

Ice Lake Platform Intel® Converged Security and Management Engine (Intel® CSME) 13.0 and Intel® Sensor Solution Consumer Firmware

Compliance and Testing Guide

Revision 1.0

May 2019

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.

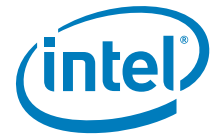
All information provided here is subject to change without notice. Contact your Intel representative to obtain the latest Intel product specifications and roadmaps.

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, Intel® Management Engine Interface (Intel® MEI), Intel® Converged Security and Management Engine (Intel® CSME), Intel® Platform Enablement Test Suite (Intel® PETS), Intel® Trusted Execution Technology (Intel® TXT), Intel® Management Engine BIOS Extension (Intel® MEBX), Intel® Active Management Technology or Intel® AMT, Intel® Power Management Script Player (Intel® PMSP), Intel® Automated Power Switch Signal Detection Board (Intel® APS SDB), Intel® vPro™, Intel® Trusted Platform Module (Intel® TPM), Intel® WiDi Technology or Intel® WiDi, Intel® WiMAX, Intel® Dynamic Application Loader (Intel® DAL), Intel® Identity Protection Technology (Intel® IPT), Intel® Small Business Advantage (Intel® SBA), Intel® Small Business Technology (Intel® SBT), Intel® Automated Power Switch (Intel® APS), Intel® Platform Trust Technology (Intel® PTT) Compliancy, Intel® Trusted Execution Engine (Intel® TXE), Intel® Virtualization Technology (Intel® VT), Intel® Setup and Configuration Software (Intel® SCS), Intel® Active Client Manager (Intel® ACM), Intel® PRO/100 PC Card Adapter, Intel® 5 Series Express Chipset, Intel® Communications Chipset 89xx Series, Intel® X58 Express Chipset, Intel® H57 Express Chipset, Intel® Q57 Express Chipset, Intel® Experience Center (Intel® EC), Intel® Integrated Sensor Solution, Intel® Ready Mode Technology (Intel® RMT), Intel® Automated Workflow Suite (Intel® AWS), Intel® Authenticate Solution, Intel® In-Target Probe (Intel® ITP), Intel® Firmware Update Tool (Intel® FWUT), Intel® Core™, Intel® Core™ M, 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.

© 2017-2019, Intel Corporation. All rights reserved.

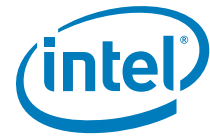


Contents

1	Introduction	12
1.1	Purpose and Scope of This Document	12
1.2	Features	12
1.3	General Notes for Intel® CSME Firmware	13
1.3.1	WoWLAN or WoL—Driver Feature	13
1.3.2	Windows* 10 Fast Startup (Partial Hibernate)	13
1.3.3	Environment Networking Recommendations	13
1.3.3.1	General	13
1.3.3.2	Wireless	13
1.4	Terminology	13
1.5	Acronyms, Definitions, and Terminology	14
1.5.1	General	14
1.5.2	System States and Power Management	14
1.5.3	Wireless and Mobile	15
1.6	Reference Documents	16
1.7	External References	16
1.8	Intel® Platform Enablement Test Suite (Intel® PETS) Testing Guidelines	17
1.9	Boot Guard—Discrete TPM and Intel® Platform Trust Technology (Intel® PTT)	17
2	Intel® Trace Hub (Intel® TH)	20
2.1	Trace Hub Compliance Test Coverage Summary	20
2.2	Intel® CSME FW—DCI Enable (MEEN)	20
2.3	BIOS—DCI Enable (HEEN)	22
2.4	BIOS—DCI Enable Post EOM	22
2.5	Capture ITH BIOS/ME Tracing Via CCA	24
3	Signing and Manifesting Compliance	26
3.1	Introduction	26
3.2	Test Environment Setup	26
3.3	Tools for Testing	26
3.4	Signing and Manifesting Compliance Test Coverage Summary	26
3.5	Image Creation with OEM signed components	27
3.6	Debug Token	29
4	Intel® Converged Security and Management Engine (Intel® CSME) BIOS Compliancy	31
4.1	BIOS Compliancy Test Coverage Summary	31
4.2	End of Power-On Self-Test (POST)	32
4.3	CF9GR Locking/Unlocking	32
4.4	DRAM INIT Done	33
5	Intel® Converged Security and Management Engine (Intel® CSME) Manufacturing Mode Compliancy—Consumer	35
5.1	Manufacturing Mode Compliance Test Coverage Summary	35
5.2	CF9GR Locking/Unlocking	36
6	SPI Flash Interface	39
6.1	Test Coverage Summary	40
6.2	Descriptor Mode Test	41
6.3	Serial Flash Discoverable Parameter Test	41
6.4	4 Kbytes Erasable Blocks Test	42
6.5	SPI Flash Size Test	43
6.6	SPI Flash Vendor Specific Capabilities (VSCC) Test	43



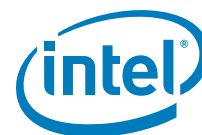
6.7	Flash Descriptor Security Override Test.....	45
6.8	Serial Flash Single Input, Dual, or Quad Output Fast Read Test.....	45
6.9	Serial Flash Dual and Quad I/O Fast Read	46
7	Common Services.....	48
7.1	Test System Configuration	48
7.2	Test Coverage Summary.....	48
7.3	Intel® ME Firmware Update.....	49
7.3.1	Tools for Testing.....	49
7.3.2	Intel® ME Firmware Update.....	49
8	Intel® Management Engine (Intel® ME) Power Management for Consumer Designs.....	52
8.1	System Power States	52
8.1.1	Deep S4/S5 Support	52
8.1.1.1	Exit from Deep S4/S5	53
8.1.2	Intel® ME Power Gating.....	53
8.1.3	Intel® Ready Mode Technology (Intel® RMT).....	53
8.2	Test Environment and System Configuration.....	53
8.2.1	Test Parameters	54
8.2.2	Tools for Testing.....	54
8.2.3	Test Environment Setup	54
8.2.4	Test Step Execution and Verification.....	56
8.2.5	Setup Environment Tests.....	58
8.3	Intel® ME Power Management Test Coverage Summary	62
8.4	ME_PM_1: S0/CM0 to S3/CM-Off	64
8.5	ME_PM_2: S3/CM-Off to S0/CM0	65
8.6	ME_PM_8: S0/CM0 to S4/CM-Off	68
8.7	ME_PM_9: G3 or S4/CM-Off (Suspend Well Off) to S0/CM0	70
8.8	ME_PM_10: S4/CM-Off (Suspend Well On) to S0/CM0.....	73
8.9	ME_PM_17: Cold Reset.....	77
8.10	ME_PM_18: Global Reset	78
8.11	ME_PM_19: Straight-to-S5, Intel® CSME Power Policy is S0 Only	79
8.12	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.....	84
8.13	ME_PM_26: Warm Reset.....	86
8.14	ME_PM_27: S0/CM0 or Sx/Mx to G3.....	89
8.15	ME_PM_44: S0/CM0-PG, CM0 to S4-S5/CM-Off	89
8.16	ME_PM_45: G3 or S4-S5/CM-Off to S0/CM0-PG, CM0.....	92
8.17	ME_PM_46: S0/CM0-PG, CM0 to S0/CM0-PG, CM0	96
9	Intel® Management Engine (Intel® ME) Power Management for Consumer Designs—Stress Testing.....	102
9.1	System Power States	102
9.2	Test Environment and System Configuration.....	102
9.2.1	Test Parameters	102
9.2.2	Tools for Testing.....	103
9.2.3	Test Environment Setup	103
9.2.4	Test Step Execution and Verification.....	104
9.2.5	Setup Environment Tests.....	104
9.3	Intel® ME Power Management Stress Test Coverage Summary	105
9.4	PM_ST_31: Host Reset from S0/CM0 (DOS/UEFI)	105
9.5	PM_ST_32: S0/CM0 to S5/CM-OFF to S0/CM0 via Power Button Override (DOS/UEFI)....	106
9.6	PM_ST_33: S0/CM0 to S3/CM-Off to S0/CM0 via Suspend and Power Button Press...	106
9.7	PM_ST_34: S0/CM0 to S4/CM-Off to S0/CM0 via Hibernate and WoL/WoWLAN	107
9.8	PM_ST_35: S0/CM0 to S5/CM-Off to S0/CM0 via Shutdown and Power Button Press.	108



10	Intel® Dynamic Application Loader (Intel® DAL)	111
10.1	Introduction	111
10.2	Test Environment for the Intel® Dynamic Application Loader (Intel® DAL)	111
10.2.1	Tools for Testing	111
10.2.2	Verify Needed Software is Installed on the Host	111
10.3	Intel® Dynamic Application Loader (Intel® DAL) Test Coverage Summary	112
11	Protected Media Playback	115
11.1	Overview	115
11.2	Scope	115
11.3	Prerequisite	115
11.4	Test Environment Setup	116
11.5	Media Playback Test Coverage Summary	116
12	Intel® Integrated Clock Control Compliance	121
12.1	Intel® Integrated Clock Control Test Coverage Summary and Details	121
12.2	Intel® Integrated Clock Control Test cases	122
12.2.1	Test Default Settings for Standard Configuration	122
12.2.2	Test Default Settings for Adaptive Configuration	122
12.2.3	Display Chipset Initialization Header Data	123
13	Manufacturing Flow Simulation Test	126
13.1	Manufacturing Flow Simulation Test	126
14	Intel® Device Protection Technology with Boot Guard	130
14.1	Overview	130
14.2	Scope	130
14.3	Prerequisite	130
14.4	Boot Guard Test Coverage Summary	131
15	Intel® Platform Trust Technology (Intel® PTT) Compliance	138
15.1	Intel® Platform Trust Technology (Intel® PTT) Compliance Test Coverage Summary	139
15.2	Verification of BIOS and Intel® Platform Trust Technology (Intel® PTT) Communication Over CRB Interface	140
15.3	Intel® Platform Trust Technology (Intel® PTT) Basic Functionality Under Windows* 10	141
15.4	Trusted Platform Module (TPM) Clear and Physical Presence	142
15.5	Windows* 10 BitLocker Integration	143
15.6	BitLocker TPM Protection	144
15.7	Virtual Smart Card Tests	145
15.8	Microsoft* Windows* Hardware Lab Kit (HLK) TPM Testing	146
15.9	Intel® Platform Trust Technology (Intel® PTT) Disable/Enable from BIOS	146
15.10	Intel® Platform Trust Technology (Intel® PTT) and Power Flows	147
15.11	Dictionary Attack Lockout After Coin Battery Removal with EOM Commit	147
16	Platform Controller Hub (PCH) SoftStrap Configuration	150
16.1	Test Coverage Summary	151
16.2	Intel Integrated Wired LAN Test	152
16.3	Wake On Wireless LAN (WoWLAN) Test	154
16.4	Flexible I/O Test	155
16.5	BIOS Boot-Block Size Test	163
16.6	Intel® Converged Security and Management Engine (Intel® CSME) SMBus Alert Sending Device (ASD) Address Test	164
16.7	Power State Deep Sx Test	166
16.8	Trusted Platform Module (TPM) on SPI Test	167
17	Intel® Virtualization Technology (Intel® VT)	169
17.1	Introduction	169



17.1.1	Purpose and Scope	169
17.1.2	Platforms Applicable.....	169
17.1.3	Terminology.....	169
17.1.4	Intel® Virtualization Testing Prerequisites	170
17.2	Intel® Virtualization Technology (Intel® VT) Test Plan and Details.....	170
17.3	Intel® VT Tests in EFI Shell.....	170
17.3.0.1	Test Environment.....	170
17.3.0.2	Verify Processor is Intel® VT Capable and Enabled.....	171
17.3.1	Intel® VT-x Tests with Microsoft* Client Hyper-V* on Windows* 10.....	173
17.3.1.1	Test Environment.....	173
17.3.1.2	User Guide—Microsoft* Client Hyper-V* and Virtual Machine Enabling and Installation Instructions	175
17.3.2	182
18	ISH firmware (FW) Compliancey.....	185
18.1	Intel® ISH firmware (FW) compliancy test coverage summary	186
18.2	Sensor communication test.....	187
18.3	Sensor data check	187
18.4	ISH FW loading and execution	188
18.5	Intel® SensorViewer test	188
18.6	Test system sensors.....	189
18.6.1	Sensor noise and error levels	189
18.6.2	Test system sensor noise and effects on sensor algorithms.....	190
18.6.3	Test worst case system interference and effect on sensor algorithms.....	191
18.7	Test system performance and effective calibration under a specific range of movements 192	
18.8	Barometer (pressure) sensor sanity test	193
18.9	Light sensor (ALS) accuracy Test	193
18.10	Light sensor (ALS) angular response test	194
18.11	360 hinge accuracy test with second accelerometer.....	195
18.12	PLM functionality verification	195
18.13	Heading sensor accuracy and drift test	197
18.14	Intel® Integrated Sensor Solution power states	198
18.15	Sensor activity contexts.....	199
18.16	Sensor terminal contexts	199
18.17	Sensor gesture contexts	200
18.18	Wake on shake test.....	200
18.19	Step Counting Test	201
19	Intel® Software Guard Extension (Intel® SGX)	203
19.1	Introduction.....	203
19.2	Intel® Software Guard Extension (Intel® SGX) Compliancey Test Coverage Summary	203
19.3	SGX Tests.....	204
19.3.1	SGX Enabled.....	204
19.3.2	SGX Disabled	205
19.3.3	SGX SW Controlled	205
19.3.4	Memory Allocation	206
19.3.5	SGX Functionality	206
19.3.6	EPID/PSE Provisioning	207
20	Enhanced Serial Peripheral Interface (eSPI).....	210
20.1	Introduction	210
20.2	Test Environment Setup.....	210
20.3	Tools for Testing	210
20.4	eSPI Compliancey Test Coverage Summary	210
20.5	Bootng with MAF configurations (straps set to MAF defaults).....	211



20.6	Platform boots with EC region	211
20.7	Platform boots with EC region in different place	212
20.8	Platform boots without EC region.....	212
20.9	IFWI with empty EC region	213
20.10	IFWI with empty EC binary	213
20.11	Platform boots with default EC region permissions	214
20.12	Platform boots with EC Read-Only permission to BIOS region	214
20.13	Platform boots with EC Read-Only permission to BIOS region and BIOS with RW permissions to EC.....	215
20.14	Perform FWUpdate with MAF configurations	215

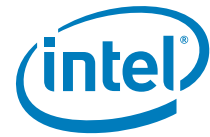


Figures

17-1 Boot Loader Settings	194
17-2 Example Warning—Allocating Space for Windows* 7/Virtual Machine	199
19-1 Intel® SGX Functional validation tool pass result example	224
19-2 Functional validation tool provisioning pass result example	225

Tables

1-1 Boot Guard—Discrete TPM and Intel® Platform Trust Technology (Intel® PTT)	18
7-1 Intel® AMT Test Coverage Summary	51
8-1 Supported Deep S4/S5 Policy Configurations	54
10-1 Compliance Tests for Verifying that the Intel® Dynamic Application Loader is Working	114
14-1 Boot Guard Tools for Testing	133
17-1 List of Applicable Platforms	173
17-2 Terminology	173
17-3 Virtualization Testing Prerequisites	174
17-4 Intel® Virtualization Technology (Intel® VT) Test Overview	174

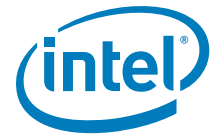


Revision History

Document Number	Revision Number	Description	Revision Date
573968	0.5	<ul style="list-style-type: none">• Initial Release based on CNL/CFL Compliance Guide revision 0.8	July 2017
	0.6	<ul style="list-style-type: none">• Intel® Trace Hub:<ul style="list-style-type: none">— Updated Intel® System Debugger documentation reference.• Signing and Manifesting:<ul style="list-style-type: none">— Updated the form factor.— Added an important note for tests.— Clarified test pass criteria.• Intel® Online Connect (Intel® IOC):<ul style="list-style-type: none">— Added secure pay test.	September 2017
	0.7	<ul style="list-style-type: none">• Intel® Management Engine Power Management for Consumer Designs:<ul style="list-style-type: none">— Updated Power Gating test cases.— Removed Deep S3 test cases and references.— Removed Intel RMT references and relevant tests and test steps.• Intel® Management Engine Power Management for Consumer Designs-Stress Testing:<ul style="list-style-type: none">— Removed Deep S3 references.— Removed Intel RMT references and relevant test steps.• Protected Media Playback:<ul style="list-style-type: none">— Removed tests Media_002 and Media_005.• Intel® Integrated Clock Control (Intel® ICC) Compliance:—<ul style="list-style-type: none">Updated supported PCHs in Intel® ICC feature support and Intel® ICC tests coverage summary tables— Updated Intel® PETS test packages for Intel® ICC— Removed tests ICC_TST_07/08/09— Removed steps that involved checking register value and added CCT API commands instead for tests ICC_TST_02/03/06— Updated test ICC_TST_003 (Adaptive profile) as follows:<ul style="list-style-type: none">o Changed the frequency from 98.875 MHz to 98.200 MHz.o Changed the Spread Spectrum from 0.48% to 0.50%.o Changed MIN frequency from 98.00 MHz to 97.50 MHz.— Added a confirmation step for test ICC_TST_10 procedure, where the returned readings are verified.• Intel® Online Connect (Intel® IOC):<ul style="list-style-type: none">— Added network and form factors.• Platform Controller Hub (PCH) Soft Strap Configuration:— Updated strap offsets for Ice Lake-LP.• Intel® Virtualization Technology (Intel® VT):<ul style="list-style-type: none">— Updated the settings for POSTBOOT SAI.	January 2018



Document Number	Revision Number	Description	Revision Date
573968	0.75	<ul style="list-style-type: none"> ● Intel® Trace Hub Compliance: <ul style="list-style-type: none"> — Updated the procedure for tests ITH_001 to ITH_003: Updated the name of the XML file reflecting the silicon and probe. Added a test step before opening the ISD. ● SPI Flash Interface: <ul style="list-style-type: none"> — Updated passing criteria of test SPI-004 ● Intel® Device Protection Technology with Boot Guard: <ul style="list-style-type: none"> — Removed Profile 1 Test Case (BtG_04) due to removal of Profile 1 and 2 ● Intel® Platform Trust Technology (Intel® PTT) Compliance:— <ul style="list-style-type: none"> — Removed the check for the manufacturer name and version from test PTT_002 ● PCH Soft Strap Configuration: <ul style="list-style-type: none"> — Corrected encoding on LAN PHY Power Control GPD11 Signal Configuration. ● ISS Compliance: <ul style="list-style-type: none"> — updated test ISS_TST_14 procedure for DeepSx test steps ● Enhanced Serial Peripheral Interface (eSPI): <ul style="list-style-type: none"> — Added new chapter with tests eSPI_001 to eSPI_011 to verify the eSPI configuration and functionality. 	March 2018
	0.8	<ul style="list-style-type: none"> ● Removed the following chapters: <ul style="list-style-type: none"> — Intel® IPT Compliance — Intel® IOC Compliance ● Intel® Trace Hub <ul style="list-style-type: none"> — Added step to perform RTC clear in test ITH_001 to make sure MEEN is effective ● Intel® Integrated Clock Controller (Intel® ICC) Compliance: <ul style="list-style-type: none"> — Removed ICC_TST_01 — Added a note for ICC_TST_10 ● Intel® Device Protection Technology with Boot Guard <ul style="list-style-type: none"> — Updated Boot Guard tool for testing (txbtginfo.exe) — Removed references of Boot Guard profiles 1 and 2 	June 2018
	1.0	<ul style="list-style-type: none"> ● Intel® Trace Hub: <ul style="list-style-type: none"> — update the method of download and location of user guide. ● Intel® Power Management: <ul style="list-style-type: none"> — In test cases "Check Deep S4, S5" added DC, since some customers platform act Deep S4, S5 in DC mode. — Added note about S4 state Wake on LAN test cases. — Removed the note about S4 Wake on LAN (WoL) since it is for WHL only. ● Intel® Power Management Stress Testing: <ul style="list-style-type: none"> — Added note about S4 state Wake on LAN test cases. — Removed the note about S4 Wake on LAN (WoL) since it is for WHL only. ● Intel® Signing and Manifesting: <ul style="list-style-type: none"> — Updated SIGN_01 test details. — Replaced SIGN_02 test with SECTOK_02. ● Intel® Dynamic Application Loader: <ul style="list-style-type: none"> — Updated Chapter Introduction description. ● Intel® Protected Media Playback: <ul style="list-style-type: none"> — Updated the picture of content protection explanation. — edited the form factor that ICL support. ● Intel® Integrated Clock Controller: <ul style="list-style-type: none"> — Dropped support for the old ICC tools and replaced it with new ICC Tool. ● Intel® Virtualization Technology: <ul style="list-style-type: none"> — Removed Xen*/ Linux* Environment tests. 	May 2019



(This page intentionally left blank.)

1 Introduction

1.1 Purpose and Scope of This Document

The Intel® Converged Security and Management Engine (Intel® CSME) Compliance Guide for Ice Lake Platforms is designed to provide original equipment and device manufacturers with the compliancy requirements for Ice Lake based platforms. Included is 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 only
- LAN + WLAN
- WLAN only

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

Note: This document supports the following Operating Systems:
— Windows* 10

1.2 Features

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

The Consumer Intel® CSME firmware binary implements a power-gating feature that can reduce Intel® CSME idle power consumption within the PCH to near zero milliwatts.

Intel® CSME enters power-gated mode when the firmware becomes idle and the platform is in either the S0 or S0ix state. This power-gated state (of the Intel® ME) is represented as CM0-PG. Intel® CSME firmware exits CM0-PG state, when Intel® CSME activity is requested, or when host activity requires firmware execution, such as when power transition events occur.



1.3 General Notes for 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 to 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 is published.

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

1.3.2 Windows* 10 Fast Startup (Partial Hibernate)

The 'Windows* 10 Fast Startup' feature should be disabled, while running Intel® PETS tests, as when enabled, the platform will not go into system power state S5, thus all S5-related tests will fail.

1.3.3 Environment Networking Recommendations

1.3.3.1 General

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

1. Disable or shutdown non-essential applications or services on the Management Console, 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 Management Console (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 the 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.

