for S3/M-Off to S3/M-Off flow; LAN Power Policy - Power Policy #2;; power source - ACDC; trigger: ACDC->DC



Test ID:	ME_PM_22.1a
Objective:	This test checks for S0/M0 to S3/M-Off (with Intel® ME Wake) to S3/M-Off (without Intel® ME Wake) flow
Procedure:	<ol style="list-style-type: none">1. Configure BIOS to keep the system in S5 after exiting G3 (Intel® ME available)2. If the SUT has WLAN support, disable the WoWLAN driver setting.3. Set the idle timeout value in Intel® MEBX to 14. Set the Original Power Policy to #2: ON in S0, Intel® ME Wake in S3/AC, S4-S5/AC5. Set the power source to AC+DC6. Boot the system to S0/M0 that is, make sure OS is up7. Verify that Intel® ME is on (Intel® AMT answers ping by means of the LAN interface)8. Move host to standby (S3)9. Verify that Intel® ME is on (This can be done by checking SLP_A# signal, that should be de-asserted, indicating Intel® ME is in M3.)10. Wait for IdleTimeout expiration to enter M-Off State (To confirm Intel® ME enters M-Off status check SLP_A# status)11. Disconnect AC power cord.12. Verify Test Pass/Fail Criteria13. FWSTS: N/A
Test Pass/Fail Criteria:	Intel® AMT does not answer ping by means of the LAN interface. Host stays in S3 state. Intel® ME stays M-Off.

§ §



C Appendix C — Power Management (PM) Stress Test Corporate in WoWLAN Coexistence Mode

For details on WoWLAN Coexistence and WoWLAN Coexistence Mode, including feature availability, review the *Intel® AMT and Wake On Wireless LAN Coexistence* feature overview found in document ID 546827.

Warning: In order to fully implement Wake on Wireless LAN (WoWLAN) in Sx states, the host BIOS must set HOST_WLAN_PP_EN. For more further details, refer the *PCH External Design Specification (EDS)* and the *Platform Design Guide (PDG)*. Failure to properly set the HOST_WLAN_PP_EN bit may result in failures for the tests described herein.

Tools for Testing:

- Intel® Platform Enablement Test Suite—Latest version of the tool from the Intel® CSME Compliancy kit release. Refer the Intel® Platform Enablement Test Suite user guide available in the Intel Compliancy kit for exact instructions on how to load and setup the Intel® Platform Enablement Test Suite software.
- System Under Test (SUT)—Should be connected to Intel® Automated Power Switch 3 (Intel® APS 3).

C.1 PM Test Coverage Summary

Test ID	Test Case Title	PETS/Manual	Form Factor
PM_ST_5	S0/M0 to S3/M-Off to S0/M0	Intel® PETS	DT, MB, WS/Server, LAN, WLAN
PM_ST_6	S0/M0 to S3/M3 to S0/M0	Intel® PETS	DT, MB, WS/Server, LAN, WLAN

Note: DT = Desktop, MB = Mobile, WS-Server = Workstation-Server, LAN = systems with LAN interface and test is performed using LAN interface, WLAN = systems with WLAN interface and test is performed using the WLAN interface, WLAN = systems with WLAN interface and test is performed using the WLAN interface, only if the WLAN card supports Host Wake on WLAN.

The tests in this section are designed to be run, individually, a large number of iterations. Some of them require changing the system configuration before being run. When performing very large numbers of iterations, the tests may each take many hours, and in some cases several days.

Intel validation runs each of these tests the number of iterations indicated. Each OEM should decide on the tolerance level required for their boards, and choose an appropriate number of iterations.



The tests in this section are not designed to be run automatically one after the other—the user needs to get the SUT into the starting state, and then run the test multiple times. However each test individually ends with the SUT in the same state as when it started, allowing for easy iteration.

Apart from where explicitly mentioned, the CSME Idle Timeout value should be set larger than 1, to ensure the system does not pass the timeout before the required state is noted.

If the platform is configured with Deep Sx or SUS Well Down enabled (on mobile platforms), according to the enabled Deep Sx S-state (DeepS4/DeepS5), expect the CSME to transition to M-Off when reaching that specific Sx state.

Tests that require the CSME Idle Timeout fails if there is noise on the network preventing CSME going to an idle state. Ensure that routers with spanning tree, for example, are not present on the network.

When running long iterations, ensure that the management console is set not to go to sleep, as this pause the test.

Ensure that the SUT can boot to OS without prompting the user for any actions (such as scanning drivers and so forth.), since this affects the stress tests that boot the SUT to the OS.

C.2 PM_ST_5: S0/M0 to S3/M-Off to S0/M0

Test ID:	PM_ST_5a
Test Case Title:	S0/M0 to S3/M-Off to S0/M0 in WoWLAN Coexistence Mode
Mandatory/Optional:	Mandatory
Form Factor:	Desktop, Mobile, and Workstation/Server
Description/Objective:	This test checks for the system power flow from S0/M0 to S3/M-Off to S0/M0
Procedure:	<p>If the SUT has WLAN support, enable the host WoWLAN driver setting.</p> <p>Initial State: S0/M0</p> <p>Power: PP1, ACDC</p> <p>Ensure that yellow bang is not seen on Drivers in Device Manager</p> <p>Trigger 1: Host go to S3</p> <p>Middle State: S3/M-Off</p> <p>Trigger 2: Ping Intel® AMT IP address by means of WS-MAN protocol by means of the WLAN interface to wake system.</p> <p>Final State: S0/M0</p> <p>Verify the system is in S0/M0 and verify the second bit of the FWSTS 2 register value should be 0x60002306</p> <p>Ensure that yellow bang is not seen on Drivers in Device Manager</p> <p>At the end of procedure ensure that no SPI flash logs are found (For example you can use MEInfo to check)</p>
Iterations:	Mobile: >= 2000 Desktop: >= 750
Test Pass/Fail Criteria:	Test passes if all steps are completed successfully, for at least the recommended number of iterations as set by the OEM per the tolerance level of the system design.



C.3 PM_ST_6: S0/M0 to S3/M3 to S0/M0

Test ID:	PM_ST_6a
Test Case Title:	S0/M0 to S3/M3 to S0/M0 in WoWLAN Coexistence Mode
Mandatory/Optional:	Mandatory
Form Factor:	Desktop, Mobile, and Workstation/Server
Description/Objective:	This test checks for the system power flow from S0/M0 to S3/M3 to S0/M0
Procedure:	<p>If the SUT has WLAN support, enable the host WoWLAN driver setting.</p> <p>Initial State: S0/M0</p> <p>Power: PP2, ACDC</p> <p>Ensure that yellow bang is not seen on Drivers in Device Manager</p> <p>Trigger 1: Host go to S3</p> <p>Middle State: S3/M3</p> <p>Trigger 2: Ping Intel® AMT IP address by means of WS-MAN protocol by means of the WLAN interface to wake system.</p> <p>Final State: S0/M0</p> <p>Verify the system is in S0/M0 and verify the second bit of the FWSTS 2 register value should be 0x68002106</p> <p>Ensure that yellow bang is not seen on Drivers in Device Manager</p> <p>At the end of procedure ensure that no SPI flash logs are found (For example you can use MEInfo to check)</p>
Iterations:	<p>Mobile: >= 2000</p> <p>Desktop: >= 750</p>
Test Pass/Fail Criteria:	Test passes if all steps are completed successfully, for at least the recommended number of iterations as set by the OEM per the tolerance level of the system design.

§ §