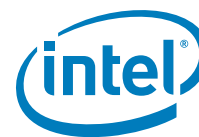
1.5 Acronyms, Definitions, and Terminology

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 Keyboard Controller (KBC)
USB-R	Integrated Device Electronics-Redirect
Intel® MEI	Intel® Management Engine Interface (Intel® MEI)
Intel® TXT	Intel® Trusted Execution Technology (Intel® TXT)—Formerly code named LaGrande Technology (LT)
MAC	Media Access Control
MC	Management Console
PET	Platform Event Trap
PID	Provisioning ID
PPS	Provisioning Pass Phrase
PSK	Pre-Shared Key
RPMC	Replay Protected Monotonic Counters
SOL	Serial Over LAN
SPI	Serial Peripheral Interface
SUT	System Under Test
TPM	Trusted Platform Module

1.5.2 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 to latest industry ACPI specification).
S0-S0ix	Core Well Powered—Intel® CSME Well Powered; (Intel® CSME 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 to the 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 to 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 to latest industry ACPI specification).
Sx	Any power state that is not S0



Acronym or Terminology	Definition
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® CSME Firmware power state where all hardware power planes are activated and the host power state is S0.
CM0-PG	Core Well Powered, Intel® CSME Well Powered, (Intel® CSME core not consuming power) DRAM available
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® CSME sub system and host sub system
PG	Power Gating

1.5.3 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 of an Access Point. All communications to and from the wireless nodes flow through the Access Point.
CCK	Complementary Code Keying
CCX	Cisco Certified Extensions
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 CCL or in VIP kit
Intel® Virtualization Technology for Directed I/O Architecture Specification	http://download.intel.com/technology/computing/vptech/Intel(r)_VT_for_Direct_IO.pdf
Intel® 64 and IA-32 Architectures Software Developer's Manual, Volume 3B	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 http://xen.org/download/index.html
Intel® TXT – Trusted Boot Checkout Kit	VIP Kit number - TBD
EFI shell (DUET – FAT32)	http://developer.intel.com/technology/efi/agreesource.htm
Ice Lake Platform Controller Hub (PCH) LP External Design Specification (EDS)	CCL: TBD
Ice Lake Platform Power Sequence Specification	TBD
Ice Lake Platform Design Guide	CCL: TBD
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) 13 Firmware PRD	TBD
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® CSME Compliance Kit
Intel® Management Engine (Intel® CSME 13) Tools - Product Requirements Document	TBD
Intel® Platform Enablement Test Suite User Guide	Located in Intel® Compliance Kit
Intel® APS Setup and Configuration Guide for OEMs	Located in Intel® Compliance Kit
Intel® Automated Power and System State Test Device (Intel® APS) User's Guide for OEMs	Located in Intel® Compliance Kit
Intel® AMT Tools User Guide	Located in Intel® Compliance 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



Document	Location
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 rev	http://www.dmtf.org/standards/asf/
ACPI Specification	http://www.acpi.info/spec20c.htm

1.8 Intel® Platform Enablement Test Suite (Intel® PETS) Testing Guidelines

Intel recommends that customers run Intel® PETS tests, whenever there are any changes in:

- BIOS
- New 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 ICC test package
3. Run SPI test package
4. Run BIOS test package
5. Run Power Test packages
6. Run Feature tests (WLAN and so forth) depending on the SKU

Note: To enable WoL, go to Device Manager > (select network adaptor) > Properties > Advanced. Change **Enable PME** to **enabled**.

1.9 Boot Guard—Discrete TPM and Intel® Platform Trust Technology (Intel® PTT)

The following table 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 to Boot Guard and Intel® PTT chapter for actual compliancy tests.

Definitions:

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

**Table 1-1. Boot Guard—Discrete TPM and Intel® Platform Trust Technology (Intel® PTT)**

Platform 2017 ⁺⁺	Intel® Active Client Manager (Intel® ACM)	Intel® CSME Firmware	Intel® PTT	TPM 1.2	TPM 2.0
ICL Based (1-Chip and 2-chip)	Intel® ACM 3.x	Consumer	Yes	Yes	Yes
		Corporate Intel® vPro™	Yes*	Yes	Yes

Notes:

1. ⁺⁺Refer to platform dashboard for PoR configurations.
2. *Refer to PTT documentations for vPro compatibility.

§ §



(This page intentionally left blank.)



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

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 to 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 to the Bring up Guide for more details on image creation.

2.1 Trace Hub Compliance 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.
- Form Factor: D = Desktop, M = Mobile, A = All in one, W = Workstation.

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

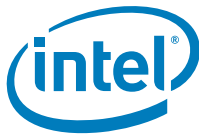
Note: ITH_003 requires the SUT to be out of manufacturing mode, refer ITH_003 for more information.

2.2 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).



Test ID:	ITH_001
Objective:	To enable DCI through Intel® CSME
Procedure:	<ol style="list-style-type: none"> 1. Install Intel® System Debugger, which supports the platform on the 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 Disabled. 5. 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\ICL and look for the xml files that reflects the silicon and probe (Example: "ICL-ICP_DCI"). 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="ICL_ICP_DCI" />). 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 user is able to connect the target over DCI and are able to see the following message in 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>

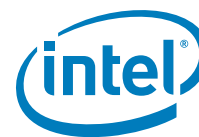


2.3 BIOS—DCI Enable (HEEN)

Test ID:	ITH_002
Test Case Title:	BIOS—DCI Enable
Mandatory/Optional:	Mandatory
Description:	Check that DCI interface can be enabled through BIOS (HEEN)
Objective:	To enable DCI through BIOS
Procedure:	<ol style="list-style-type: none">1. Install Intel® System Debugger, which supports the platform on a 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 to # 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\ICL and look for the xml files that reflects the silicon and probe (Example: "ICL-ICP_DCI").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="ICL_ICP_DCI" />). 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 user is able to connect the target over DCI and are able to see the following message in 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>

2.4 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 will not be capable of enabling DCI on the platform. DCI interface can be enabled only through BIOS
Objective:	To enable DCI through BIOS



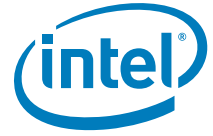
Test ID:	ITH_003
Procedure:	<ol style="list-style-type: none"> 1. Install Intel® System Debugger which supports the platform on a console. 2. Execute fpt -closemfn so that the platform is out of manufacturing mode. Check FWSTS to confirm that the platform is out of manufacturing (HECI1_CSE_FS - Host 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 to # 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\ICP and look for the xml files that reflects your silicon and probe (Example:"ICL-ICP_DCI"). 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="ICL_ICP_DCI" />). 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 user is able to connect the target over DCI and are able to see the following message:</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 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">1. Flash image that has DCI and Intel(R) CSME trace enabled.2. 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.3. Open the Intel® System Debugger.4. Use a fresh workspace and use the setup project menu to configure the trace project. Refer to System Trace chapter of System Debugger Getting started Guide for more details.5. 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">6. Connect to the target by clicking the green button on the Target Connection tab.7. Start the trace by clicking the play button in the Trace Capture tab.8. Restart the target with the restart option from Windows* menu.9. Check, if we are able to collect BIOS and Intel® CSME logs in the STT and the messages are time correlated.10. Shut down target by selecting shutdown option from Windows* menu.11. Power on the target to boot from S5 to S0 state.12. Check, if we are able to collect BIOS and Intel® CSME logs in the STT and the messages are time correlated.13. Put the target to standby mode (S3).14. Resume the target to boot from standby by pressing the Power Button.15. Check, if we are able to collect BIOS and Intel® CSME logs in the STT and the messages are time correlated.16. Execute a cold reset by writing 0xE to CF9 register (mm CF9 0xE -io)17. Check, if we are able to collect BIOS and Intel® CSME logs in the STT and the messages are time correlated.18. Execute a warm reset by writing 0x6 to CF9 register (mm CF9 0x6 -io)19. 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 we are able to collect BIOS and Intel® CSME logs in the STT and the messages are time correlated.





(This page intentionally left blank.)



3 Signing and Manifesting Compliance

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 another 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

- Platform Flash Tool (PFT): 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.
- Flash Image Tool (FIT): Tool used to stitch FW image, can be found in ME FW kit.
- Flash Programming Tool (FPT): Tool used to burn images on SPI platforms, and set EOM state.

3.4 Signing and Manifesting Compliance Test 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 Supported	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 will sign OEM-provided binaries and add them to the image. The public key hashes of all the OEM-provided binaries signatures will be entered into the OEM Key Manifest, which will be 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:	SECTOK 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 will recognize the injected token.
Test Pass Criteria:	Platform is in OEM Unlock State
Description:	OEM will create a token. The public key hash will be entered into the OEM Key Manifest, which will be included in the IFWI image. The token will be injected into the platform using DnX. Platform moves to OEM Unlock Status
Windows* Procedure:	<p>Manual procedure.</p> <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 user choose NOT to stitch within IFWI, then continue to inject token via Intel® Flash Programming tool OR Intel® Platform Flash Tool if user is using DnX APIs (Refer to 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 enabled. b. Connect Lauterbach to capture NPK messages (using NPK decoder released in compliance kit). c. Initiate warm reset. d. Verify NPK log contains the following message: "Accept secure token".





(This page intentionally left blank.)



4 Intel® Converged Security and Management Engine (Intel® CSME BIOS Compliance

The Intel® Management Engine 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® Converged Security and Management Engine (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).

Tools for testing:

- Intel® Platform Enablement Test Suite—Latest version of the tool from the Intel® CSME Compliance kit release. Refer to 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.

4.1 BIOS Compliance Test Coverage Summary

OS Support', and 'How?' Columns 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.

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

Network Factor: 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	How?	Intel® PETS Package Name	OS Support	Form Factor	Network Factor
BIOS_01	End of POST	A	Compliance_MeBios.xml	W WI	D M A	LAN+WLAN; WLAN only
BIOS_02	CF9GR locking/unlocking - non Manufacturing Mode	A	Compliance_MeBios.xml	W WI	D M A	LAN+WLAN; WLAN only
BIOS_03	DRAM INIT Done	A	Compliance_MeBios.xml	W WI	D M A	LAN+WLAN; WLAN only

Note: BIOS_04 belongs to "Intel® Management Engine Manufacturing Mode" Compliance Chapter, available at summary Table



4.2 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 that BIOS is required to send an “End of POST” message to the Intel® Management Engine 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) at PCI address space at B0:D22:F0 register offset 40h [bit 4] can determine if the Intel® CSME is in the Manufacturing Mode. For shipping machine, HFSTS at PCI address space at PCH B0:D22:F0 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 will perform 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 (CM-Off->CM0)iii. S4 -> S0 (CM-Off->CM0)b. Boot to OS and verify if END_OF_POST message was sent by BIOS or not.c. Read the PCI address space at PCH B0:D22:F0 register offset 40h [bit 4] to verify the Intel® CSME Manufacturing Mode bit is set as given below. 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.

4.3 CF9GR Locking/Unlocking

Test ID:	BIOS_02
Test Case Title:	CF9GR 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.



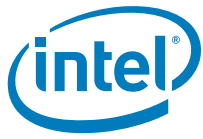
Test ID:	BIOS_02
Objective:	For security reasons, the BIOS must ensure that CF9GR is cleared and locked before handing control to the OS in the shipping machine (Intel® CSME not in manufacturing mode). Note. The recommended allocation of PWRMBASE is 0xFE000000 in PCH BIOS Specification.
Procedure:	<ol 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.

4.4 DRAM INIT Done

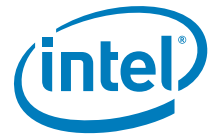
Test ID:	BIOS_03
Test Case Title:	DRAM INIT Done
Mandatory/Optional:	Mandatory
Description:	The BIOS is required to send the DRAM INIT Done message which belongs to MKHI_OSBUP_COMMON_GROUP. This message is sent by the BIOS prior to the End of Post (EOP) on the boot where host wants to indicate to Intel®ME firmware that DRAM initialization is complete and CSME UMA is ready to use.
Objective:	Verify that the BIOS sets the DRAM INIT Done message and the Intel® CSME transitions to CM0 with UMA. Note: Host Firmware Status Register (HFSTS at PCI address space at PCH B0:D22:F0 register offset 40h bits [8:6] can determine if the Intel® CSME is in the CM0 with UMA state. Check for "CM0 with UMA" state once CSME exits from "CM0-PG" state.
Procedure:	<p>For each of the following system transitions:</p> <p>G3 -> S0 (CM-Off->CM0) S5 -> S0 (CM-Off->CM0) S4 -> S0 (CM-Off->CM0)</p> <p>Boot to OS and read the PCI address space at PCH B0:D22:F0 register offset 40h to verify the Intel® CSME HFSTS1 [bits 8:6] is set to '001'. If [bits 8:6] is equal to '001', it means Intel® CSME has transitioned to CM0 with UMA. If [bit 8:6] is 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.





(This page intentionally left blank.)



5 Intel® Converged Security and Management Engine (Intel® CSME Manufacturing Mode Compliance—Consumer

The Intel® Management Engine Manufacturing Mode compliance 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 Compliance section:

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

Tools for testing:

- Intel® Platform Enablement Test Suite (Intel® PETS)—Latest version of the tool from the Intel® CSME Compliance Kit release. Refer to the *Intel® Platform Enablement Test Suite User Guide* available in the Intel® Compliance 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.

5.1 Manufacturing Mode Compliance Test Coverage Summary

'OS Support', and 'How?' Columns 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.

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

Network Factor: 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.

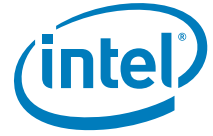
Test ID	Test Case Title	How?	Intel® PETS Package Name	OS Support	Form Factor	Network Factor
BIOS_04	CF9GR locking/unlocking - Manufacturing Mode	A	Compliance_MeBios_ManufacturingMode.xml	W WI	D M A	LAN+WLAN; WLAN only



5.2 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® CSME manufacturing mode, BIOS must set the CF9GR register (Memory-mapped address at PWRMBASE register offset 1048h [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 PWRMBASE register offset 1048h [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. Note. The recommended allocation of PWRMBASE is 0xFE000000 in PCH BIOS Specification.
Procedure:	<ol style="list-style-type: none">1. Boot the system under test to OS.2. Intel Platform Enablement Test Suite will perform 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® CSME Manufacturing Mode bit is equal to '1'.b. Manually read the memory-mapped address at PWRMBASE register offset 1048h [bit 20] to verify the bit is set to '0'.c. Manually read the memory-mapped address at PWRMBASE register offset 1048h [bit 31] to verify the bit is set to '0'.
Test Pass/Fail Criteria:	Test passes if the PWRMBASE register offset 1048h [bit 20] = '0' and [bit 31] of the same register is '0' when the system is in the Intel® CSME manufacturing mode.







(This page intentionally left blank.)



6 SPI Flash Interface

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 verifies implementation of SPI Dual and Quad I/O Fast Read, SPI Flash Descriptor mode, and ensure compliance with Intel® CSME and Intel® GbE requirements.

Tools for Testing:

Intel® Platform Enablement Test Suite (PETS)—Use latest version of this kit. Refer to 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).

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).



6.1 Test Coverage Summary

OS Support', and 'How?' Columns 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.

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

Network Factor: 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	How?	Intel® PETS Package Name	OS Support	Form Factor	Network Factor
SPI_001	Descriptor Mode Test	A	Compliance_SpiFlashC onfiguration.xml	W WI	D M	LAN+WLAN; WLAN only
SPI_002	Serial Flash Discoverable Parameter Test	A	Compliance_SpiFlashC onfiguration.xml	W WI	D M	LAN+WLAN; WLAN only
SPI_003	4 Kbytes Erasable Blocks Test	A	Compliance_SpiFlashC onfiguration.xml	W WI	D M	LAN+WLAN; WLAN only
SPI_004	SPI Flash Size Test	A	Compliance_SpiFlashC onfiguration.xml	W WI	D M	LAN+WLAN; WLAN only
SPI_005	SPI Flash VSCC Test	A	Compliance_SpiFlashC onfiguration.xml	W WI	D M	LAN+WLAN; WLAN only
SPI_006	Flash Descriptor Security Override Test	A	Compliance_SpiFlashC onfiguration.xml	W WI	D M	LAN+WLAN; WLAN only
SPI_007	Single Input, Dual or Quad Output Fast Read Test	A	Compliance_SpiFlashC onfiguration.xml	W WI	D M	LAN+WLAN; WLAN only
SPI_008	Dual and Quad I/O Fast Read	A	Compliance_SpiFlashC onfiguration.xml	W WI	D M	LAN+WLAN; WLAN only



6.2 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:	<ol style="list-style-type: none"> 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.

6.3 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.
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 to SPI Programming Guide for details of these registers.
Test Pass/Fail Criteria:	Test passes if all steps return expected values.



6.4 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.
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® Converged Security and 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.



6.5 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:</p> <ol style="list-style-type: none"> 1. Intel® PETS will maintain a list of SPI flash device sizes.
Test Pass/Fail Criteria	<p>The test passes if the following conditions is true:</p> <ol style="list-style-type: none"> 1. The flash components' sizes in the SUT are less than or equal to the size stated in the SPI device manufacturer datasheet.

6.6 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.



Test ID:	SPI_005
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.



6.7 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 13 2. 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 will help 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 - closemfnf. 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.

6.8 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 will support 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.

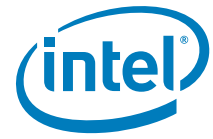


Test ID:	SPI_007
Objective:	This test is to verify that the flash parts will support Single Input, Dual, or Quad Output fast read if selected.
Procedure:	<p>PETS will ask the user whether 'Single Input Dual or Quad Output Fast Read' is supported.</p> <p>If yes,</p> <ol style="list-style-type: none">1. PETS will verify that FLCOMP bit 20 is set to 1b.2. PETS will then use Serial Flash Discovery Parameters to verify that all flash parts in the system support 'Single Input, Dual or Quad Output Fast Read'.3. PETS will check 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 will check if FLCOMP bit 12 is set to 1b. For Quad Output Read. PETS will check 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 will verify 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>

6.9 Serial Flash Dual and Quad I/O Fast Read

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 will support 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 will support Dual or Quad I/O Fast Read
Procedure:	<p>PETS will ask 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 will use Serial Flash Discovery Parameters (SFDP) to verify that all flash parts in the system support 'Dual or Quad I/O Fast Read'.2. PETS will 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; orb. FLCOMP bit 15 is set to 1, if Quad I/O fast read is supported.3. PETS will verify that FLCOMP bit 20 set to 1 <p>If No,</p> <ol style="list-style-type: none">4. PETS will 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; or5. 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 will 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>





(This page intentionally left blank.)

7 Common Services

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

- Intel® ME Firmware Update

7.1 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
<input checked="" type="checkbox"/> Desktop <input checked="" type="checkbox"/> Mobile	<input checked="" type="checkbox"/> Standard <input checked="" type="checkbox"/> Modern Standby or InstantGo

Form Factor: Describes the kind of system for which the test is applicable. These tests cover feature availability for associated platform.

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 or DeepS3 resting system state. Systems that support Modern Standby or Microsoft* Windows InstantGo will 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.

7.2 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 Requirement (Req.) column describes the requirement for test execution. The **Form Factor**, Operating System (OS), and network (Net) indicate the applicable test system configuration. **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 and M = Mobile

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 7-1. Intel® AMT Test Coverage Summary

Test ID	Title	Req.	Form Factor D M W	Power Model S M/I	Net	How?
CS_020	Intel® ME Firmware Update	C	<input checked="" type="checkbox"/> <input checked="" type="checkbox"/> <input checked="" type="checkbox"/>	<input checked="" type="checkbox"/> <input checked="" type="checkbox"/>	N	M

7.3 Intel® ME Firmware

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

7.3.1 Tools for Testing

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

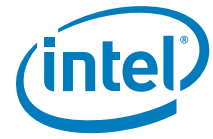
7.3.2 Intel® ME Firmware Update

ID:	CS_020					
Title:	Intel® ME Firmware Update					
Requirement:	Mandatory - exempt when upgrade/downgrade support is not yet available in firmware					
System:	<table><tr><td>Form Factor</td><td>System Power Model</td></tr><tr><td><input checked="" type="checkbox"/> Mobile</td><td><input checked="" type="checkbox"/> Standard <input checked="" type="checkbox"/> Modern Standby or InstantGo</td></tr></table>		Form Factor	System Power Model	<input checked="" type="checkbox"/> Mobile	<input checked="" type="checkbox"/> Standard <input checked="" type="checkbox"/> Modern Standby or InstantGo
Form Factor	System Power Model					
<input checked="" type="checkbox"/> Mobile	<input checked="" type="checkbox"/> Standard <input checked="" type="checkbox"/> Modern Standby or InstantGo					
Method:	Manual					
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:	<ol style="list-style-type: none">1. Enter a formatted USB Key into the management console.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.3. Place the selected update firmware image on the USB Key.4. Move the USB Key to the SUT.5. Run the Intel® FWUpdLcl tool on the SUT with the -save option, to save the current firmware image to the USB Key.6. Extract the current version of the Intel® ME firmware, using the Intel® MEInfo tool.7. Run the Intel® FWUpdLcl tool on the SUT to update the firmware to the image on the USB Key.8. Restart the SUT.9. Verify the SUT has booted to the Host OS.10. Extract the new version of the Intel® ME firmware using Intel® MEInfo and ensure that it has changed from the original firmware version.11. Verify that the new firmware version is correct.					



ID:	CS_020
Procedure: (continued)	<p>12. Run the Intel® FWUpdLcl tool on the SUT to restore the firmware to the original image extracted earlier from the SUT.</p> <p>13. Restart the SUT.</p> <p>14. Verify the SUT has booted to the Host OS.</p> <p>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.</p>
Pass Criteria:	<p>The test passes if the firmware update is successful, and the original firmware can be restored for each of the following conditions:</p> <ul style="list-style-type: none">• Update to newer version of firmware than what is installed on the SUT.• Downgrade to an older version of firmware than what is installed on the SUT. <p>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.</p>
References:	For details on Intel® ME firmware tools, refer to the <i>Intel® ME System Tools User Guide</i> .

§ §



(This page intentionally left blank.)



8 Intel® Management Engine (Intel® ME) Power Management for Consumer Designs

This chapter covers system power flow transitions which involve the Intel® ME firmware (and/or software).

8.1 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.

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

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

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

Table 8-1. 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
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.

8.1.1.1 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#.

Note: For additional details on Deep S4/S5, refer to the *KabyLake Mobile Platform Controller Hub-Low Power (PCH-LP) External Design Specification (EDS)*.

8.1.2 Intel® ME Power Gating

Note: Power Gating test cases validation should not be validated until the Alpha milestone.

Intel® ME firmware enters power gated state (CM0-PG) when the firmware is idle and system state is either S0 or S0ix. Intel® ME firmware exits CM0-PG state to process power management events on the system and when host applications require Intel® ME firmware services.

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

- Intel® ME Power Gating feature supported when the platform is in S0 state. In this case Intel® ME may enter power gated state (CM0-PG) when the firmware reaches idle state.

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 to Intel® ME 12.0 Firmware for Cannon Lake Mobile 1-Chip Based Platform—Product Requirements Document (PRD).

8.1.3 Intel® Ready Mode Technology (Intel® RMT)

Intel® Ready Mode Technology (Intel® RMT) is applicable for Desktop/All-in-one designs and is a replacement for Windows* Sleep (S3). Hence when Intel® RMT is enabled on desktop platforms, S3 test cases will be not applicable. If Intel® RMT is disabled, S3 test cases are applicable, and in this configuration Windows* should move to Sleep on S3.

8.2 Test Environment and System Configuration

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

The 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, e.g. 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.



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

8.2.1 Test Parameters

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

Example 8-1.Two-State Single 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

Example 8-2.Three-State with Double 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

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.

8.2.2 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 to 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.

8.2.3 Test Environment Setup

The management console may be a laptop or a desktop with a version of Windows* supported by Intel® Platform Enablement Test Suite (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.



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.

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® ME firmware Power Management testing:

- 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 should be setup on different subnets
- For Global reset tests to pass (ME_PM_18), the SUT should be in manufacturing mode.
- Following Test step has been added to Power flows which ends at S0 state Resuming back from S4 Hibernation. This will help 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*"}



8.2.4 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).

1. 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.
2. Ensure that CF9h Global Reset (CF9GR) is [set,cleared].
 - CF9GR bit is located at 0xFE001048 (BIT20) in PMC PWRM space on CNL. 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, 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.
 - CF9GR bit is located at 0xFE001048 (BIT20) in PMC PWRM space on CNL. Confirm that CF9 Lock down (CF9LOCK) bit 31 is set to **0b**. Information describing how to access this value may be found in the PCH EDS.
2. 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**.



3. 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® ME 'MeOn' states will appear the same in the table above. Follow the procedure below via the Host OS on the SUT to confirm if the Intel® ME is Power Gated (CM0-PG):
 - Get the Intel® CSME PG value by reading PPFEAR0 (n=0,1). Information describing how to access this value may be found in either the PCH EDS or the PCH BIOS Specification.
 - Read 8 bytes at 0xfe001d93 and 0xfe001d94 and verify these bits 15:0 equal FFh.
 - The above fields include non-CSME IP status, BIT25,26 are not part of CSME PG values. So if you see 0xF9 at 0xFE001D93, it is OK as PG test case.

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.

4. Verify that the SUT is in G3/MeOff (CM-Off).

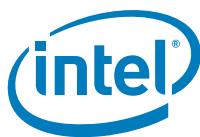
- Confirm that signals SLP_S3#, SLP_S4#, SLP_S5#, and SLP_A# are asserted low. Additionally, VccSus3_3 (and VccDSW3_3 for systems supporting Deep Sx) should be powered off.
- The signal and power rail state should remain stable for at least **5 seconds**. Furthermore, measurements should not be taken for at least **10 seconds** after state transition to allow full electric dissipation from the system.

5. 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.



6. 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**.
7. Verify that the Intel® ME on the SUT is off.
 - Confirm that the SLP_A# signal is asserted (low) for at least **5 seconds**.
8. Verify that the Intel® ME is configured in manufacturing mode.
 - The manufacturing mode status is available by querying the Intel® ME 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® ME Manufacturing Mode status should read "Enabled". The MEInfo tool is available from Intel via the Intel® ME firmware kit.
9. 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.

8.2.5 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.

ID:	Check S3	
Title:	S0/CM0 to S3/CM-Off to S0/CM0 via Host OS suspend cycle (AC-only)	
Requirement:	Optional	Non-Support <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 Host OS suspend cycle with the parameters outlined below.	
Parameters:	System Power Source 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 ➡ Power Button press
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. 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. 	
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). 	
Pass Criteria:	The test passes if the SUT moves to S3 and then to S0, and the Intel® ME is in MeOn (CM0, CM0-PG).	



ID:	Check S4	
Title:	S0/CM0 to S4/CM-Off to S0/CM0 via Host OS hibernate cycle (AC-only)	
Requirement:	Optional	
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:	If Deep S4, Deep S5, and/or G3 are 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/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 S4, S5, Deep S4, Deep S5, G3/MeOff (CM-Off)
		Final S0/MeOn (CM0,CM0-PG)
		Trigger Host OS hibernate ➡ Power Button press
Setup:	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. 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:	4. Hibernate the SUT via the Host OS. 5. Verify that the SUT is in S4,S5,Deep S4,Deep S5,G3/MeOff (CM-Off). 6. Briefly press the Power Button on the SUT. 7. Verify that the SUT is in S0/MeOn (CM0,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*"}	
Pass Criteria:	The test passes if the SUT moves to S4, S5, Deep S4, Deep S5, or G3, and then to S0, and the Intel® ME is in MeOn (CM0, CM0-PG).	

ID:	Check S5	
Title:	S0/CM0 to S5/CM-Off to S0/CM0 via Host OS shutdown cycle (AC-only)	
Requirement:	Optional	
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:	If Deep S5 and/or G3 are 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 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, Deep S5, G3/MeOff (CM-Off)
		Final S0/MeOn (CM0,CM0-PG)
		Trigger Host OS suspend ➡ Power Button press
Setup:	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. 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:	4. Shutdown the SUT via the Host OS. 5. Verify that the SUT is in S5,Deep S5,G3/MeOff (CM-Off). 6. Briefly press the Power Button on the SUT. 7. Verify that the SUT is in S0/MeOn (CM0,CM0-PG).	



ID:	Check S5
Pass Criteria:	The test passes if the SUT moves to S5, Deep S5, or G3, and then to S0, and the Intel® ME 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, DC)		
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:	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, DC
	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
Setup:	1. Set the SUT power source based on Deep Sx policy . 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 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:	4. Request the test operator to confirm the SUT is properly configured to enter Deep S4 upon Host OS hibernate. 5. Hibernate the SUT via the Host OS. 6. Verify that the SUT is in Deep S4/MeOff (CM-Off). 7. Briefly press the Power Button on the SUT. 8. 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® ME 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, DC)		
Requirement:	Optional Non-Support <input checked="" type="checkbox"/> 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:	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, DC
	Power States	Initial	S0/MeOn (CM0,CM0-PG)
		Middle	Deep S5/MeOff (CM-Off)
		Final	S0/MeOn (CM0,CM0-PG)
		Trigger	Host OS suspend ➡ Power Button press
Setup:	1. Set the SUT power source based on Deep Sx policy . 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 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.		



ID:	Check Deep S5
Procedure:	<ol style="list-style-type: none"> Request the test operator to confirm the SUT is properly configured to enter Deep S5 upon Host OS shutdown. Shutdown the SUT via the Host OS. Verify that the SUT is in Deep S5/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 S5 and then to S0, and the Intel® ME is in MeOn (CM0, CM0-PG).

ID:	Check Intel® ME	
Title:	S0/CM0 to S5/CM-Off to S0/CM0 via Host OS suspend cycle (AC-only)	
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:	If Deep S5 and/or G3 are 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 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 suspend ➡ Power Button press
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. 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® ME 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.	
Parameters:	System Power Source	
	AC+DC	
	Power States	Initial S0/MeOn (CM0,CM0-PG)
		Final S0/MeOn (CM0,CM0-PG)
		Trigger AC-detach
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.		
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
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)		
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:	If Deep S5 and/or G3 are 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 or G3 entry.The correct Deep Sx policy is applied to the SUT profile in Intel® PETS.		
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
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 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).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).		
Pass Criteria:	The test passes if the SUT moves to G3, and the Intel® ME moves to MeOff (CM-Off).		

8.3 Intel® ME Power Management 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 and All-in-One 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 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	S3/CM-Off to S0/CM0	Intel® PETS Package: Compliance_Power_G3-S5.xml Compliance_Power_Network_Wake.xml
ME_PM_8	S0/CM0 to S4-S5/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
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_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® ME Power Policy is S0 Only	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
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

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 will include 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_18.1/2, ME_PM_19.1/2, ME_PM_26.5/6, ME_PM_26.13, ME_PM_27.1, ME_PM_46.3 through ME_PM_46.6.



8.4 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)		
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
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.		
Procedure:	<ol style="list-style-type: none">5. Suspend the SUT via the Host OS.6. Verify that the SUT is in S3/MeOff (CM-Off).		
Pass Criteria:	The test passes if the SUT moves to S3 and the Intel® ME 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)		
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.		
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
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 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.		
Procedure:	<ol style="list-style-type: none">4. Suspend the SUT via the Host OS.5. Verify that the SUT is in S3/MeOff (CM-Off).		
Pass Criteria:	The test passes if the SUT moves to S3 and the Intel® ME moves to MeOff (CM-Off).		



8.5 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)	
Requirement:	Mandatory	Exemptions <ul style="list-style-type: none"> <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 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 S3/MeOff (CM-Off)
		Final S0/MeOn (CM0,CM0-PG)
		Trigger Magic Packet receipt
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, 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). Ensure that 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 the second nibble of the FWSTS2 register on the SUT have a value of 0x60xxxxxx. 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 that 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 S3 to S0. the Intel® ME moves to MeOn (CM0, CM0-PG). 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)	
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 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.	



ID:	ME_PM_2.2		
Parameters:	System Power Source		DC-only
	Power States	Initial	S3/MeOff (CM-Off)
		Final	S0/MeOn (CM0,CM0-PG)
		Trigger	Power Button press
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 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. Record the Host OS last boot time on the SUT (to verify successful return from S3). Ensure that 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 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 that 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 S3 to S0. the Intel® ME moves to MeOn (CM0, CM0-PG). 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)		
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
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 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. Record the Host OS last boot time on the SUT (to verify successful return from S3). Ensure that 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). 		



ID:	ME_PM_2.3
Procedure:	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 the second nibble of the FWSTS2 register on the SUT have a value of 0x60xxxxxx. 13. Ensure that 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 S3 to S0. the Intel® ME moves to MeOn (CM0, CM0-PG). the Host OS last boot time has not changed.

ID:	ME_PM_2.7											
Title:	S3/CM-Off to S0/CM0 via magic packet (DC-only)											
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/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 shall be the initial active network interface in the test, and WLAN shall be the secondary network interface.											
Parameters:	<table> <tr> <th colspan="2">System Power Source</th><td>DC-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> </table>	System Power Source		DC-only	Power States	Initial	S3/MeOff (CM-Off)	Final	S0/MeOn (CM0,CM0-PG)	Trigger	Magic Packet receipt	
System Power Source		DC-only										
Power States	Initial	S3/MeOff (CM-Off)										
	Final	S0/MeOn (CM0,CM0-PG)										
	Trigger	Magic Packet receipt										
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. 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. Record the Host OS last boot time on the SUT (to verify successful return from S3). 7. Ensure that yellow bang is not seen on Drivers in Device Manager											
Procedure:	8. Suspend the SUT via the Host OS. 9. Verify that the SUT is in S3/MeOff (CM-Off). 10. Send three magic packets, at 2 second intervals, by means of the active network interface. 11. Verify that the SUT is in S0/MeOn (CM0,CM0-PG). 12. Verify that the Host OS on the SUT is available. 13. Verify the Host OS last boot time on the SUT matches the boot time recorded before entry into S3. 14. Verify that the second nibble of the FWSTS2 register on the SUT have a value of 0x60xxxxxx. 15. Ensure that yellow bang is not seen on Drivers in Device Manager If both LAN and WLAN network interfaces are available, repeat this test procedure with the WLAN interface set as the active network interface.											
Pass Criteria:	The test passes if: <ul style="list-style-type: none"> the SUT moves from S3 to S0. the Intel® ME moves to MeOn (CM0, CM0-PG). the Host OS last boot time has not changed. 											



8.6 ME_PM_8 - S0/CM0 to S4/CM-Off

ID:	ME_PM_8.1		
Title:	S0/CM0 to S4/CM-Off via Host OS hibernate (DC-only)		
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:	If Deep S4, Deep S5, and/or G3 are 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/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	S4, S5, Deep S4, Deep S5, G3/MeOff (CM-Off)
		Trigger	Host OS hibernate
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 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">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® ME 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)		
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:	If Deep S4, Deep S5, and/or G3 are 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/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	S4, S5, Deep S4, Deep S5, G3/MeOff (CM-Off)
		Trigger	Host OS hibernate
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 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">Hibernate the SUT via the Host OS.Verify that the SUT is in S4,S5,Deep S4,Deep S5,G3/MeOff (CM-Off).		



ID:	ME_PM_8.2
Pass Criteria:	The test passes if the SUT moves to S4, S5, Deep S4, Deep S5, or G3, and the Intel® ME moves to MeOff (CM-Off).

ID:	ME_PM_8.3		
Title:	S0/CM0 to S5/CM-Off via Host OS shutdown (DC-only)		
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 Host OS shutdown with the parameters outlined below.		
Configuration:	<p>If Deep S5 and/or G3 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 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	S3/MeOff (CM-Off)
		Trigger	Host OS shutdown
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 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). 		
Pass Criteria:	The test passes if the SUT moves to S5 (or Deep S5 or G3), and the Intel® ME 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)		
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:	<p>If Deep S5 and/or G3 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 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	Host OS shutdown
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 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. 		



ID:	ME_PM_8.4
Procedure:	4. Shutdown the SUT via the Host OS. 5. 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® ME moves to MeOff (CM-Off).

8.7 ME_PM_9 - G3 or S4/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)		
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:	If Deep S4, Deep S5, and/or G3 are 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/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/MeOff (CM-Off)
		Final	S0/MeOn (CM0, CM0-PG)
		Trigger	Power Button press
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 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 that yellow bang is not seen on Drivers in Device ManagerHibernate 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">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 the second nibble of the FWSTS2 register on the SUT have a value of 0x60xxxxxx.Ensure that 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® ME moves to MeOn (CM0, CM0-PG).		

ID:	ME_PM_9.2		
Title:	S4/CM-Off to S0/CM0 via Power Button press (AC+DC, AC-only)		
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.		



ID:	ME_PM_9.2	
Configuration:	If Deep S4, Deep S5, and/or G3 are 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/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
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. 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. 4. Ensure that yellow bang is not seen on Drivers in Device Manager 5. Hibernate the SUT via the Host OS. 6. Verify that the SUT is in S4,S5,Deep S4,Deep S5,G3/MeOff (CM-Off).	
Procedure:	7. Briefly press the Power Button on the SUT. 8. Verify that the SUT is in S0/MeOn (CM0,CM0-PG). 9. Verify that the Host OS on the SUT is available. 10. 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*"} 11. Verify that the second nibble of the FWSTS2 register on the SUT have a value of 0x60xxxxxx. 12. Ensure that 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® ME moves to MeOn (CM0, CM0-PG).	

ID:	ME_PM_9.4	
Title:	S5/CM-Off to S0/CM0 via Power Button press (DC-only)	
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:	If Deep S5 and/or G3 are 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 or G3 entry. The correct Deep Sx policy is applied to the SUT profile in Intel® PETS. Confirm that the Host OS is configured to shutdown the SUT upon Power Button press. 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 S5, Deep S5, G3/MeOff (CM-Off)
		Final S0/MeOn (CM0,CM0-PG)
		Trigger Power Button press



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. 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 that yellow bang is not seen on Drivers in Device Manager 7. Shutdown the SUT via the brief Power Button press. 8. Verify that the SUT is in S5,Deep S5,G3/MeOff (CM-Off).
Procedure:	<ol style="list-style-type: none"> 9. Briefly press the Power Button on the SUT. 10. Verify that the SUT is in S0/MeOn (CM0,CM0-PG). 11. Verify that the Host OS on the SUT is available. 12. Verify that the second nibble of the FWSTS2 register on the SUT have a value of 0x60xxxxxx. 13. Ensure that 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® ME moves to MeOn (CM0).

ID:	ME_PM_9.5		
Title:	S5/CM-Off to S0/CM0 via Power Button press (AC+DC, AC-only)		
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:	If Deep S5 and/or G3 are 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 or G3 entry.The correct Deep Sx policy is applied to the SUT profile in Intel® PETS. Confirm that the Host OS is configured to shutdown the SUT upon Power Button press. 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
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. 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>4. Ensure that yellow bang is not seen on Drivers in Device Manager</div> <div>5. Shutdown the SUT via the brief Power Button press.</div> <div>6. Verify that the SUT is in S5,Deep S5,G3/MeOff (CM-Off).</div>		
Procedure:	<div>7. Briefly press the Power Button on the SUT.</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 the second nibble of the FWSTS2 register on the SUT have a value of 0x60xxxxxx.</div> <div>11. Ensure that yellow bang is not seen on Drivers in Device Manager</div>		
Pass Criteria:	The test passes if the SUT moves from S5 (or Deep S5 or G3) to S0, and the Intel® ME moves to MeOn (CM0, CM0-PG).		

ID:	ME_PM_9.7
Title:	G3/CM-Off to S0/CM0 via AC-attach (AC+DC,AC-only)



ID:	ME_PM_9.7		
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>If Deep S5 and/or G3 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 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:	System Power Source		AC+DC or AC-only
	Power States	Initial	G3/MeOff (CM-Off)
		Final	S0/MeOn (CM0,CM0-PG)
		Trigger	AC-attach
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 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 that yellow bang is not seen on Drivers in Device Manager Shutdown the SUT via the brief Power Button press. Verify that the SUT is in S5,Deep S5,G3/MeOff (CM-Off). 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). 		
Procedure:	<ol style="list-style-type: none"> 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 S0/MeOn (CM0,CM0-PG). Verify that the Host OS on the SUT is available. Verify that the second nibble of the FWSTS2 register on the SUT have a value of 0x60xxxxx. Ensure that yellow bang is not seen on Drivers in Device Manager 		
Pass Criteria:	The test passes if the SUT moves from G3 to S0, and the Intel® ME moves to MeOn (CM0, CM0-PG).		

8.8 ME_PM_10 - S4/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)		
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>If Deep S4, Deep S5, and/or G3 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 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 shall be the initial active network interface in the test, and WLAN shall be 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
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, 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. 4. Ensure that yellow bang is not seen on Drivers in Device Manager 	
Procedure:	<ol style="list-style-type: none"> 5. Hibernate the SUT via the Host OS. 6. Verify that the SUT is in S4,S5,Deep S4,Deep S5,G3/MeOff (CM-Off). 7. Send three magic packets, at 2 second intervals, by means of the active network interface. 8. Verify that the SUT is in S0/MeOn (CM0,CM0-PG). 9. Verify that the Host OS on the SUT is available. 10. 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*"} 11. Verify that the second nibble of the FWSTS2 register on the SUT have a value of 0x60xxxxxx. 12. Ensure that 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 the SUT moves from S4, S5, Deep S4, Deep S5, or G3 to S0, and the Intel® ME moves to MeOn (CM0, CM0-PG).	

ID:	ME_PM_10.5	
Title:	S5/CM-Off to S0/CM0 via magic packet (AC+DC,AC-only)	
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>If Deep S4, Deep S5, and/or G3 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 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 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 S5, Deep S5, G3/MeOff (CM-Off)
		Final S0/MeOn (CM0,CM0-PG)
		Trigger Magic Packet receipt
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, 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. 4. Ensure that yellow bang is not seen on Drivers in Device Manager 	



ID:	ME_PM_10.5
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). 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 the second nibble of the FWSTS2 register on the SUT have a value of 0x60xxxxxx. Ensure that 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 the SUT moves from S5 (or Deep S5 or G3) to S0, and the Intel® ME moves to MeOn (CM0, CM0-PG).

ID:	ME_PM_10.6		
Title:	S5/CM-Off to S0/CM0 via Power Button press (AC+DC,AC-only)		
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:	If Deep S5 and/or G3 are 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 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
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 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 that 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/MeOn (CM0,CM0-PG).Verify that the Host OS on the SUT is available.Verify that the second nibble of the FWSTS2 register on the SUT have a value of 0x60xxxxx.Ensure that 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® ME moves to MeOn (CM0, CM0-PG).		

ID:	ME_PM_10.9
Title:	S4/CM-Off to S0/CM0 via magic packet (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 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_10.9	
Configuration:	<p>If Deep S4, Deep S5, and/or G3 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 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 shall be the initial active network interface in the test, and WLAN shall be the secondary network interface.</p>	
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 Magic Packet receipt
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, 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 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 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 that 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 the SUT moves from S4, S5, Deep S4, Deep S5, or G3 to S0, and the Intel® ME moves to MeOn (CM0, CM0-PG).	

ID:	ME_PM_10.11	
Title:	S5/CM-Off to S0/CM0 via magic packet (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 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>If Deep S5 and/or G3 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 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 shall be the initial active network interface in the test, and WLAN shall be the secondary network interface.</p>	
Parameters:	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



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. 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 yellow bang is not seen on Drivers in Device Manager
Procedure:	<ol style="list-style-type: none"> 7. Shutdown the SUT via the Host OS. 8. Verify that the SUT is in S5,Deep S5,G3/MeOff (CM-Off). 9. Send three magic packets, at 2 second intervals, by means of the active network interface. 10. Verify that the SUT is in S0/MeOn (CM0,CM0-PG). 11. Verify that the Host OS on the SUT is available. 12. Verify that the second nibble of the FWSTS2 register on the SUT have a value of 0x60xxxxx. 13. Ensure that 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 the SUT moves from S5 (or Deep S5 or G3) to S0, and the Intel® ME moves to MeOn (CM0, CM0-PG).

8.9 ME_PM_17 - Cold Reset

ID:	ME_PM_17.6		
Title:	S0/CM0 to S0/CM0 via CF9 Cold Reset (AC+DC,AC-only)		
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:	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
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. Record the Host OS last boot time on the SUT (to verify reset execution). 4. Ensure that yellow bang is not seen on Drivers in Device Manager 		
Procedure:	<ol style="list-style-type: none"> 5. Ensure that CF9h Global Reset (CF9GR) is cleared to 0b. 6. Perform a cold reset of the SUT by writing Eh to I/O register CF9h. 7. Verify that the SUT is in S0/MeOn (CM0,CM0-PG). 8. 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. 9. Ensure that 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® ME is available in MeOn (CM0, CM0-PG). • the Host OS last boot time does not match, or the Host OS is unavailable. 		



8.10 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)		
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® 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
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.Record the Host OS last boot time on the SUT (to verify reset execution).Verify that the Intel® ME is configured in manufacturing mode.Ensure that yellow bang is not seen on Drivers in Device ManagerWrite 1b to CF9GR 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/MeOn (CM0,CM0-PG).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.Ensure that 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® ME is available in MeOn (CM0, CM0-PG).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)		
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® 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



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. Record the Host OS last boot time on the SUT (to verify reset execution). 4. Verify that the Intel® ME is configured in manufacturing mode. 5. Ensure that yellow bang is not seen on Drivers in Device Manager 6. Write 1b to CF9GR to enable Global Reset
Procedure:	<ol style="list-style-type: none"> 7. Ensure that CF9h Global Reset (CF9GR) is set to 1b to enable global reset. 8. Perform a global reset of the SUT by writing either 6h or Eh to I/O register CF9h. 9. Verify that the SUT is in S0/MeOn (CM0,CM0-PG). 10. 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. 11. Ensure that 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® ME is available in MeOn (CM0, CM0-PG). • the Host OS last boot time does not match, or the Host OS is unavailable.

8.11 ME_PM_19 - Straight-to-S5, Intel® CSME Power Policy is S0 Only

ID:	ME_PM_19.1		
Title:	S0/CM0 to S5/CM-Off via Power Button override (DC-only)		
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>If Deep S5 and/or G3 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 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
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 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"> 6. Shutdown the SUT via a Power Button press for more than 5 seconds. 7. 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® ME 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)		
Requirement:	Mandatory	Exemptions	None



ID:	ME_PM_19.2		
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:	If Deep S5 and/or G3 are 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 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	Power Button override
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. 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:	4. Shutdown the SUT via a Power Button press for more than 5 seconds . 5. 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® ME moves to MeOff (CM-Off).		

ID:	ME_PM_19.3		
Title:	S3/CM-Off to S5/CM-Off via Power Button override (DC-only)		
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:	If Deep S5, and/or G3 are supported on the SUT, confirm the following: <ul style="list-style-type: none"> The SUT and/or BIOS are properly configured to permit 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	S3/MeOff (CM-Off)
		Final	S5, Deep S5, G3/MeOff (CM-Off)
		Trigger	Power Button override
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. 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. Suspend the SUT via the Host OS. 7. Verify that the SUT is in S3/MeOff (CM-Off).		
Procedure:	8. Shutdown the SUT via a Power Button press for more than 5 seconds . 9. Verify that the SUT is in S5,Deep S5,G3/MeOff (CM-Off).		



ID:	ME_PM_19.3
Pass Criteria:	The test passes if the SUT moves to S5 (or Deep S5 or G3), and the Intel® ME 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)		
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:	<p>If Deep S5, and/or G3 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 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	S3/MeOff (CM-Off)
		Final	S5, Deep S5, G3/MeOff (CM-Off)
		Trigger	Power Button override
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 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. 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® ME 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)		
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>If Deep S4, Deep S5, and/or G3 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 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



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. 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. Hibernate the SUT via the Host OS. 7. Verify that the SUT is in S4,S5,Deep S4,Deep S5,G3/MeOff (CM-Off).
Procedure:	<ol style="list-style-type: none"> 8. Shutdown the SUT via a Power Button press for more than 5 seconds. 9. 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® ME 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)		
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:	If Deep S4, Deep S5, and/or G3 are 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/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	S5, Deep S5, G3/MeOff (CM-Off)
		Trigger	Power Button override
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. 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. 4. Hibernate the SUT via the Host OS. 5. Verify that the SUT is in S4,S5,Deep S4,Deep S5,G3/MeOff (CM-Off).		
Procedure:	6. Shutdown the SUT via a Power Button press for more than 5 seconds . 7. Verify that the SUT is in S5,Deep S5,G3/MeOff (CM-Off).		
Pass Criteria:	The test passes if the SUT moves to, if not already there, S5 (or Deep S5 or G3), and the Intel® ME 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_19.7
Title:	S5/CM-Off to S5/CM-Off via Power Button override (DC-only)
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.



ID:	ME_PM_19.7	
Configuration:	If Deep S5 and/or G3 are 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 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 S5, Deep S5, G3/MeOff (CM-Off)
		Final S5, Deep S5, G3/MeOff (CM-Off)
		Trigger Power Button override
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. 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. Shutdown the SUT via the Host OS. 7. Verify that the SUT is in S5,Deep S5,G3/MeOff (CM-Off).	
Procedure:	8. Shutdown the SUT via a Power Button press for more than 5 seconds . 9. Verify that the SUT is in S5,Deep S5,G3/MeOff (CM-Off).	
Pass Criteria:	The test passes if the SUT ends the test in S5 (or Deep S5 or G3), and the Intel® ME is in MeOff (CM-Off). Note: that some systems may briefly move electrically to S0 before final transition to S5 (or Deep S5 or G3).	

ID:	ME_PM_19.8	
Title:	S5/CM-Off to S5/CM-Off via Power Button override (AC+DC,AC-only)	
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:	If Deep S5 and/or G3 are 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 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 S5, Deep S5, G3/MeOff (CM-Off)
		Trigger Power Button override
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. 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. 4. Shutdown the SUT via the Host OS. 5. Verify that the SUT is in S5,Deep S5,G3/MeOff (CM-Off).	
Procedure:	6. Shutdown the SUT via a Power Button press for more than 5 seconds . 7. Verify that the SUT is in S5,Deep S5,G3/MeOff (CM-Off).	
Pass Criteria:	The test passes if the SUT ends the test in S5 (or Deep S5 or G3), and the Intel® ME is in MeOff (CM-Off). Note: Some systems may briefly move electrically to S0 before final transition to S5 (or Deep S5 or G3).	



8.12 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

ID:	ME_PM_25.1		
Title:	S4/CM-Off to S0/CM0 via magic packet (DC-only)		
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.		
Configuration:	If Deep S4, Deep S5, and/or G3 are 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/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. 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		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
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, 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 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 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 that 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 the SUT moves from S4, S5, Deep S4, Deep S5, or G3 to S0, and the Intel® ME moves to MeOn (CM0).		
ID:	ME_PM_25.2		
Title:	S5/CM-Off to S0/CM0 via magic packet (DC-only)		



ID:	ME_PM_25.2	
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 S5/CM-Off to S0/CM0 via magic packet with the parameters outlined below.	
Configuration:	<p>If Deep S5 and/or G3 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 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 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 S5, Deep S5, G3/MeOff (CM-Off)
		Final S0/MeOn (CM0,CM0-PG)
		Trigger Magic Packet receipt
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, 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 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 the second nibble of the FWSTS2 register on the SUT have a value of 0x60xxxxxx. Ensure that 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 the SUT moves from S5, (or Deep S5 or G3) to S0, and the Intel® ME moves to MeOn (CM0).	

ID:	ME_PM_25.3	
Title:	G3/CM-Off to S0/CM0 via magic packet (DC-only)	
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 G3/CM-Off to S0/CM0 via magic packet with the parameters outlined below.	



ID:	ME_PM_25.3		
Configuration:	<p>If Deep S5 and/or G3 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 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 shall be the initial active network interface in the test, and WLAN shall be the secondary network interface.</p>		
Parameters:	System Power Source		DC-only
	Power States	Initial	G3/MeOff (CM-Off)
		Final	S0/MeOn (CM0,CM0-PG)
		Trigger	Magic Packet receipt
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, 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 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). 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,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 the second nibble of the FWSTS2 register on the SUT have a value of 0x60xxxxxx. Ensure that 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 the SUT moves from S5, (or Deep S5 or G3) to S0, and the Intel® ME moves to MeOn (CM0).		

8.13 ME_PM_26 - Warm Reset

ID:	ME_PM_26.5		
Title:	S0/CM0 to S0/CM0 via Reset Button press (or logic) (DC-only)		
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:	This test assumes that either LAN-only, WLAN-only, or both LAN and WLAN network interfaces are available on the SUT.		



ID:	ME_PM_26.5		
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)
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 yellow bang is not seen on Drivers in Device Manager 		
Procedure:	<ol style="list-style-type: none"> 6. 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. 7. Verify that the SUT is in S0/MeOn (CM0,CM0-PG). 8. Verify that the second nibble of the FWSTS2 register on the SUT have a value of 0x6xxxxx. 9. Ensure that 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® ME is available in MeOn (CM0, CM0-PG).		

ID:	ME_PM_26.6		
Title:	S0/CM0 to S0/CM0 via Reset Button press (or logic) (AC+DC,AC-only)		
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:	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)
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 yellow bang is not seen on Drivers in Device Manager 		
Procedure:	<ol style="list-style-type: none"> 4. 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. 5. Verify that the SUT is in S0/MeOn (CM0,CM0-PG). 6. Verify that the second nibble of the FWSTS2 register on the SUT have a value of 0x6xxxxx. 7. Ensure that 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® ME is available in MeOn (CM0, CM0-PG).		

ID:	ME_PM_26.9		
Title:	S0/CM0 to S0/CM0 via Host OS restart (DC-only)		
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:	This test assumes that either LAN-only, WLAN-only, or both LAN and WLAN network interfaces are available on the SUT.		



ID:	ME_PM_26.9		
Parameters:	System Power Source		DC-only
	Power States	Initial	S0/MeOn (CM0,CM0-PG)
		Final	S0/MeOn (CM0,CM0-PG)
		Trigger	Host OS restart
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 yellow bang is not seen on Drivers in Device Manager 		
Procedure:	<ol style="list-style-type: none"> 6. Perform a warm reset of the SUT via Host OS graceful restart. 7. Verify that the SUT is in S0/MeOn (CM0,CM0-PG). 8. Verify that the second nibble of the FWSTS2 register on the SUT have a value of 0x6xxxxxx. 9. Ensure that 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® ME is available in MeOn (CM0, CM0-PG).		

ID:	ME_PM_26.10		
Title:	S0/CM0 to S0/CM0 via Host OS restart (AC+DC,AC-only)		
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:	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
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 yellow bang is not seen on Drivers in Device Manager 		
Procedure:	<ol style="list-style-type: none"> 4. Perform a warm reset of the SUT via Host OS graceful restart. 5. Verify that the SUT is in S0/MeOn (CM0,CM0-PG). 6. Verify that the second nibble of the FWSTS2 register on the SUT have a value of 0x6xxxxxx. 7. Ensure that 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® ME is available in MeOn (CM0, CM0-PG).		

ID:	ME_PM_26.13		
Title:	S0/CM0 to S0/CM0 via CF9 Warm Reset (AC+DC,AC-only)		
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:	This test assumes that either LAN-only, WLAN-only, or both LAN and WLAN network interfaces are available on the SUT.		



ID:	ME_PM_26.13		
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
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. Record the Host OS last boot time on the SUT (to verify reset execution). 4. Ensure that yellow bang is not seen on Drivers in Device Manager		
Procedure:	5. Ensure that CF9h Global Reset (CF9GR) is cleared to 0b . 6. Perform a warm reset of the SUT by writing 6h to I/O register CF9h. 7. Verify that the SUT is in S0/MeOn (CM0,CM0-PG). 8. 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. 9. Ensure that 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® ME is available in MeOn (CM0, CM0-PG). the Host OS last boot time does not match, or the Host OS is unavailable. 		

8.14 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)		
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:	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
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.		
Procedure:	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 from S0 to G3, and the Intel® ME moves to MeOff (CM-Off).		

8.15 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)		



ID:	ME_PM_44.3		
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:	If Deep S4, Deep S5, and/or G3 are 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/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-PG)
		Final	S4, S5, Deep S4, Deep S5, G3/MeOff (CM-Off)
		Trigger	Host OS hibernate
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. Ensure that the Host OS is configured to not sleep on either AC or DC power. 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 the Host OS on the SUT is available. 8. Check for 3 minutes to check Intel® ME is in CM0-PG state for more than 50% of the time. 9. Verify that the SUT is in S0/MeOn (CM0-PG).		
Procedure:	10. Hibernate the SUT via the Host OS. 11. 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® ME 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:	If Deep S4, Deep S5, and/or G3 are 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/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-PG)
		Final	S4, S5, Deep S4, Deep S5, G3/MeOff (CM-Off)
		Trigger	Host OS hibernate



ID:	ME_PM_44.4
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 the Host OS is configured to not sleep on either AC (or DC, where available) power source configuration. 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. 5. Verify that the Host OS on the SUT is available. 6. Check for 3 minutes to check Intel® ME is in CM0-PG state for more than 50% of the time 7. Verify that the SUT is in S0/MeOn (CM0-PG).
Procedure:	<ol style="list-style-type: none"> 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).
Pass Criteria:	The test passes if the SUT moves to S4, S5, Deep S4, Deep S5, or G3, and the Intel® ME 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	<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 S5/CM-Off via Host OS shutdown with the parameters outlined below.		
Configuration:	If Deep S5 and/or G3 are 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 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-PG)
		Final	S5, Deep S5, G3/MeOff (CM-Off)
		Trigger	Host OS shutdown
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 the Host OS is configured to not sleep on either AC or DC power.</div> <div>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.</div> <div>7. Verify that the Host OS on the SUT is available.</div> <div>8. Check for 3 minutes to check Intel® ME is in CM0-PG state for more than 50% of the time</div> <div>9. Verify that the SUT is in S0/MeOn (CM0-PG).</div>		
Procedure:	<div>10. Shutdown the SUT via the Host OS.</div> <div>11. 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® ME 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	<div><input checked="" type="checkbox"/> Systems with a LAN-only network interface</div>
Method:	Automated by Intel® PETS with potential Test Operator interaction.		



ID:	ME_PM_44.6		
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:	If Deep S5 and/or G3 are 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 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-PG)
		Final	S5, Deep S5, G3/MeOff (CM-Off)
		Trigger	Host OS shutdown
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 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.Check for 3 minutes to check Intel® ME is in CM0-PG state for more than 50% of the timeVerify 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).		
Pass Criteria:	The test passes if the SUT moves to S5 (or Deep S5 or G3), and the Intel® ME moves to MeOff (CM-Off).		

8.16 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	<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:	If Deep S4, Deep S5, and/or G3 are 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/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/MeOff (CM-Off)
		Final	S0/MeOn (CM0-PG)
		Trigger	Power Button press



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 the Host OS is configured to not sleep on either AC or DC power. 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 the Host OS on the SUT is available. 8. Ensure that 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,Deep S4,Deep S5,G3/MeOff (CM-Off).
Procedure:	<ol style="list-style-type: none"> 11. Briefly press the Power Button on the SUT. 12. Verify that the SUT is in S0. 13. Verify that the Host OS on the SUT is available. 14. Check for 3 minutes to check Intel® ME is in CM0-PG state for more than 50% of the time 15. Verify that the SUT is in S0/MeOn (CM0-PG). 16. 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*"} 17. Ensure that 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® ME 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	<div><input checked="" type="checkbox"/> Systems without WoL and/or WoWLAN support</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 S4/CM-Off to S0/CM0-PG via magic packet with the parameters outlined below.		
Configuration:	If Deep S4, Deep S5, and/or G3 are 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/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. 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	S4, S5, Deep S4, Deep S5, G3/MeOff (CM-Off)
		Final	S0/MeOn (CM0-PG)
		Trigger	Magic Packet receipt
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. Ensure that the Host OS is configured to not sleep on either AC (or DC, where available) power source configuration.</div> <div>4. 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>5. Verify that the Host OS on the SUT is available.</div> <div>6. Ensure that yellow bang is not seen on Drivers in Device Manager</div>		



ID:	ME_PM_45.4
Procedure:	<ol style="list-style-type: none"> 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). 9. Send three magic packets, at 2 second intervals, by means of the active network interface. 10. Verify that the SUT is in S0. 11. Verify that the Host OS on the SUT is available. 12. Check for 3 minutes to check Intel® ME is in CM0-PG state for more than 50% of the time 13. Verify that the SUT is in S0/MeOn (CM0-PG). 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*"} 15. Ensure that 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 the SUT moves from S4, S5, Deep S4, Deep S5, or G3 to S0, and the Intel® ME 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:	If Deep S5 and/or G3 are 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 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	S5, Deep S5, G3/MeOff (CM-Off)
		Final	S0/MeOn (CM0-PG)
		Trigger	Power Button press
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 the Host OS is configured to not sleep on either AC or DC power. 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 the Host OS on the SUT is available. 8. Ensure that 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,Deep S5,G3/MeOff (CM-Off). 		
Procedure:	<ol style="list-style-type: none"> 11. Briefly press the Power Button on the SUT. 12. Verify that the SUT is in S0. 13. Verify that the Host OS on the SUT is available. 14. Check for 3 minutes to check Intel® ME is in CM0-PG state for more than 50% of the time 15. Verify that the SUT is in S0/MeOn (CM0-PG). 16. Ensure that 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® ME 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.		
Configuration:	If Deep S5 and/or G3 are 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 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	G3/MeOff (CM-Off)
		Final	S0/MeOn (CM0-PG)
		Trigger	(DC-attach then) Power Button press
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. Ensure that the Host OS is configured to not sleep on either AC or DC power. 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 the Host OS on the SUT is available. 8. Ensure that 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,Deep S5,G3/MeOff (CM-Off). 11. Remove power from the SUT 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).		
Procedure:	13. Set the SUT power source to DC-only. 14. Briefly press the Power Button on the SUT. 15. Verify that the SUT is in S0. 16. Verify that the Host OS on the SUT is available. 17. Check for 3 minutes to check Intel® ME is in CM0-PG state for more than 50% of the time 18. Verify that the SUT is in S0/MeOn (CM0-PG). 19. Ensure that 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® ME moves to MeOn (CM0-PG).		



8.17 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	<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 Host OS restart 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-PG)
		Final	S0/MeOn (CM0-PG)
		Trigger	Host OS restart
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 the Host OS is configured to not sleep on either AC or DC power.</div> <div>6. Verify that the Host OS on the SUT is available.</div> <div>7. Ensure that yellow bang is not seen on Drivers in Device Manager</div> <div>8. Check for 3 minutes to check Intel® ME is in CM0-PG state for more than 50% of the time</div> <div>9. Verify that the SUT is in S0/MeOn (CM0-PG).</div>		
Procedure:	<div>10. Perform a warm reset of the SUT via Host OS graceful restart.</div> <div>11. Verify that the SUT is in S0.</div> <div>12. Verify that the Host OS on the SUT is available.</div> <div>13. Check for 3 minutes to check Intel® ME is in CM0-PG state for more than 50% of the time</div> <div>14. Verify that the SUT is in S0/MeOn (CM0-PG).</div> <div>15. Ensure that yellow bang is not seen on Drivers in Device Manager</div>		
Pass Criteria:	The test passes if the SUT is reset to S0, and the Intel® ME 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:	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-PG)
		Final	S0/MeOn (CM0-PG)
		Trigger	Host OS restart



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 the Host OS is configured to not sleep on either AC (or DC, where available) power source configuration. 4. Verify that the Host OS on the SUT is available. 5. Ensure that yellow bang is not seen on Drivers in Device Manager 6. Check for 3 minutes to check Intel® ME is in CM0-PG state for more than 50% of the time 7. Verify that the SUT is in S0/MeOn (CM0-PG).
Procedure:	<ol style="list-style-type: none"> 8. Perform a warm reset of the SUT via Host OS graceful restart. 9. Verify that the SUT is in S0. 10. Verify that the Host OS on the SUT is available. 11. Check for 3 minutes to check Intel® ME is in CM0-PG state for more than 50% of the time 12. Verify that the SUT is in S0/MeOn (CM0-PG). 13. Ensure that 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® ME 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:	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-PG)
		Final	S0/MeOn (CM0-PG)
		Trigger	CF9 Cold Reset
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 the Host OS is configured to not sleep on either AC or DC power.</div> <div>6. Verify that the Host OS on the SUT is available.</div> <div>7. Record the Host OS last boot time on the SUT (to verify reset execution).</div> <div>8. Ensure that yellow bang is not seen on Drivers in Device Manager</div> <div>9. Check for 3 minutes to check Intel® ME is in CM0-PG state for more than 50% of the time</div> <div>10. Verify that the SUT is in S0/MeOn (CM0-PG).</div>		
Procedure:	<div>11. Ensure that CF9h Global Reset (CF9GR) is cleared to 0b.</div> <div>12. Perform a cold reset of the SUT by writing Eh to I/O register CF9h.</div> <div>13. Verify that the SUT is in S0.</div> <div>14. Verify that the Host OS on the SUT is available.</div> <div>15. Verify the Host OS last boot time on the SUT does not match the boot time recorded before reset.</div> <div>16. Check for 3 minutes to check Intel® ME is in CM0-PG state for more than 50% of the time</div> <div>17. Verify that the SUT is in S0/MeOn (CM0-PG).</div> <div>18. Ensure that yellow bang is not seen on Drivers in Device Manager</div>		



ID:	ME_PM_46.3
Pass Criteria:	<p>The test passes if:</p> <ul style="list-style-type: none"> the SUT is reset to S0. and the Intel® ME 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:	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-PG)
		Final	S0/MeOn (CM0-PG)
		Trigger	CF9 Cold Reset
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 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). Ensure that yellow bang is not seen on Drivers in Device Manager Check for 3 minutes to check Intel® ME is in CM0-PG state for more than 50% of the time Verify that the SUT is in S0/MeOn (CM0-PG). 		
Procedure:	<ol style="list-style-type: none"> Ensure that CF9h Global Reset (CF9GR) is cleared to 0b. Perform a cold reset of the SUT by writing 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 for 3 minutes to check Intel® ME is in CM0-PG state for more than 50% of the time Verify that the SUT is in S0/MeOn (CM0-PG). Ensure that 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® ME 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	<input checked="" type="checkbox"/> Non-Mobile (AC-only) systems
			<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.		



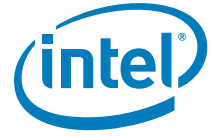
ID:	ME_PM_46.5	
Configuration:	Intel® ME should be configured in manufacturing mode. Confirm that the BIOS has not set the CF9 Lockdown. This test assumes that either LAN-only, WLAN-only, or both LAN and WLAN network interfaces are available on the SUT.	
Parameters:	System Power Source	DC-only
	Power States	Initial S0/MeOn (CM0-PG)
		Final S0/MeOn (CM0-PG)
		Trigger CF9 Global Reset
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 the Host OS is configured to not sleep on either AC or DC power. 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. Ensure that yellow bang is not seen on Drivers in Device Manager Check for 3 minutes to check Intel® ME is in CM0-PG state for more than 50% of the time Verify that the SUT is in S0/MeOn (CM0-PG). Write 1b to CF9GR 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 for 3 minutes to check Intel® ME is in CM0-PG state for more than 50% of the time Verify that the SUT is in S0/MeOn (CM0-PG). Ensure that 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. and the Intel® ME 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 <ul style="list-style-type: none"> <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:	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-PG)
		Final S0/MeOn (CM0-PG)
		Trigger CF9 Global Reset



ID:	ME_PM_46.6
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. Ensure that the Host OS is configured to not sleep on either AC (or DC, where available) power source configuration.4. Verify that the Host OS on the SUT is available.5. Record the Host OS last boot time on the SUT (to verify reset execution).6. Verify that the Intel® ME is configured in manufacturing mode.7. Ensure that yellow bang is not seen on Drivers in Device Manager8. Check for 3 minutes to check Intel® ME is in CM0-PG state for more than 50% of the time9. Verify that the SUT is in S0/MeOn (CM0-PG).10. Write 1b to CF9GR to enable Global Reset
Procedure:	<ol style="list-style-type: none">11. Ensure that CF9h Global Reset (CF9GR) is set to 1b to enable global reset.12. Perform a global reset of the SUT by writing either 6h or Eh to I/O register CF9h.13. Verify that the SUT is in S0.14. Verify that the Host OS on the SUT is available.15. Verify the Host OS last boot time on the SUT does not match the boot time recorded before reset.16. Check for 3 minutes to check Intel® ME is in CM0-PG state for more than 50% of the time17. Verify that the SUT is in S0/MeOn (CM0-PG).18. Ensure that 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® ME is available in MeOn (CM0-PG).• the Host OS last boot time does not match.

§ §



(This page intentionally left blank.)



9 Intel® Management Engine (Intel® ME) Power Management for Consumer Designs—Stress Testing

This chapter covers system power flow transitions which involve the Intel® ME firmware (and/or software). The tests in this chapter are specifically intended to cover topics related to stress testing of the System Under Test (SUT).

9.1 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. See the main Power Management chapter for further details on Deep Sx and Intel® ME Power Gating.

9.2 Test Environment and System Configuration

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

Because of the nature of the stress test and the flows that are 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 networking interface used by the test is documented in the test configuration section. '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, e.g. 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.

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

9.2.1 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 9-1. Two-State with Single 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



Example 9-2.Three-State with Double 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

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.

9.2.2 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 to 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.

9.2.3 Test Environment Setup

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, 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, See 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.

9.2.4 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 be run individually through 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 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.

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.

9.2.5 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.



9.3 Intel® ME Power Management Stress 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. See the test Requirement section for details on test applicability.

Form Factor:

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

System Power Model:

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

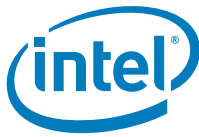
Methodology:

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

Test ID	Test Case Title	SUT Boot Target
PM_ST_31	Host Reset from S0/CM0 (DOS/UEFI)	DOS or UEFI Shell
PM_ST_32	S0/CM0 to S5/CM-Off to S0/CM0 via Power Button Override (DOS/UEFI)	DOS or UEFI Shell
PM_ST_33	S0/CM0 to S3/CM-Off to S0/CM0 via Suspend and Power Button press	Microsoft* Windows*
PM_ST_34	S0/CM0 to S4/CM-Off to S0/CM0 via Hibernate and WoL/WoWLAN	Microsoft* Windows*
PM_ST_35	S0/CM0 to S5/CM-Off to S0/CM0 via Shutdown and Power Button press	Microsoft* Windows*

9.4 PM_ST_31 - Host Reset from S0/CM0 (DOS/UEFI)

ID:	PM_ST_31		
Title:	Host Reset from S0/CM0 (AC+DC,AC-only)		
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:	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)
		Final	S0/MeOn (CM0,CM0-PG)
		Trigger	Reset Button press (or logic)
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).		



ID:	PM_ST_31
Procedure:	<ol style="list-style-type: none">Wait 5 seconds before proceeding to allow for power state stabilization.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). <p>Repeat this procedure for the remaining number of cycles desired in the stress test.</p>
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. Suggested Iterations: Mobile: >=2000, Desktop/AIO >=750

9.5 PM_ST_32 - S0/CM0 to S5/CM-OFF to S0/CM0 via Power Button Override (DOS/UEFI)

ID:	PM_ST_32		
Title:	S0/CM0 to S5/CM-Off to S0/CM0 via Power Button override cycle (AC+DC,AC-only)		
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 Power Button override cycle with the parameters outlined below.		
Configuration:	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,Deep S5/MeOff (CM-Off)
		Final	S0/MeOn (CM0,CM0-PG)
		Trigger	Power Button override → Power Button press
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).		
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/MeOff (CM-Off).Briefly press the Power Button on the SUT.Verify that the SUT is in S0/MeOn (CM0,CM0-PG). <p>Repeat this procedure for the remaining number of cycles desired in the stress test.</p>		
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. Suggested Iterations: Mobile: >=2000, Desktop/AIO: >=750		

9.6 PM_ST_33 - S0/CM0 to S3/CM-Off to S0/CM0 via Suspend and Power Button Press

ID:	PM_ST_33		
Title:	S0/CM0 to S3/CM-Off to S0/CM0 via Host OS suspend/Power Button press cycle (AC+DC,AC-only)		
Requirement:	Mandatory	Exemptions	<input checked="" type="checkbox"/> Microsoft Windows* InstantGo* systems
Method:	Automated by Intel® PETS		



ID:	PM_ST_33		
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:	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 ➡ Remote Power Up
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. 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 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). 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 second nibble of the FWSTS2 register on the SUT have a value of 0x60xxxxxx. Ensure that yellow bang is not seen on Drivers in Device Manager <p>Repeat this procedure for the remaining number of cycles desired in the stress test.</p>		
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. Suggested Iterations: Mobile: >=2000, Desktop/AIO: >=750		

9.7 PM_ST_34 - S0/CM0 to S4/CM-Off to S0/CM0 via Hibernate and WoL/WoWLAN

ID:	PM_ST_34		
Title:	S0/CM0 to S4/CM-Off to S0/CM0 via Host OS hibernate/magic packet cycle (AC+DC,AC-only)		
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 S0/CM0 to S4/CM-Off to S0/CM0 via Host OS hibernate and magic packet cycle with the parameters outlined below.		
Configuration:	If Deep S4 and/or Deep S5 are 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/S5 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. 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	S4,S5,Deep S4,Deep S5/MeOff (CM-Off)
		Final	S0/MeOn (CM0,CM0-PG)
		Trigger	Host OS hibernate ➡ Magic Packet receipt



ID:	PM_ST_34
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, 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.4. Ensure that yellow bang is not seen on Drivers in Device Manager
Procedure:	<ol style="list-style-type: none">5. Hibernate the SUT via the Host OS.6. Verify that the SUT is in S4,S5,Deep S4,Deep S5/MeOff (CM-Off).7. Send three magic packets, at 2 second intervals, by means of the active network interface.8. Verify that the SUT is in S0/MeOn (CM0,CM0-PG).9. Verify that the Host OS on the SUT is available.10. Verify the second nibble of the FWSTS2 register on the SUT have a value of 0x60xxxxxx.11. 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. If available, set the active network interface to WLAN (from LAN) to run the following:<ol style="list-style-type: none">a. Hibernate the SUT via the Host OS.b. Verify that the SUT is in S4,S5,Deep S4,Deep S5/MeOff (CM-Off).c. Send three magic packets, at 2 second intervals, by means of the WLAN network interface.d. Verify that the SUT is in S0/MeOn (CM0,CM0-PG).e. Verify that the Host OS on the SUT is available.f. Verify the second nibble of the FWSTS2 register on the SUT have a value of 0x60xxxxxx. and 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*"}"13. Ensure that yellow bang is not seen on Drivers in Device Manager <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: >=750</p>

9.8 PM_ST_35 - S0/CM0 to S5/CM-Off to S0/CM0 via Shutdown and Power Button Press

ID:	PM_ST_35
Title:	S0/CM0 to S5/CM-Off to S0/CM0 via Host OS shutdown/Power Button press cycle (AC+DC,AC-only)
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>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>



ID:	PM_ST_35		
Parameters:	System Power Source		AC+DC or AC-only
	Power States	Initial	S0/MeOn (CM0,CM0-PG)
		Middle	S5,Deep S5/MeOff (CM-Off)
		Final	S0/MeOn (CM0,CM0-PG)
		Trigger	Host OS shutdown ➡ Power Button press
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 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. 4. Ensure that yellow bang is not seen on Drivers in Device Manager 		
Procedure:	<ol style="list-style-type: none"> 5. Shutdown the SUT via the Host OS. 6. Verify that the SUT is in S5,Deep S5/MeOff (CM-Off). 7. Briefly press the Power Button on the SUT. 8. Verify that the SUT is in S0/MeOn (CM0,CM0-PG). 9. Verify that the Host OS on the SUT is available. 10. Verify the second nibble of the FWSTS2 register on the SUT have a value of 0x60xxxxxx. 11. Ensure that yellow bang is not seen on Drivers in Device Manager <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: >=750</p>		

§ §



(This page intentionally left blank.)



10 Intel® Dynamic Application Loader (Intel® DAL)

10.1 Introduction

Intel® Dynamic Application Loader (Intel® DAL) is an Intel® CSME infrastructure for applications.

The table below documents the compliancy tests to verify that the Intel® Dynamic Application Loader is working on the platform.

This Test plan is targeted to all OEMs.

10.2 Test Environment for the Intel® Dynamic Application Loader (Intel® DAL)

Note: No OEM implementation is required on the board/BIOS or EC level. Intel® CSME should be set to Enabled in FITC 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.

10.2.1 Tools for Testing

Intel® Platform Enablement Test Suite—Latest version of the tool from the Intel® CSME Compliancy kit release. Refer to 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.

Package Compliance_DAL.xml should be loaded to Intel® PETS in order to compete the tests in this section.

10.2.2 Verify Needed Software is Installed on the Host

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).



10.3 Intel® Dynamic Application Loader (Intel® DAL) Test Coverage Summary

Table 10-1. Compliancy Tests for Verifying that the Intel® Dynamic Application Loader is Working

Test ID	Test Case Title	PETS/Manual	Form Factor ¹	Network Factor
DAL_001	Intel® DAL applications cleanup	PETS		LAN+WLAN, WLAN only
DAL_002	Intel® DAL test application installation and load	PETS		LAN+WLAN, WLAN only
DAL_003	Intel® DAL communication channel exercise	PETS		LAN+WLAN, WLAN only

Notes:

1. Form Factor is grayed out as DAL is present both in consumer and corporate Ice Lake SKUs
2. OS: Test will run on Microsoft® Windows® 7/8.x/10 only

Test ID	DAL_001
Test Case Title:	Intel® DAL applications cleanup
Mandatory/Optional:	Mandatory
Firmware SKU:	Consumer and Corporate SKUs (Desktop, Mobile, and Intel® Ultrabook™)
Description:	Intel® DAL applications cleanup mechanism test
Objective:	To test that the Intel® Dynamic Application Loader cleanup 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 will perform the following steps:</p> <ol style="list-style-type: none">1. Confirm the Intel® Dynamic Application Loader is enabled in Firmware.2. Confirm needed Host software components are available (Intel® MEI driver and Intel® Dynamic Application Loader host software).3. Perform cleanup of all Intel® DAL applications.
Test Pass/Fail Criteria:	All steps return the value "Passed"

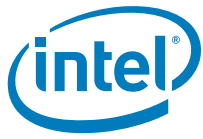
Test ID:	DAL_002
Test Case Title:	Intel® DAL test application installation and load
Mandatory/Optional:	Mandatory
Firmware SKU:	Consumer and Corporate SKUs (Desktop, Mobile and Intel® Ultrabook™)
Description:	Intel® DAL test application will be installed and loaded, verifying basic functionality of Intel® DAL applications execution capability.
Objective:	To test that the Intel® Dynamic Application Loader basic functionality works properly.



Test ID:	DAL_002
Procedure:	<p>Start test DAL_002 in the Intel® Platform Enablement Test Suite from management console.</p> <p>Intel® Platform Enablement Test Suite will perform the following steps:</p> <ol style="list-style-type: none"> 1. Confirm the Intel® Dynamic Application Loader is enabled in firmware. 2. Confirm needed Host software components are available (Intel® MEI driver and Intel® Dynamic Application Loader 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
Firmware SKU:	Consumer and Corporate SKUs (Desktop, Mobile and Intel® Ultrabook™)
Description:	Intel® DAL test application will be installed and loaded, followed by a communication channel exercise between application and host side application.
Objective:	To test that the Intel® Dynamic Application Loader 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 will perform the following steps:</p> <ol style="list-style-type: none"> 1. Confirm the Intel® Dynamic Application Loader is enabled in firmware. 2. Confirm needed Host software components are available (MEI driver and Intel® Dynamic Application Loader host software). 3. Exercise basic communication channel between test application and host to verify connectivity flow 4. Unload the test application.
Test Pass/Fail Criteria:	All steps return the value "Passed"

§ §



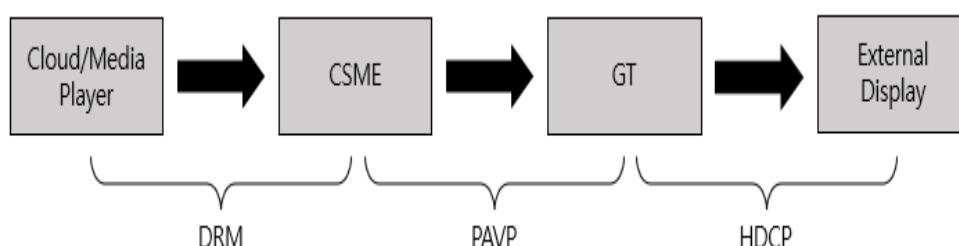
(This page intentionally left blank.)

11 Protected Media Playback

11.1 Overview

Protected Media Playback is supported by Intel® CSME Firmware. Intel® ME employs the following content protection mechanism to safe guard premium content form copy:

- a. Intel® Protected Audio Video Path
- b. Intel® High-bandwidth Digital Content Protection



The Protected Audio/Video Path (PAVP is an Intel-specific collection of content protection features in the Intel "Gen" graphics products. The purpose of PAVP is to first support premium content video playback including UHD Blu-ray discs and supported DRMS such as Microsoft PlayReady3, and second is to provide a protected path from the media player application to the GPU HW.

Protection of the data as it leaves the GPU and goes to an external display is typically done using industry standard HDCP.

11.2 Scope

This chapter describes a test plan for verifying the PAVP FW base capability that is required to enable PAVP for protected playback. The objective is to provide validation professionals with additional insight into Media Playback protection offered by Intel® CSME by highlighting validation considerations. This chapter is not a technology overview. The reader is expected to be familiar with Protected Media Playback or Content Protection and to use this document as a validation supplement to develop his own validation plan. Refer Product Requirement Document(PRD) for additional information on content protection.

11.3 Pre-requisite

This Protected Media Playback evaluation plan documented in this chapter requires the following components and tools for execution.

Intel® Flash Image Tool (fit.exe)

Intel® Flash Programming Tool (Intel® FPT) - is available in Windows* 32-bit (fptw.exe, Windows 64-bit (fptw64.exe operating systems, EFI 32-bit and EFI 64-bit.



11.4 Test Environment Setup

The System Under Test (SUT) is to be configured in manual configuration mode with a 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 (Platform Enabling Test Suite). The network configuration consists of a hub or switch, network cables, and a wireless Access Point (AP).

11.5 Media Playback Test Coverage Summary

'OS Support', and 'How?' Columns describes the test methodology.

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

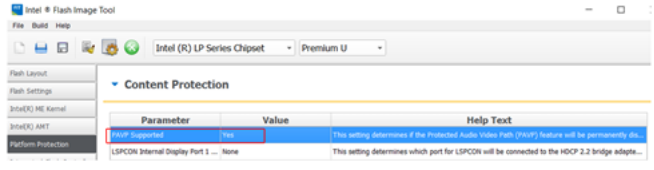
How?: A = Fully Automated using Intel® PETS, I = Interactive using Intel® PETS and M = Manual.

Form Factor: D = Desktop, M = Mobile, A = All in one

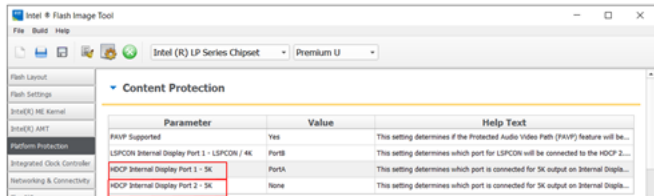
Network Factor: LAN = systems with LAN interface and test is performed using LAN interface, WLAN = systems with WLAN interface and test is performed using the WLAN interface.

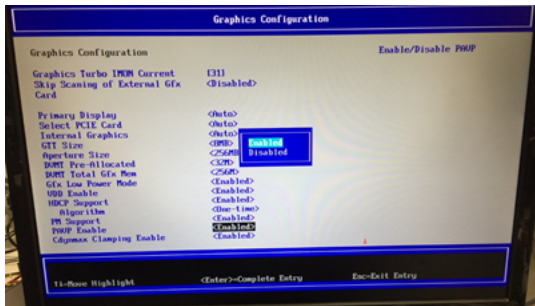
Test ID	Test Case Title	How?	OS Support	Form Factor	Network Factor
Media_001	Verify default configuration settings for Protected Audio Video Path [PAVP] in Firmware Image Tool [FIT]	M	W WI	All	All
Media_003	Verify Internal Port configuration in Firmware Image Tool [FIT]	M	W WI	All	All
Media_004	Verify PAVP Enabled in BIOS (Only if the SUT BIOS menu displays PAVP Mode)	M	W WI	All	All



Test ID:	Media_001
Test Case Title:	Verify default configuration settings for Protected Audio Video Path [PAVP] in Firmware Image Tool [FIT]
Platform	ICL
Mandatory/Optional:	Mandatory
Mobile Only:	No
Firmware SKU:	Consumer/Corporate
Description:	<p>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.</p> <p>In this test we verify the PAVP is enabled in the SUT SPI image using FIT.</p>
Objective:	Verify if the PAVP control in Intel® FIT are set correctly
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	ICL
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 will verify 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 planned 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 will assign 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.
Procedure:	<div><div><div><div>1. Open customer image in FIT tool</div><div>2. Got to Platform Protection tab</div><div>3. Verify the right ports are assigned in the Internal Port parameters</div></div></div><div></div></div>
Test Pass/Fail Criteria:	<p>Test pass criteria:</p> <p>The FIT Internal Port parameters have the right ports assigned intended to be connected to internal panel/eDP</p>

Test ID:	Media_004
Test Case Title:	Verify PAVP Enabled in BIOS
Platform	ICL
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 will verify 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 your BIOS menu where you have PAVP Option [e.g. in Intel BIOS goto - Intel Advance Menu->System Agent (SA) Configuration->Graphics Configuration-> PAVP Enable 3. Verify the PAVP mode setup  <p>The screenshot shows the 'Graphics Configuration' BIOS menu. The 'PAVP Enable' option is highlighted and set to 'Enabled'. Other options include 'Graphics Turbo', 'Skip Scanning of External Gfx Card', 'Primary Display', 'Select PCIe Card', 'Internal Graphics', 'GT Size', 'Aperture Size', 'DMM Pre-Allocated', 'DMM Total Gfx Mem', 'Gfx Low Power Mode', 'USB Enable', 'HDCP Support', 'Higer LDR', 'PM Support', 'PAVP Enable', and 'Capmax Clamping Enable'. The 'PAVP Enable' option is currently set to 'Enabled'.</p>
Test Pass/Fail Criteria:	Test passes if we PAVP is enabled in SUT BIOS.

§ §



(This page intentionally left blank.)



12 Intel® Integrated Clock Control Compliance

This chapter covers details of Intel® ICC test cases supported by all Ice Lake platforms across different segments.

Intel® ICC feature support:

ICC feature support is based on a PCH used on the platform. Refer to below table for more details.

PCH Supported	ICC Feature/Configuration Supported
ICL-LP SKUs	<ul style="list-style-type: none"> Standard Adaptive

Intel® PETS test package detail for Intel® ICC

- 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 ICL-LP SKUs, select xml file from:../ICL/./**Compliance_ICC_ICL_LP**

12.1 Intel® Integrated Clock Control Test Coverage Summary and Details

This section provides summary of ICC test cases applicable to Ice Lake based platforms.

Test ID	Test Case Title	Mandatory	PETS/Manual	Applicable to PCH SKU	Network Factor
ICC_TST_02	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	<ul style="list-style-type: none"> ICL-LP 	LAN+WLAN; WLAN only
ICC_TST_03	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	<ul style="list-style-type: none"> ICL-LP 	LAN+WLAN; WLAN only
ICC_TST_04	Display Chipset Initialization header data	Yes	PETS	<ul style="list-style-type: none"> ICL-LP 	LAN+WLAN; WLAN only



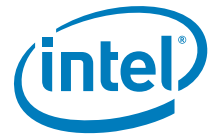
12.2 Intel® Integrated Clock Control Test cases

12.2.1 Test Default Settings for Standard Configuration

Test ID:	ICC_TST_02
Test Case Title:	Test default settings for Standard configuration
Mandatory/Optional:	Mandatory. Note: Only for SUTs with boot profile that to "standard" profile under FIT ->ICC -> Boot Profile or by means of BIOS. 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.
Description:	Verify if the current ICC registers setting in the SUT are set correctly based on standard configuration
Objective:	Ensure that critical ICC register values are configured correctly for standard configuration.
Procedure:	<ol style="list-style-type: none">1. Get ICC Profile: (ICC_GET_PROFILE_CMD) CCT command: <i>CCT.exe -gp</i>2. Check current ICC profile base (it should be standard, otherwise test would fail)3. Get BCLK PLL Settings:<ul style="list-style-type: none">• CCT Command: <i>CCT.exe -gc -clock bclk -get-type current</i> and check that support change allowed = noIf the above is different then the test has failed.4. Try to set the bclk PLL settings:<ul style="list-style-type: none">• CCT Command: <i>CCT.exe -sc -clock bclk -freq 99000000 -ssc 3 -set-type permanent</i>Command result should be: "Clock is not configurable" otherwise the test has failed.
Test Pass/Fail Criteria:	Pass if the critical ICC registers values read are set correctly based on the standard configuration. Note: For FIT, Check parameter under Flash Image Tool Integrated Clock Controller Boot profile selection. If Boot profile is not based on standard profile (for example, Adaptive, Overclocking, or Overclocking Plus or Overclocking Ext), this test is expected to fail.

12.2.2 Test Default Settings for Adaptive Configuration

Test ID:	ICC_TST_03
Test Case Title:	Test default settings for Adaptive configuration
Mandatory/Optional:	Mandatory Note: Only for SUTs with boot profile set to "Adaptive" profile under FIT ->ICC -> Boot Profile or by means of BIOS. Note: Under FIT Tool, ICC Configuration is now moved out of CSME Region. ICC configuration is now added as a independent top level tab. 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 you can skip to execute it.
Description:	Verify if the current ICC registers setting in the SUT are set correctly based on Adaptive configuration

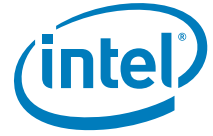


Test ID:	ICC_TST_03
Objective:	Ensure that critical ICC register values match defaults for Adaptive configuration
Procedure:	<ol style="list-style-type: none"> 1. Get ICC Profile: (ICC_GET_PROFILE_CMD) CCT command: <i>CCT.exe -gp</i> 2. Check current ICC profile base (it should be adaptive, otherwise test would fail) 3. Get BCLK PLL Settings: <ul style="list-style-type: none"> • CCT Command: <i>CCT.exe -gc -clock bclk -get-type current</i> and check that under Changeallowed = Yes <p>If one of the above is not 1 then the test has failed.</p> <ol style="list-style-type: none"> 4. Try to set the bclk PLL settings: <ul style="list-style-type: none"> • CCT Command: <i>CCT.exe -sc -clock bclk -freq 99800000 -ssc 3 -set-type permanent</i> 5. Command result should be: "Status: SUCCESS" otherwise the test has failed. <p>Note: The frequency set in step 4 should be defined in the clock range while creating the image in FIT</p>
Test Pass/Fail Criteria:	<p>Pass if the critical ICC registers values read are set correctly based on the standard 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 (for example, Standard this test is expected to fail.</p> <p>Note: Default frequency and SSC supported for Adaptive is 100MHz with 0.50%. Supported Min.-Max. frequency range is [97.50 - 100.00 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>

12.2.3 Display Chipset Initialization Header Data

Test ID:	ICC_TST_04
Test Case Title:	Display Chipset Initialization header data
Mandatory/Optional:	Mandatory, This is informative test.
Description:	<p>This test output high level detail like CRC count into a binary file, Version and product detail of chipset initialization settings.</p> <p>User to manually verify data displayed looks correct or not.</p>
Objective:	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.
Procedure:	<ol style="list-style-type: none"> 1. Get ICC clock capabilities (ICC_GET_HSIO_SETTINGS_CMD) CCT command: <i>.CCT.exe -rm -offset 0x0 -length 0x00ff -file txt.bin</i> 2. The should return HECI CMD Status as "Status: SUCCESS" <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.





(This page intentionally left blank.)



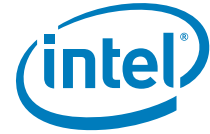
13 Manufacturing Flow Simulation Test

13.1 Manufacturing Flow Simulation Test

Test ID	Test Case Title	PETS/Manual	Form Factor ¹	Network Factor
MFG_001	Intel Manufacturing Flow Simulation Test	Manual		LAN+WLAN; WLAN only

Note: ¹Form Factor is grayed out as LPT-LP supports MB form factor only.

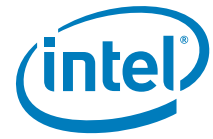
Test ID:	MFG_001
Test Case Title:	Intel Manufacturing Flow Simulation Test
Mandatory/Optional:	Mandatory
Firmware SKU:	Consumer
Description:	For platforms with Intel® ME, it is necessary to perform steps in the manufacturing line to ensure the Intel® CSME is functional and the system is secure, and ready for shipment. The minimum requirements can be met by following the Intel 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 will be 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 will be like during production/manufacturing phase. For 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, for 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 variable check. If this test is conducted on platform with PV or later Production Firmware with production MCP, also configure the desired secure boot setting (OEM public key hash, policy, and so forth.) for Intel(R) Boot Guard and Intel® PTT Supported [FPF] for PTT in MEManuf.xml under configuration check. For pre-production system, there is new flexibility in FIT UI to allow customer disable FPF Hardware Binding including FPF burning on pre-production silicon part while FPT-closemfn command being issued for re-use purpose. In this case, skip step 8 MEManuf EOL test as all real FPFs will remain same and use UEP (firmware) instead or you will expect to see some error. <ul style="list-style-type: none"> PS: For production system this parameter should be set to Enabled by default and FPF burning will be enforced always in revenue platforms. <p>Test Procedure:</p> <ol style="list-style-type: none"> 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). If using pre-lock (the descriptor Master Access permission set to Intel recommended production value during image preparation), do only steps 5, 6, and 8. Reprogram the image currently on board (image.bin). <ul style="list-style-type: none"> Example: FPTW64.exe -f image.bin Reset Intel® CSME and Host after program successfully <ul style="list-style-type: none"> Example: FPTW64.exe -greset Verify Intel® CSME <ul style="list-style-type: none"> Example: MEManufWin64.exe Example (option): MEManufWin64.exe -f MEManuf.xml (use the MEManuf.xml configuration file configured during preparation) Check Boot Guard, PTT, and all the variables match with setting configured in FIT <ul style="list-style-type: none"> Example: MEManufWin64.exe -EOL var -f MEManuf.xml (use the MEManuf configuration file configured during preparation) Set Intel® CSME EOM NVAR and descriptor Master Access permission to Intel recommended production value, then perform global reset to make sure Intel® CSME manufacturing mode is disabled <ul style="list-style-type: none"> Example: FPTW64.exe -closemfn -y Perform end of line check on Intel recommended default test item and also Boot Guard, PTT, and all the configuration check <ul style="list-style-type: none"> Example: MEManufWin64.exe -EOL (Intel recommended default test) Example (option): MEManufWin64.exe -EOL config -f MEManuf.xml (use the MEManuf.xml configuration file configured during preparation) <p>Note: It's highly recommended you create your 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 below items:</p> <ul style="list-style-type: none"> CRB test result in Compliance kit Intel® ME Firmware release note for known issues.



§ §



(This page intentionally left blank.)



14 Intel® Device Protection Technology with Boot Guard

14.1 Overview

Boot Guard formerly Anchor Cove (AnC) is an Intel platform boot integrity protection technology. Boot Guard can help 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 will trigger the platform protection per the OEM policies. Based in the hardware, Boot Guard will also extend 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.

14.2 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 BFItoot 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.

14.3 Pre-requisite

This Boot Guard evaluation plan documented in this chapter requires the following components and tools for execution.

Table 14-1. Boot Guard Tools for Testing

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-Win OS: Use the EFI version of the ME tools (MEinfo.efi) to confirm Boot Guard Policies
TXBTgInfo.efi	0.7.10 or higher	TXBTgInfo.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 Boot Guard status can be determined using various platform status registers: 1. Refer to BIOS Writers Guide for status registers (for example, ERRORCODE, BOOTSTATUS, ANC_SACM_INFO) usage 2. Refer to ME BIOS Writer's Guide for Boot Guard related FWSTS registers verification



14.4 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 TXTBtgInfo.efi tool runs only from EFI shell

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

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

Network Factor: 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	How?
BtG_001	Successful VM (Verified Measured) Boot to OS ¹	M
BtG_002	Unsecure Boot to OS ¹	M
BtG_003	Failed VM (Verified Measured) Boot fail to Fallback	M
BtG_004	Platform Public Signing Key Provisioned	M
BtG_005	Successful VM (Verified Measured) Boot to OS ¹ using FPF	M
BtG_006	BIOS Update Procedure includes Signature Verification	M
BtG_007	Service Center's Recovery process for Boot Guard failed platform	M
BtG_008	BIOS Continues the Chain of Trust	M

Note: ¹Please refer to Chapter 1- Introduction, Section 1.1 for supported Operating Systems (OS)

Test ID:	BtG_001
Test Case Title:	Successful VM (Verified-Measured) Boot to OS
Mandatory/Optional:	Mandatory
Firmware SKU:	Consumer / Corporate
Description:	In this test case, Boot Guard will perform a successful verification and measuring of the SUT Initial Boot Block (IBB.) Upon successful verification Boot Guard will 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">1. Provision the SUT Persistent Policies (NVAR if this is development system) to either the VM or FVE or FVME profile. Per your testing objective<ul style="list-style-type: none">— Note: The FVME profile usage is not advised for the development or testing environment. In this strictest protection mode, test failure will require BIOS flashing to restore the system.— Refer the ME Firmware Bring Up Guide for information on the Boot Guard related FIT options and settings2. 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)3. Install the targeted OS (OS) if not already installed on the SUT4. 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">5. Power-off the SUT.6. Power-on the SUT.7. Boot to EFI shell and execute TXTBtgInfo.efi8. 8. Verify the TXTBtgInfo.efi output to confirm that Boot Guard has booted as configured to verify and measure the IBB.9. Boot to OS.10. Execute PETS package for Boot Guard from Remote Console11. Verify 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 will perform a successful un secure boot of SUT Initial Boot Block (IBB.) Upon successful completion Boot Guard will pass 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



Test ID:	BtG_002
Procedure:	<p>Prepare the SUT Persistent Policy (FPF)</p> <ol style="list-style-type: none"> 1. 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. 2. 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) 3. Install the targeted OS (OS, OS) if not already installed on the SUT 4. 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"> 5. Power-off the SUT 6. Power-on the SUT 7. Boot to EFI shell and execute TXTBtgInfo.efi 8. 8. Verify the TXTBtgInfo.efi output to confirm that Boot Guard has booted as configured to verify and measure the IBB. 9. Boot to the targeted OS 10. Execute PETS package for Boot Guard from Remote Console 11. Verify 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 • 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 will perform an unsuccessful verification and measuring of the SUT Initial Boot Block (IBB.) Upon verification failure Boot Guard will perform 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



Test ID:	BtG_003
Procedure:	<p>Prepare the SUT Persistent Policy (FPF)</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 your testing objective<ul style="list-style-type: none">— Note: The <i>FVME</i> profile usage is not advised for the development or testing environment. In this strictest protection mode, test failure will require BIOS flashing to restore the system.— Refer the ME Firmware Bring Up Guide for information on the Boot Guard related FIT options and settings2. 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)3. Install the targeted OS (OS) if not already installed on the SUT4. 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">5. 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">6. Power-off the SUT7. Power-on the SUT8. Execute PETS package for Boot Guard from Remote Console9. Verify PETS results should Fail10. Verify that the platform has failed per the persistent policy.<ul style="list-style-type: none">— Refer to 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 will halt upon verification failure• FVME - The platform will halt upon verification failure• VM - The platform will 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.
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 your testing objective<ul style="list-style-type: none">— Note: The <i>FVE</i> profile usage is not advised for the development or testing environment. In this strictest protection mode, test failure will require 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 OS3. Run MEInfo.exe4. Evaluate the Boot Guard related fields:<ul style="list-style-type: none">• "FPF" for committed Persistent policies• "ME" for NVAR stored Persistent policies



Test ID:	BtG_004
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 will perform 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 FPFs (Field Programmable Fuses)
Procedure:	<p>Prerequisite: 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 will become 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 will be done automatically after ME Manufacturing mode is disabled (during the global reset from FPT -closemfn 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 ME 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 will indicate 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 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 will be the same as criteria mentioned for each of the tests above (test id #BtG_001 or BtG_004)

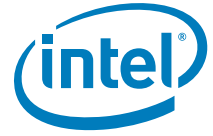


Test ID:	BtG_006
Test Case Title:	BIOS Update Procedure includes Signature Verification
Mandatory/Optional:	Optional
Firmware SKU:	Consumer / Corporate
Description:	This is a manual assessment of your platform BIOS update process to ensure that signature verification is applied to maintain BIOS integrity.
Objective:	Confirm the signature authorization structure defined by the Persistent Policy (FPF)->KM->BPM->IBB are maintained in your BIOS update process.
Procedure:	1. Confirm with your BIOS Development team that your BIOS update process is using proper authorization process to maintain the Boot Guard authorization structure from FPF->KM->BPM->IBB.
Test Pass/Fail Criteria:	Test passes if the SUT: <ul style="list-style-type: none">• If your 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 your 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 your configured persistent policy
Procedure:	1. Evaluate your platform service process for the failed Boot Guard scenario. <ul style="list-style-type: none">• Does the service process meet your platform business objective?
Test Pass/Fail Criteria:	Test passes if the SUT: <ul style="list-style-type: none">• If the platform recovery process meets your 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
Procedure:	1. Confirm with your BIOS Development team that your IBB and the next boot phase is protecting the integrity of the secure boot on your 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: If the BIOS team confirms that the proper protection are implemented for the SUT





(This page intentionally left blank.)



15 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 see 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 to 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)



15.1 Intel® Platform Trust Technology (Intel® PTT) Compliance 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 to Microsoft* support.



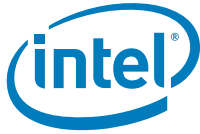
15.2 Verification of BIOS and Intel® Platform Trust Technology (Intel® PTT) Communication Over CRB Interface

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 07. Verify TPM_CRB_CTRL_STS_0.tpmIdle (0xfed40044, bit 1) is 08. 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). Note: For detailed information on how to send a TPM command, refer to the PC client specific platform TPM profile for TPM 2.0
Test Pass/Fail Criteria:	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. Note: HCI reference code provides serial output status of whether or not TPM command is received by PTT. Check PttHciReceive function for more details.



15.3 Intel® Platform Trust Technology (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 installation 2. 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"> a. <code>\$ptt.IsEnabled()</code> b. <code>\$ptt.IsActivated()</code> c. <code>\$ptt.IsAutoProvisioningEnabled()</code> d. <code>\$ptt.IsOwned()</code> e. <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"



15.4 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. We will 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">1. Save the current SrkPublicKey by performing the following actions:<ol style="list-style-type: none">a. Open elevated command prompt and enter PowerShell by typing "powershell" at the prompt and type:b. <code>\$ptt = get-wmiobject -namespace "root/cimv2/security/microsofttpm" win32_tpm</code>c. <code>\$ret = \$ptt.GetSrkPublicKeyModulus()</code>d. <code>\$ret.SrkPublicKeyModulus > SrkPubModOld.txt</code>2. Run "tpm.msc" to open TPM Management Console3. Click 'Clear TPM...' in the Actions pane on right.4. In the pop-up window click 'Restart' to invoke TPM Clear flow.5. 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 will authorize, ESC rejects the operation.6. Upon booting to Windows*, pop-up window will show up indicating OS is taking ownership of the TPM7. After ownership operation completes, press OK.8. Save the new SrkPublicKey by performing the following actions:<ol style="list-style-type: none">a. Open elevated command prompt and enter PowerShell by typing "powershell" at the prompt and type:b. <code>\$ptt = get-wmiobject -namespace "root/cimv2/security/microsofttpm" win32_tpm</code>c. <code>\$ret = \$ptt.GetSrkPublicKeyModulus()</code>d. <code>\$ret.SrkPublicKeyModulus > SrkPubModNew.txt</code>9. Compare the old and new keys
Test Pass/Fail Criteria:	OS takes ownership of TPM, new/old keys differ



15.5 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 will verify 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"> In elevated permissions command line run: "bdehdcfg.exe -driveinfo" and check system drive is configured to support BitLocker Set BitLocker to use TPM for measuring boot devices in Windows* Group Policy by: <ol style="list-style-type: none"> Run "gpedit.msc" to open Group Policy Editor Open "Local Computer Policy" > "Computer Configuration" > "Administrative Templates" > "Windows Components" > "BitLocker Drive Encryption" > "Operating System Drives" On the right pane double click "Configure TPM platform profile for native UEFI firmware configuration" Check the enabled radio button. Verify PCR 0, PCR2, PCR4 and PCR11 are checked in the "Options" pane. Click apply and OK. 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> 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"> manage-bde -protectors -add c: -tpm manage-bde -protectors -add c: -rp 000000-000000-000000-000000-000000-000000-000000-000000 manage-bde -on c: shutdown -r -t 0 After OS completes reboot, verify no error messages displayed. Wait for "Encryption in Progress" notification or type "manage-bde -status" to check on encryption status After encryption reaches 10%, restart system, and verify encryption continues without error message after reboot completes. Turn off BitLocker by typing "manage-bde -off c:" at the command line, decryption process should start 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



15.6 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 will enter recovery mode if any protected component changed during boot. By disabling Intel® PTT, we will check 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 <code>manage-bde -status</code> 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 <code>TPM_Clear</code> command. Note: Clearing TPM by means of the OS will disable Bitlocker and will 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 successfully4. Disable BitLocker by typing "<code>manage-bde -off c:</code>" at the command line, decryption process should start5. 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.



15.7 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 manager 3. Restart Windows*, and check the device is not yellow banded in device manager 4. 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:00000001 b. Open an elevated command prompt c. 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 will pop up, click OK to close 6. Restart the platform, and run step 5 again, to verify certificate persists after reboot 7. 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



15.8 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 to 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 to 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

15.9 Intel® Platform Trust Technology (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's possible for dTPM to show up pending on your platform design).



15.10 Intel® Platform Trust Technology (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 enabled 2. 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 Restart b. OS Shutdown/Power up c. Hibernation/Resume d. 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

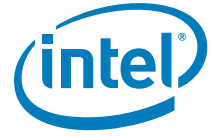
15.11 Dictionary Attack Lockout After Coin Battery Removal with EOM Commit

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 will enter 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 will 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 will be blown. With such parts, test will consistently enter 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 will not occur during manufacturing mode2. 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* 105. Try to view the certificate in VSC by running: CertUtil.exe -scinfo -pin "12345678".6. The command should fail due to Dictionary Attack lockout7. Wait 2 hours for lockout to pass, and try again, it should be possible to access the certificate8. 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 will not allow access to user data (VSC during lockout period post coin battery removal)</p> <p>Note: In this test Field Programmable Fuses (FPF) will be blown on every battery removal and there is no recovery for it. Only select few processors to be used for this test and track them.</p>

§ §



(This page intentionally left blank.)



16 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 to 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 to the Intel® PETS user guide available in the Intel® Compliance 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).



16.1 Test Coverage Summary

OS Support', and 'How?' Columns describe 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.

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

Network Factor: 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	How?	Intel® PETS Package Name	Network Factor
PSS_001	Intel Integrated Wired LAN Test	I	Compliance_PSS.xml	LAN+WLAN; WLAN only
PSS_002	Wake On Wireless LAN (WoWLAN) Test	I	Compliance_PSS.xml	LAN+WLAN; WLAN only
PSS_003	Flexible I/O Test	I	Compliance_PSS.xml	LAN+WLAN; WLAN only
PSS_004	BIOS Boot-Block Size Test	I	Compliance_PSS.xml	LAN+WLAN; WLAN only
PSS_005	Intel® CSME SMBus ASD Address Test	I	Compliance_PSS.xml	LAN+WLAN; WLAN only
PSS_007	Power State Deep Sx Test	I	Compliance_PSS.xml	LAN+WLAN; WLAN only
PSS_008	TPM on SPI Test	I	Compliance_PSS.xml	LAN+WLAN; WLAN only



16.2 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 your platform, these PCH SoftStraps must be configured correctly as well.																					
Objective:	To verify correct configuration of PCH SoftStraps related to Intel Integrated Wired LAN.																					
Procedure:	Boot to targeted OS. Verify correct configuration of the PCH SoftStraps below:																					
	1. If using the Intel Integrated Wired LAN solution:																					
	<table><tr><th>Name</th><th>Location</th><th>Value</th></tr><tr><td>SMLink0 Enable</td><td>Offset 0x191 [0] LP</td><td>1h</td></tr><tr><td>GbE PHY SMBus Address</td><td>Offset 0x1C4 [6:0] LP</td><td>64h</td></tr><tr><td>GbE MAC SMBus Address</td><td>Offset 0x1BC [6:0] LP</td><td>70h</td></tr><tr><td>GbE MAC SMBus Address Enable</td><td>Offset 0x1BF [0] LP</td><td>1h</td></tr><tr><td>PHY Connection</td><td>Offset 0x21E [2:0] LP</td><td>2h</td></tr><tr><td>Intel® Integrated wired LAN Enable</td><td>Offset 0xC18 [0] LP</td><td>0h</td></tr></table>	Name	Location	Value	SMLink0 Enable	Offset 0x191 [0] LP	1h	GbE PHY SMBus Address	Offset 0x1C4 [6:0] LP	64h	GbE MAC SMBus Address	Offset 0x1BC [6:0] LP	70h	GbE MAC SMBus Address Enable	Offset 0x1BF [0] LP	1h	PHY Connection	Offset 0x21E [2:0] LP	2h	Intel® Integrated wired LAN Enable	Offset 0xC18 [0] LP	0h
	Name	Location	Value																			
	SMLink0 Enable	Offset 0x191 [0] LP	1h																			
	GbE PHY SMBus Address	Offset 0x1C4 [6:0] LP	64h																			
	GbE MAC SMBus Address	Offset 0x1BC [6:0] LP	70h																			
	GbE MAC SMBus Address Enable	Offset 0x1BF [0] LP	1h																			
	PHY Connection	Offset 0x21E [2:0] LP	2h																			
	Intel® Integrated wired LAN Enable	Offset 0xC18 [0] LP	0h																			
a. What PCIe* port is the Intel® PHY attached?																						
<table><tr><th>Name</th><th>Location</th><th>Value</th></tr><tr><td rowspan="5">GBE PCIe* Port Select</td><td>Offset 0x1F0 [3:0] LP</td><td>8h = Port 7</td></tr><tr><td>Offset 0x1F0 [7:4]</td><td>8h = Port 8</td></tr><tr><td>Offset 0x1F1 [3:0]</td><td>8h = Port 9</td></tr><tr><td>Offset 0x1F3 [3:0]</td><td>8h = Port 13</td></tr><tr><td>Offset 0x1F3 [7:4]</td><td>8h = Port 14</td></tr></table>	Name	Location	Value	GBE PCIe* Port Select	Offset 0x1F0 [3:0] LP	8h = Port 7	Offset 0x1F0 [7:4]	8h = Port 8	Offset 0x1F1 [3:0]	8h = Port 9	Offset 0x1F3 [3:0]	8h = Port 13	Offset 0x1F3 [7:4]	8h = Port 14								
Name	Location	Value																				
GBE PCIe* Port Select	Offset 0x1F0 [3:0] LP	8h = Port 7																				
	Offset 0x1F0 [7:4]	8h = Port 8																				
	Offset 0x1F1 [3:0]	8h = Port 9																				
	Offset 0x1F3 [3:0]	8h = Port 13																				
	Offset 0x1F3 [7:4]	8h = Port 14																				
Caution: Mapping GbE to any of the PCIe* ports means all 4 Lanes of that PCIe* will no longer be available as PCIe* ports.																						



Test ID:	PSS_001															
	<div>b. Is GPD11 from PCH routed to LAN_DISABLE_N on the Intel wired LAN PHY? (Requires Schematic Review)</div> <div>— If YES:</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 0x110 [4] LP</td><td>0h</td></tr></tbody></table> <div>— If NO:</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 0x110 [4] LP</td><td>1h</td></tr></tbody></table>	Name	Location	Value	LAN PHY Power Control GPD11 Signal Configuration	Offset 0x110 [4] LP	0h	Name	Location	Value	LAN PHY Power Control GPD11 Signal Configuration	Offset 0x110 [4] LP	1h			
Name	Location	Value														
LAN PHY Power Control GPD11 Signal Configuration	Offset 0x110 [4] LP	0h														
Name	Location	Value														
LAN PHY Power Control GPD11 Signal Configuration	Offset 0x110 [4] LP	1h														
	<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 0x110 [4] LP</td><td>0h</td></tr><tr><td>Gbe MAC SMBus Address Enable</td><td>Offset 0x1BF [0] LP</td><td>0h</td></tr><tr><td>PHY Connection</td><td>Offset 0x21E [2:0] LP</td><td>0h</td></tr><tr><td>Intel® Integrated wired LAN Enable</td><td>Offset 0xC18 [0] LP</td><td>1h</td></tr></tbody></table>	Name	Location	Value	LAN PHY Power Control GPD11 Signal Configuration	Offset 0x110 [4] LP	0h	Gbe MAC SMBus Address Enable	Offset 0x1BF [0] LP	0h	PHY Connection	Offset 0x21E [2:0] LP	0h	Intel® Integrated wired LAN Enable	Offset 0xC18 [0] LP	1h
Name	Location	Value														
LAN PHY Power Control GPD11 Signal Configuration	Offset 0x110 [4] LP	0h														
Gbe MAC SMBus Address Enable	Offset 0x1BF [0] LP	0h														
PHY Connection	Offset 0x21E [2:0] LP	0h														
Intel® Integrated wired LAN Enable	Offset 0xC18 [0] LP	1h														
Test Pass/Fail Criteria:	Test passes if SoftStraps/register setting in this step matches to the configuration in the target system.															



16.3 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?</p> <p>— 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 0x110 [3] LP</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 0x110 [3] LP</td><td>1h</td></tr></table>		Name	Location	Value	SLP_WLAN# / GPD9 Signal Configuration	Offset 0x110 [3] LP	0h	Name	Location	Value	SLP_WLAN# / GPD9 Signal Configuration	Offset 0x110 [3] LP	1h
Name	Location	Value												
SLP_WLAN# / GPD9 Signal Configuration	Offset 0x110 [3] LP	0h												
Name	Location	Value												
SLP_WLAN# / GPD9 Signal Configuration	Offset 0x110 [3] LP	1h												
Test Pass/Fail Criteria:	Test passes if SoftStraps/register setting in this step matches to the configuration in the target system.													



16.4 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.



Test ID:

PSS_003

Procedure:

Boot to targeted OS. Verify correct configuration of the PCH SoftStraps below:

1. How do you have PCIe Controller 1 (Port 1-4) configured?

a. 1x4 – one 4 lane PCIe* Port

Name	Location	Value
PCIe Controller 1 (Port 1-4)	Offset 0x155 [4:3] LP	3h

iii. Are the lanes reversed?

– If Reversed:

Name	Location	Value
PCIe Controller 1 Lane Reversal	Offset 0x155 [2] LP	1h

– If NOT Reversed:

Name	Location	Value
PCIe Controller 1 Lane Reversal	Offset 0x155 [2] LP	0h

b. 2x2 – two 2 lane PCIe* Port

Name	Location	Value
PCIe Controller 1 (Port 1-4)	Offset 0x155 [4:3] LP	2h

c. 1x2, 2x1- One 2 lane PCIe* Port, Two 1 lane PCIe* Port

Name	Location	Value
PCIe Controller 1 (Port 1-4)	Offset 0x155 [4:3] LP	1h

d. 4x1: Ports (1-4) (x1)

Name	Location	Value
PCIe Controller 1 (Port 1-4)	Offset 0x15D [4:3] LP	0h

2. How do you have PCIe Controller 2 (Port 5-8) configured?

a. 1x4 – One 4 lanes PCIe* Port.

Name	Location	Value
PCIe Controller 2 (Port 5-8)	Offset 0x15D [4:3] LP	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 0x15D [2] LP</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 0x15D [2] LP</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 0x15D [4:3] LP</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 0x15D [4:3] LP</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 0x15D [4:3] LP</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 0x165 [4:3] LP</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 0x165 [2] LP</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 0x165 [2] LP</td> <td>0h</td> </tr> </tbody> </table>			Name	Location	Value	PCIe Controller 2 Lane Reversal	Offset 0x15D [2] LP	1h	Name	Location	Value	PCIe Controller 2 Lane Reversal	Offset 0x15D [2] LP	0h	Name	Location	Value	PCIe Controller 2 (Port 5-8)	Offset 0x15D [4:3] LP	2h	Name	Location	Value	PCIe Controller 2 (Port 5-8)	Offset 0x15D [4:3] LP	1h	Name	Location	Value	PCIe Controller 2 (Port 5-8)	Offset 0x15D [4:3] LP	0h	Name	Location	Value	PCIe Controller 3 (Port 9-12)	Offset 0x165 [4:3] LP	3h	Name	Location	Value	PCIe Controller 3 Lane Reversal	Offset 0x165 [2] LP	1h	Name	Location	Value	PCIe Controller 3 Lane Reversal	Offset 0x165 [2] LP	0h
Name	Location	Value																																																	
PCIe Controller 2 Lane Reversal	Offset 0x15D [2] LP	1h																																																	
Name	Location	Value																																																	
PCIe Controller 2 Lane Reversal	Offset 0x15D [2] LP	0h																																																	
Name	Location	Value																																																	
PCIe Controller 2 (Port 5-8)	Offset 0x15D [4:3] LP	2h																																																	
Name	Location	Value																																																	
PCIe Controller 2 (Port 5-8)	Offset 0x15D [4:3] LP	1h																																																	
Name	Location	Value																																																	
PCIe Controller 2 (Port 5-8)	Offset 0x15D [4:3] LP	0h																																																	
Name	Location	Value																																																	
PCIe Controller 3 (Port 9-12)	Offset 0x165 [4:3] LP	3h																																																	
Name	Location	Value																																																	
PCIe Controller 3 Lane Reversal	Offset 0x165 [2] LP	1h																																																	
Name	Location	Value																																																	
PCIe Controller 3 Lane Reversal	Offset 0x165 [2] LP	0h																																																	



Test ID:	PSS_003	
b. 2x2 – two 2 lanes PCIe* Port.		
Name	Location	Value
PCIe Controller 3 (Port 9-12)	Offset 0x165 [4:3] LP	2h
c. 1x2, 2x1 – One 2 lanes PCIe* Port, Two 1 lane PCIe*.		
Name	Location	Value
PCIe Controller 3 (Port 9-12)	Offset 0x165 [4:3] LP	1h
4x1- One 1 lane PCIe** Port.		
Name	Location	Value
PCIe Controller 3 (Port 9-12)	Offset 0x165 [4:3] LP	0h
4. How do you have PCIe Controller 4 (Port 13-16) configured?		
a. 1x4 – One 4 lanes PCIe* Port.		
Name	Location	Value
PCIe Controller 4 (Port 13-16)	Offset 0x16D [4:3] LP	3h
i. Are the lanes reversed? — If reversed:		
Name	Location	Value
PCIe Controller 4 Lane Reversal	Offset 0x16D [2] LP	1h
— If NOT reversed:		
Name	Location	Value
PCIe Controller 4 Lane Reversal	Offset 0x16D [2] LP	0h
b. 2x2 – two 2 lanes PCIe* Port.		
Name	Location	Value
PCIe Controller 4 (Port 13-16)	Offset 0x16D [4:3] LP	2h
c. 1x2, 2x1 – One 2 lanes PCIe* Port, Two 1 lane PCIe* Port.		
Name	Location	Value
PCIe Controller 4 (Port 13-16)	Offset 0x16D [4:3] LP	1h
4x1- One 1 lane PCIe** Port.		
Name	Location	Value
PCIe Controller 4 (Port 13-16)	Offset 0x16D [4:3] LP	0h



Test ID:	PSS_003																																																
	<p>7. Does this platform use PCH PCIe port 1 as USB3 Port 1? — If yes, PCH PCIe Port 1 configured as USB3</p> <table><tr><th>Name</th><th>Location</th><th>Value</th></tr><tr><td>USB3 / PCIe Combo Port 0</td><td>Offset 0x1ED [3:0] LP</td><td>1h</td></tr></table> <p>— If no, PCH PCIe Port 1 configured as PCIe</p> <table><tr><th>Name</th><th>Location</th><th>Value</th></tr><tr><td>USB3 / PCIe Combo Port 0</td><td>Offset 0x1ED [1:0] LP</td><td>5h</td></tr></table> <p>8. Does this platform use PCH PCIe Port 2 as USB3 Port 2? — If yes, PCH PCIe Port 2 configured as USB3</p> <table><tr><th>Name</th><th>Location</th><th>Value</th></tr><tr><td>USB3 / PCIe Combo Port 1</td><td>Offset 0x1ED [7:4] LP</td><td>1h</td></tr></table> <p>— If no, PCH PCIe Port 2 configured as PCIe</p> <table><tr><th>Name</th><th>Location</th><th>Value</th></tr><tr><td>USB3 / PCIe Combo Port 1</td><td>Offset 0x1ED [7:4] LP</td><td>5h</td></tr></table> <p>9. Does this platform use PCH PCIe Port 3 as USB3 Port 3? — If yes, PCH PCIe Port 3 configured as USB3</p> <table><tr><th>Name</th><th>Location</th><th>Value</th></tr><tr><td>USB3 / PCIe Combo Port 2</td><td>Offset 0x1EE [3:0] LP</td><td>1h</td></tr></table> <p>— If no, PCH PCIe Port 3 configured as PCIe</p> <table><tr><th>Name</th><th>Location</th><th>Value</th></tr><tr><td>USB3 / PCIe Combo Port 2</td><td>Offset 0x1EE [3:0] LP</td><td>5h</td></tr></table> <p>10. Does this platform use PCH PCIe Port 4 as USB3 Port 4? — If yes, PCH PCIe Port 4 configured as USB3</p> <table><tr><th>Name</th><th>Location</th><th>Value</th></tr><tr><td>USB3 / PCIe Combo Port 3</td><td>Offset 0x1EE [7:4] LP</td><td>1h</td></tr></table> <p>— If no, PCH PCIe Port 4 configured as PCIe</p> <table><tr><th>Name</th><th>Location</th><th>Value</th></tr><tr><td>USB3 / PCIe Combo Port 3</td><td>Offset 0x1EE [7:4] LP</td><td>5h</td></tr></table>	Name	Location	Value	USB3 / PCIe Combo Port 0	Offset 0x1ED [3:0] LP	1h	Name	Location	Value	USB3 / PCIe Combo Port 0	Offset 0x1ED [1:0] LP	5h	Name	Location	Value	USB3 / PCIe Combo Port 1	Offset 0x1ED [7:4] LP	1h	Name	Location	Value	USB3 / PCIe Combo Port 1	Offset 0x1ED [7:4] LP	5h	Name	Location	Value	USB3 / PCIe Combo Port 2	Offset 0x1EE [3:0] LP	1h	Name	Location	Value	USB3 / PCIe Combo Port 2	Offset 0x1EE [3:0] LP	5h	Name	Location	Value	USB3 / PCIe Combo Port 3	Offset 0x1EE [7:4] LP	1h	Name	Location	Value	USB3 / PCIe Combo Port 3	Offset 0x1EE [7:4] LP	5h
Name	Location	Value																																															
USB3 / PCIe Combo Port 0	Offset 0x1ED [3:0] LP	1h																																															
Name	Location	Value																																															
USB3 / PCIe Combo Port 0	Offset 0x1ED [1:0] LP	5h																																															
Name	Location	Value																																															
USB3 / PCIe Combo Port 1	Offset 0x1ED [7:4] LP	1h																																															
Name	Location	Value																																															
USB3 / PCIe Combo Port 1	Offset 0x1ED [7:4] LP	5h																																															
Name	Location	Value																																															
USB3 / PCIe Combo Port 2	Offset 0x1EE [3:0] LP	1h																																															
Name	Location	Value																																															
USB3 / PCIe Combo Port 2	Offset 0x1EE [3:0] LP	5h																																															
Name	Location	Value																																															
USB3 / PCIe Combo Port 3	Offset 0x1EE [7:4] LP	1h																																															
Name	Location	Value																																															
USB3 / PCIe Combo Port 3	Offset 0x1EE [7:4] LP	5h																																															



Test ID:	PSS_003		
	15. Does this platform use PCH PCIe Port 5 as USB3 Port 5? — If yes, PCH PCIe Port 3 configured as USB3		
	Name	Location	Value
	USB3 / PCIe Combo Port 4	Offset 0x1EF [3:0] LP	1h
	— If no, PCH PCIe Port 5 configured as PCIe		
	Name	Location	Value
	USB3 / PCIe Combo Port 4	Offset 0x1EF [3:0] LP	5h
	16. Does this platform use PCH PCIe Port 6 as USB3 Port 6? — If yes, PCH PCIe Port 4 configured as USB3		
	Name	Location	Value
	USB3 / PCIe Combo Port 5	Offset 0x1EF [7:4] LP	1h
	— If no, PCH PCIe Port 6 configured as PCIe		
	Name	Location	Value
	USB3 / PCIe Combo Port 5	Offset 0x1EF [7:4] LP	5h



Test ID:	PSS_003																																																
	<div>1. How is SATA / PCIe* Combo Port 0 Strap configured on the platform?</div> <div><div>i. Statically assigned to SATA Port 0.</div><table><tr><th>Name</th><th>Location</th><th>Value</th></tr><tr><td>SATA / PCIe Combo Port 0 Strap</td><td>Offset 1F2 [3:0] LP</td><td>7h</td></tr></table></div> <div><div>ii. Statically assigned to PCIe* Port 11.</div><table><tr><th>Name</th><th>Location</th><th>Value</th></tr><tr><td>SATA / PCIe Combo Port 0 Strap</td><td>Offset 1F2 [3:0] LP</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 1F2 [3:0] LP</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 1F2 [3:0] LP</td><td>Dh</td></tr></table></div> <div>2. How is SATA / PCIe* Combo Port 1 Strap configured on the platform?</div> <div><div>i. Statically assigned to SATA Port 1a.</div><table><tr><th>Name</th><th>Location</th><th>Value</th></tr><tr><td>SATA / PCIe Combo Port 1 Strap</td><td>Offset 1F2 [7:4] LP</td><td>7h</td></tr></table></div> <div><div>ii. Statically assigned to PCIe* Port 12.</div><table><tr><th>Name</th><th>Location</th><th>Value</th></tr><tr><td>SATA / PCIe Combo Port 1 Strap</td><td>Offset 1F2 [7:4] LP</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 1F2 [7:4] LP</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 1F2 [7:4] LP</td><td>Dh</td></tr></table></div>	Name	Location	Value	SATA / PCIe Combo Port 0 Strap	Offset 1F2 [3:0] LP	7h	Name	Location	Value	SATA / PCIe Combo Port 0 Strap	Offset 1F2 [3:0] LP	5h	Name	Location	Value	SATA / PCIe Combo Port 0 Strap	Offset 1F2 [3:0] LP	Ch	Name	Location	Value	SATA / PCIe Combo Port 0 Strap	Offset 1F2 [3:0] LP	Dh	Name	Location	Value	SATA / PCIe Combo Port 1 Strap	Offset 1F2 [7:4] LP	7h	Name	Location	Value	SATA / PCIe Combo Port 1 Strap	Offset 1F2 [7:4] LP	5h	Name	Location	Value	SATA / PCIe Combo Port 1 Strap	Offset 1F2 [7:4] LP	Ch	Name	Location	Value	SATA / PCIe Combo Port 1 Strap	Offset 1F2 [7:4] LP	Dh
Name	Location	Value																																															
SATA / PCIe Combo Port 0 Strap	Offset 1F2 [3:0] LP	7h																																															
Name	Location	Value																																															
SATA / PCIe Combo Port 0 Strap	Offset 1F2 [3:0] LP	5h																																															
Name	Location	Value																																															
SATA / PCIe Combo Port 0 Strap	Offset 1F2 [3:0] LP	Ch																																															
Name	Location	Value																																															
SATA / PCIe Combo Port 0 Strap	Offset 1F2 [3:0] LP	Dh																																															
Name	Location	Value																																															
SATA / PCIe Combo Port 1 Strap	Offset 1F2 [7:4] LP	7h																																															
Name	Location	Value																																															
SATA / PCIe Combo Port 1 Strap	Offset 1F2 [7:4] LP	5h																																															
Name	Location	Value																																															
SATA / PCIe Combo Port 1 Strap	Offset 1F2 [7:4] LP	Ch																																															
Name	Location	Value																																															
SATA / PCIe Combo Port 1 Strap	Offset 1F2 [7:4] LP	Dh																																															
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						
	Icelake-U Only						
	3. How is SATA / PCIe* Combo Port 2 Strap configured on the platform?						
	i. Statically assigned to SATA Port 1b.						
	<table><tr><th>Name</th><th>Location</th><th>Value</th></tr><tr><td>SATA / PCIe Combo Port 2 Strap</td><td>Offset 1F4 [3:0] LP</td><td>7h</td></tr></table>	Name	Location	Value	SATA / PCIe Combo Port 2 Strap	Offset 1F4 [3:0] LP	7h
	Name	Location	Value				
	SATA / PCIe Combo Port 2 Strap	Offset 1F4 [3:0] LP	7h				
	ii. Statically assigned to PCIe* Port 13.						
	<table><tr><th>Name</th><th>Location</th><th>Value</th></tr><tr><td>SATA / PCIe Combo Port 2 Strap</td><td>Offset 1F4 [3:0] LP</td><td>5h</td></tr></table>	Name	Location	Value	SATA / PCIe Combo Port 2 Strap	Offset 1F4 [3:0] LP	5h
	Name	Location	Value				
	SATA / PCIe Combo Port 2 Strap	Offset 1F4 [3:0] LP	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 2 Strap</td><td>Offset 1F4 [3:0] LP</td><td>Ch</td></tr></table>	Name	Location	Value	SATA / PCIe Combo Port 2 Strap	Offset 1F4 [3:0] LP	Ch
	Name	Location	Value				
	SATA / PCIe Combo Port 2 Strap	Offset 1F4 [3:0] LP	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 2 Strap</td><td>Offset 1F4 [3:0] LP</td><td>Dh</td></tr></table>	Name	Location	Value	SATA / PCIe Combo Port 2 Strap	Offset 1F4 [3:0] LP	Dh	
Name	Location	Value					
SATA / PCIe Combo Port 2 Strap	Offset 1F4 [3:0] LP	Dh					
4. How is SATA / PCIe* Combo Port 3 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 3 Strap</td><td>Offset 1F4 [7:4] LP</td><td>7h</td></tr></table>	Name	Location	Value	SATA / PCIe Combo Port 3 Strap	Offset 1F4 [7:4] LP	7h	
Name	Location	Value					
SATA / PCIe Combo Port 3 Strap	Offset 1F4 [7:4] LP	7h					
ii. Statically assigned to PCIe* Port 14.							
<table><tr><th>Name</th><th>Location</th><th>Value</th></tr><tr><td>SATA / PCIe Combo Port 3 Strap</td><td>Offset 1F4 [7:4] LP</td><td>5h</td></tr></table>	Name	Location	Value	SATA / PCIe Combo Port 3 Strap	Offset 1F4 [7:4] LP	5h	
Name	Location	Value					
SATA / PCIe Combo Port 3 Strap	Offset 1F4 [7:4] LP	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 3 Strap</td><td>Offset 1F4 [7:4] LP</td><td>Ch</td></tr></table>	Name	Location	Value	SATA / PCIe Combo Port 3 Strap	Offset 1F4 [7:4] LP	Ch	
Name	Location	Value					
SATA / PCIe Combo Port 3 Strap	Offset 1F4 [7:4] LP	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 3 Strap</td><td>Offset 1F4 [7:4] LP</td><td>Dh</td></tr></table>	Name	Location	Value	SATA / PCIe Combo Port 3 Strap	Offset 1F4 [7:4] LP	Dh	
Name	Location	Value					
SATA / PCIe Combo Port 3 Strap	Offset 1F4 [7:4] LP	Dh					
Test Pass/Fail Criteria:	Test passes if SoftStraps/register setting in this step matches to the configuration in the target system.						



16.5 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 will 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 your 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 0x140 [6:4] LP</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 0x140 [6:4] LP</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 0x140 [6:4] LP</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 0x140 [6:4] LP</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 0x140 [6:4] LP</td><td>4h</td></tr> </tbody> </table>		Name	Location	Value	Top Swap Block size	Offset 0x140 [6:4] LP	0h	Name	Location	Value	Top Swap Block size	Offset 0x140 [6:4] LP	1h	Name	Location	Value	Top Swap Block size	Offset 0x140 [6:4] LP	2h	Name	Location	Value	Top Swap Block size	Offset 0x140 [6:4] LP	3h	Name	Location	Value	Top Swap Block size	Offset 0x140 [6:4] LP	4h
Name	Location	Value																														
Top Swap Block size	Offset 0x140 [6:4] LP	0h																														
Name	Location	Value																														
Top Swap Block size	Offset 0x140 [6:4] LP	1h																														
Name	Location	Value																														
Top Swap Block size	Offset 0x140 [6:4] LP	2h																														
Name	Location	Value																														
Top Swap Block size	Offset 0x140 [6:4] LP	3h																														
Name	Location	Value																														
Top Swap Block size	Offset 0x140 [6:4] LP	4h																														
Test Pass/Fail Criteria:	Test passes if SoftStraps/register setting in this step matches to the configuration in the target system.																															



16.6 Intel® Converged Security and Management Engine (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:	<p>Boot to targeted OS. Verify correct configuration of the PCH SoftStraps below:</p> <p>1. Is there an Alert Sending Device (ASD) on Host SMBus?</p> <p>Note: This is only valid for Intel® AMT enabled platforms (See SPI Programming Guide for more information)</p> <p>— If YES,</p> <table><tr><th>Name</th><th>Location</th><th>Value</th></tr><tr><td>Intel® CSME SMBus ASD Address</td><td>Offset 0x180 [6:0] LP</td><td>See details in ¹SPI Programming Guide</td></tr><tr><td>Intel® CSME SMBus ASD Address Enable</td><td>Offset 0x183 [0] LP</td><td>1h</td></tr><tr><td>Intel® CSME SMBus Subsystem Device ID for ASF</td><td>Offset 0x186 [31:0] LP</td><td>See details in ²SPI Programming Guide</td></tr></table> <p>— If NO,</p> <table><tr><th>Name</th><th>Location</th><th>Value</th></tr><tr><td>Intel® CSME SMBus ASD Address</td><td>Offset 0x180 [6:0] LP</td><td>0h</td></tr><tr><td>Intel® CSME SMBus ASD Address Enable</td><td>Offset 0x183 [0] LP</td><td>0h</td></tr><tr><td>Intel® CSME SMBus Subsystem Device ID for ASF</td><td>Offset 0x186 [31:0] LP</td><td>0h</td></tr></table> <p>Note:</p> <p>¹Intel® 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.</p> <p>²Intel® CSME SMBus Subsystem Vendor and Device ID.</p>	Name	Location	Value	Intel® CSME SMBus ASD Address	Offset 0x180 [6:0] LP	See details in ¹ SPI Programming Guide	Intel® CSME SMBus ASD Address Enable	Offset 0x183 [0] LP	1h	Intel® CSME SMBus Subsystem Device ID for ASF	Offset 0x186 [31:0] LP	See details in ² SPI Programming Guide	Name	Location	Value	Intel® CSME SMBus ASD Address	Offset 0x180 [6:0] LP	0h	Intel® CSME SMBus ASD Address Enable	Offset 0x183 [0] LP	0h	Intel® CSME SMBus Subsystem Device ID for ASF	Offset 0x186 [31:0] LP	0h
Name	Location	Value																							
Intel® CSME SMBus ASD Address	Offset 0x180 [6:0] LP	See details in ¹ SPI Programming Guide																							
Intel® CSME SMBus ASD Address Enable	Offset 0x183 [0] LP	1h																							
Intel® CSME SMBus Subsystem Device ID for ASF	Offset 0x186 [31:0] LP	See details in ² SPI Programming Guide																							
Name	Location	Value																							
Intel® CSME SMBus ASD Address	Offset 0x180 [6:0] LP	0h																							
Intel® CSME SMBus ASD Address Enable	Offset 0x183 [0] LP	0h																							
Intel® CSME SMBus Subsystem Device ID for ASF	Offset 0x186 [31:0] LP	0h																							
Test Pass/Fail Criteria:	Test passes if SoftStraps/register setting in this step matches to the configuration in the target system.																								





16.7 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 0x178 [20] LP Offset 0xC14 [20]</td><td>1h 1h</td></tr></table>			Name	Location	Value	Deep Sx Enable	Offset 0x178 [20] LP Offset 0xC14 [20]	1h 1h
	Name	Location	Value						
	Deep Sx Enable	Offset 0x178 [20] LP 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 0x178 [20] LP Offset 0xC14 [20]</td><td>0h 0h</td></tr></table>			Name	Location	Value	Deep Sx Enable	Offset 0x178 [20] LP Offset 0xC14 [20]	0h 0h	
Name	Location	Value							
Deep Sx Enable	Offset 0x178 [20] LP 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.								



16.8 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 0x1E8 [0] LP</td><td>1h 1h</td></tr></table>	Name	Location	Value	TPM Over SPI Bus Enable	Offset 0x1E8 [0] LP	1h 1h		
	Name	Location	Value						
	TPM Over SPI Bus Enable	Offset 0x1E8 [0] LP	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 0x1E8 [0] LP</td><td>0h</td></tr></table>	Name	Location	Value	TPM Over SPI Bus Enable	Offset 0x1E8 [0] LP	0h		
	Name	Location	Value						
	TPM Over SPI Bus Enable	Offset 0x1E8 [0] LP	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 0x145 [2:0] LP</td><td>2h</td></tr></table>	Name	Location	Value	SPI TPM Clock Frequency	Offset 0x145 [2:0] LP	2h		
Name	Location	Value							
SPI TPM Clock Frequency	Offset 0x145 [2:0] LP	2h							
b. 30MHz									
<table><tr><th>Name</th><th>Location</th><th>Value</th></tr><tr><td>SPI TPM Clock Frequency</td><td>Offset 0x145 [2:0] LP</td><td>4h</td></tr></table>	Name	Location	Value	SPI TPM Clock Frequency	Offset 0x145 [2:0] LP	4h			
Name	Location	Value							
SPI TPM Clock Frequency	Offset 0x145 [2:0] LP	4h							
c. 17MHz									
<table><tr><th>Name</th><th>Location</th><th>Value</th></tr><tr><td>SPI TPM Clock Frequency</td><td>Offset 0x145 [2:0] LP</td><td>6h</td></tr></table>	Name	Location	Value	SPI TPM Clock Frequency	Offset 0x145 [2:0] LP	6h			
Name	Location	Value							
SPI TPM Clock Frequency	Offset 0x145 [2:0] LP	6h							
d.									
Test Pass/Fail Criteria:	Test passes if SoftStraps/register setting in this step matches to the configuration in the target system.								

§ §



(This page intentionally left blank.)



17 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.

17.1 Introduction

17.1.1 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 (see [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.

17.1.2 Platforms Applicable

This validation guide is applicable to the following Client platforms and their corresponding chipsets:

Table 17-1. List of Applicable Platforms

Platform Name
Intel® Core™ and Intel® Core™ M Processors Platforms
Ice Lake Platform

17.1.3 Terminology

Table 17-2. Terminology (Sheet 1 of 2)

Term	Description
DMA	Direct Memory Access
GPA	Guest Physical Address



Table 17-2. Terminology (Sheet 2 of 2)

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

17.1.4 Intel® Virtualization Testing Pre-requisites

Table 17-3. Virtualization Testing Pre-requisites

Prerequisite Checklist	Location
Client VT Info Tool	CCL Document Number 551893

17.2 Intel® Virtualization Technology (Intel® VT) Test Plan and Details

Table 17-4. 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* 10	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

17.3 Intel® VT Tests in EFI Shell

17.3.0.1 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**. **Skip POSTBOOT SAI Setting** must be selected as **TRUE** under Advanced Debug Settings.

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 CCL using Document #551893.

17.3.0.2 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 BIOS Note: Make Sure TXT is disabled (for test purposes only). 2. Download Client VT Info Tool CCL #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 number 7. Record score. (Make a note of how many tests PASS and how many FAIL.) See example outputs below in section Section 17.3.0.2.1: "Sample Output for Client VT Info Tool Results—Passing All Tests", Section 17.3.0.2.2: "Sample Output for Client VT Info Tool Results—Failing Some Tests", and Section 17.3.0.2.3: "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

17.3.0.2.1 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

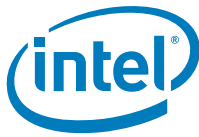
```
-----
Pass | 52
Fail | 00
Warn | 00
NA   | 05
Total | 57
-----
```

Note: Tests which do not apply to the system under test will not be shown in results but will be in NA.

17.3.0.2.2 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 will not be shown in results.

17.3.0.2.3 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(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 will not be shown in results.

17.3.1 Intel® VT-x Tests with Microsoft* Client Hyper-V* on Windows* 10

17.3.1.1 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**

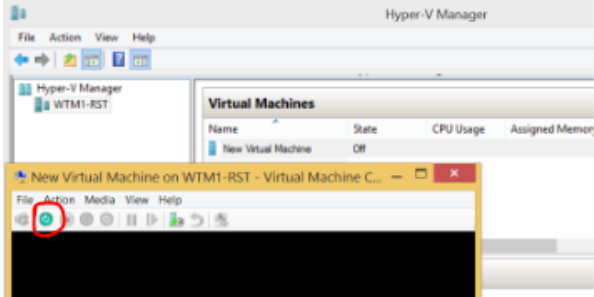
Note: Disabling TXT is just for test purposes.

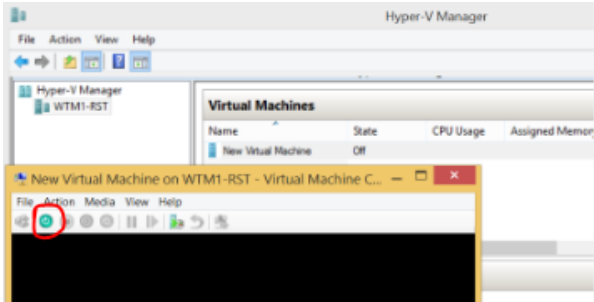
Tools for Testing:

— **Microsoft* Windows* 10 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* 10
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* 10 and open Client Hyper-V* Manager <p>Note: Refer to Section 17.3.1.2: "User Guide—Microsoft* Client Hyper-V* and Virtual Machine Enabling and Installation Instructions" for instructions on how to enable Client Hyper-V*.</p>
Test Pass/Fail Criteria:	Test passes when: Microsoft* Client Hyper-V* Manager Boots



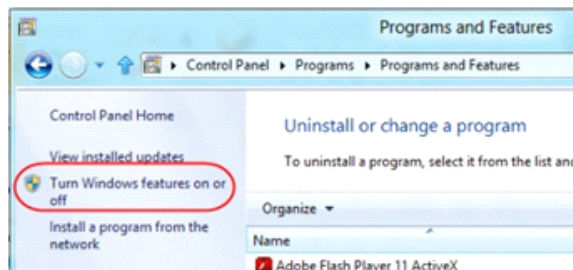
Test ID:	VT_TC02B
Test Case Title:	Verify Virtual Machine Boots in Microsoft* Client Hyper-V* Manager
Mandatory/Optional:	Mandatory
Description:	Microsoft* Client Hyper-V* uses Intel® VT to launch a virtual guest OS in Windows* 10 host OS.
Objective:	Verify Intel® VT-x implementation at platform level
Procedure:	<ol style="list-style-type: none">1. Enable Intel® Virtualization Technology (VT-x) in BIOS2. Boot to Windows* 10 and open Client Hyper-V* Manager3. Open virtual machine by double clicking on it. If it is not running, you can click on the start button.  <p>Note: Refer to Section 17.3.1.2.2: "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* 10 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 you are running Client Hyper-V* on a laptop and close the lid, the VMs that are running will be 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* 10 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* 10 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>

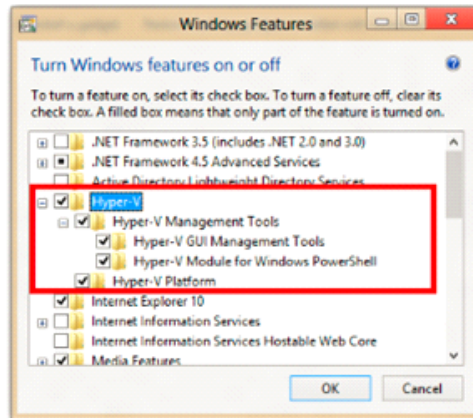
17.3.1.2 User Guide—Microsoft* Client Hyper-V* and Virtual Machine Enabling and Installation Instructions

17.3.1.2.1 How to Enable Microsoft* Client Hyper-V*

1. In the Windows* 10 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**.



Windows* searches for and installs the required files.

4. **Restart After Enabling or Disabling Microsoft* Client Hyper-V***

Note:

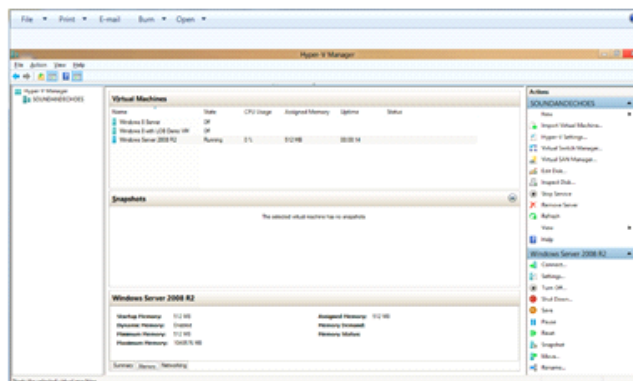
Enabling Client Hyper-V* installs Hyper-V* Manager. You will use Hyper-V* Manager to create and manage your virtual machines.

For more information on the Hyper-V* Manager user interface, go to <http://technet.microsoft.com/library/cc770494.aspx>.

17.3.1.2.2 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

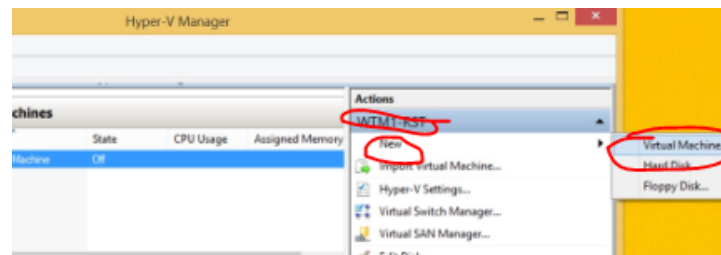
1. Open Hyper-V* Manager from Windows* Start screen (In Windows* 10 you may need to go to Start screen > Click arrow at bottom left > Hyper-V Management tools > Hyper-V Manager.)



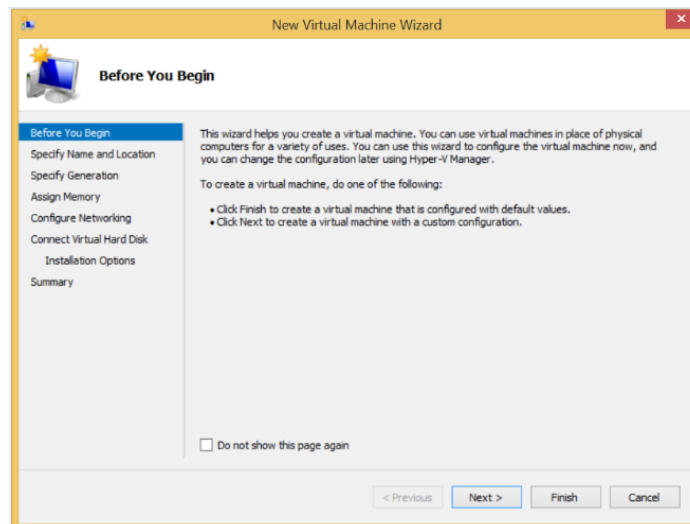
2. From the navigation pane of Hyper-V* Manager, select the computer name.



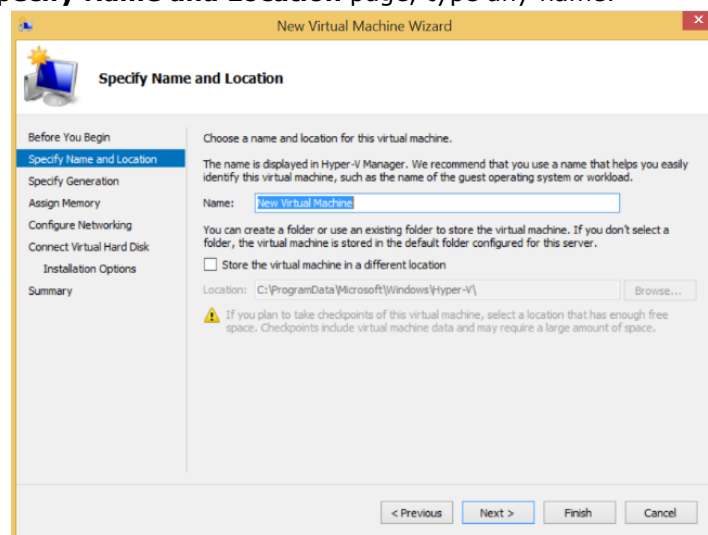
3. From the **Action** pane on the right side, click **New**, and then click **Virtual Machine**. The New Virtual



4. Machine wizard opens. Click **Next**.

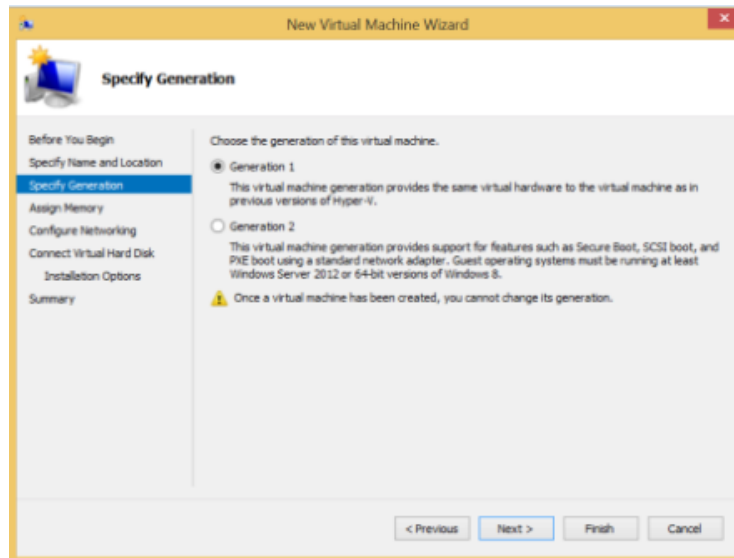


5. On the **Specify Name and Location** page, type any name.

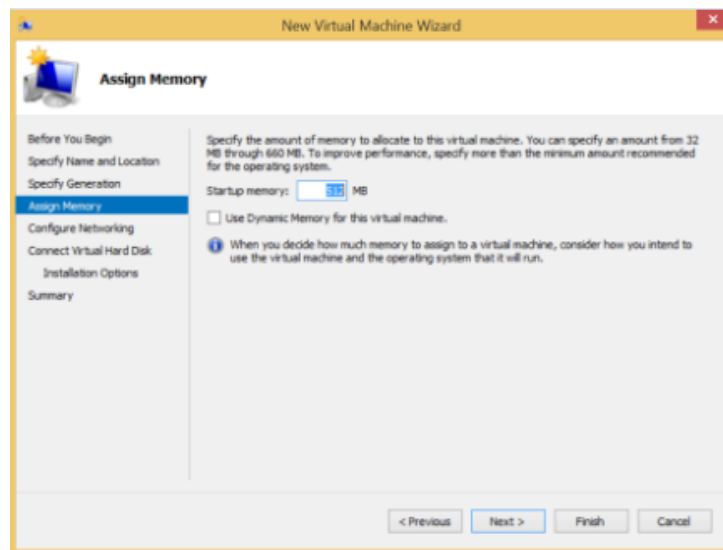


6. On the **Specify Generation** page, leave the default, Generation 1.

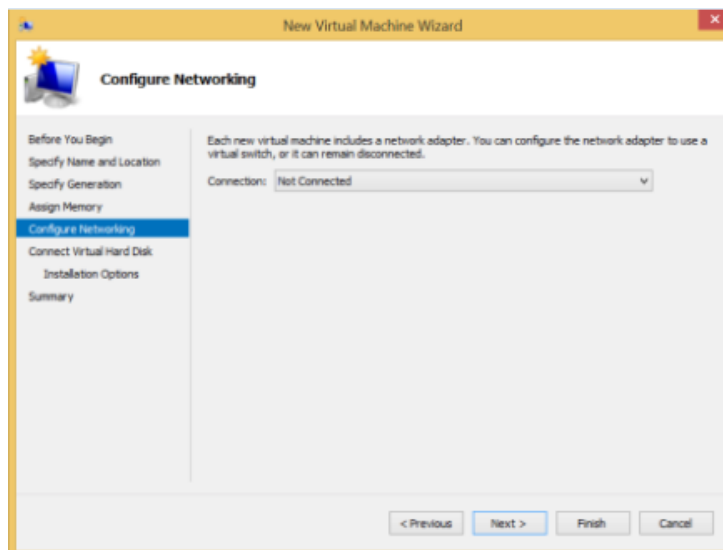
Note: Earlier versions of Client Hyper-V* may not have this step.



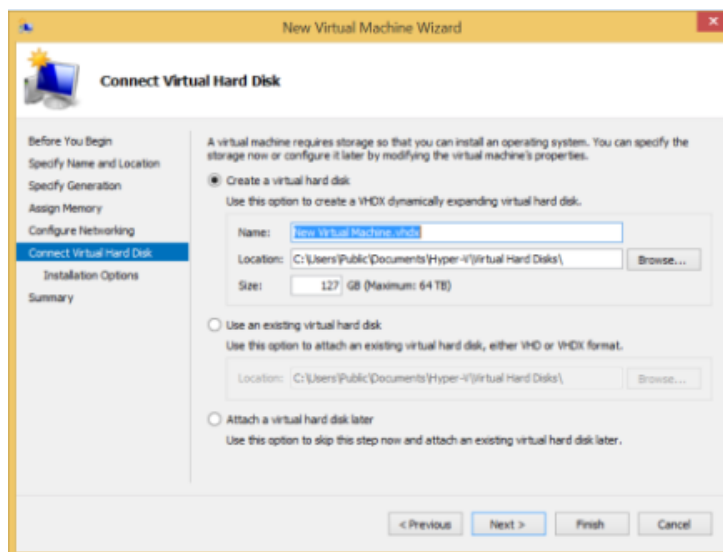
7. On the **Assign Memory** page, specify enough memory to start the guest operating system.

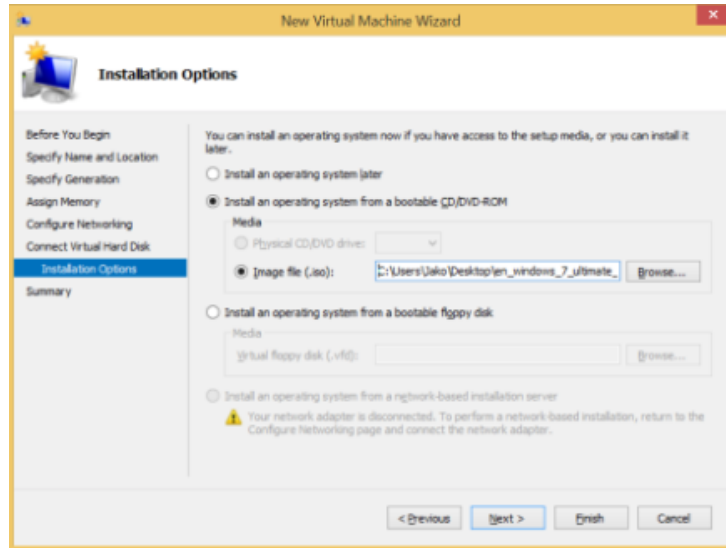


8. On the **Configure Networking** page, leave the default settings.



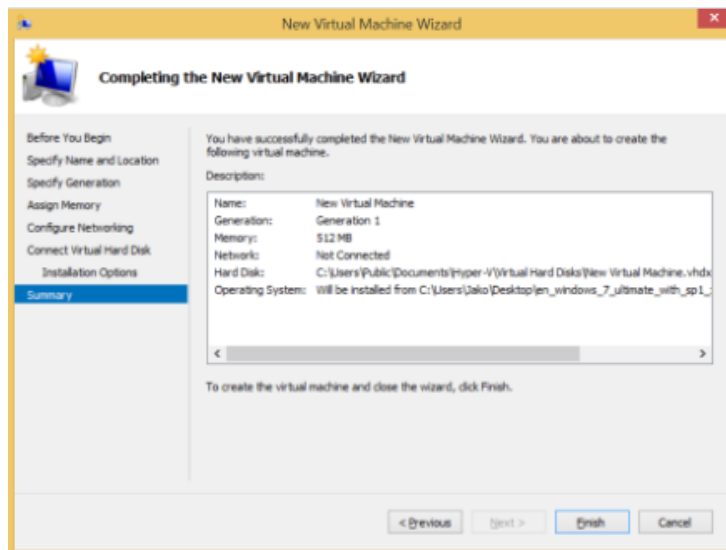
On the **Connect Virtual Hard Disk** and **Installation Options** pages, choose the option that is appropriate for how you plan to install the guest operating system: If you will install the guest operating system from a DVD or an image file (an ISO file), choose **Create a virtual hard disk**. Click **Next**, and then click the option that describes the type of media you will 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)**





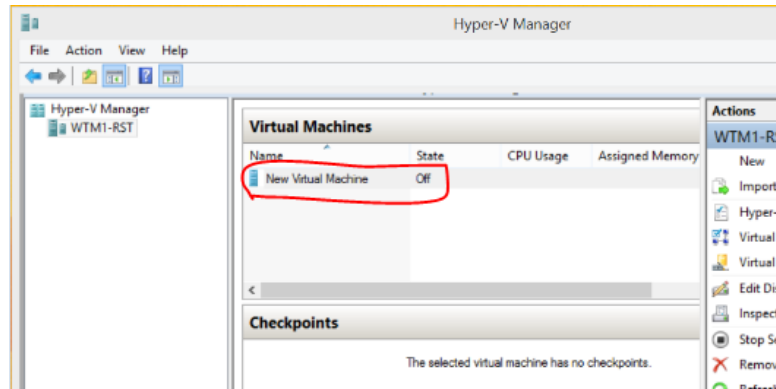
- g. If the guest operating system is already installed in a virtual hard disk, choose **Use an existing virtual hard disk** and click Next. (See figure at top of page). Then, choose **Install an operating system later**.

9. On the **Summary** page, verify your selections and then click **Finish**.

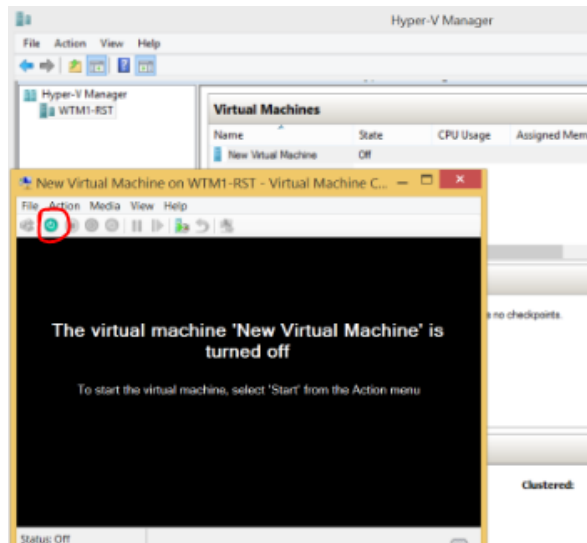




10. **Double Click** on your **Virtual Machine** to Open it.

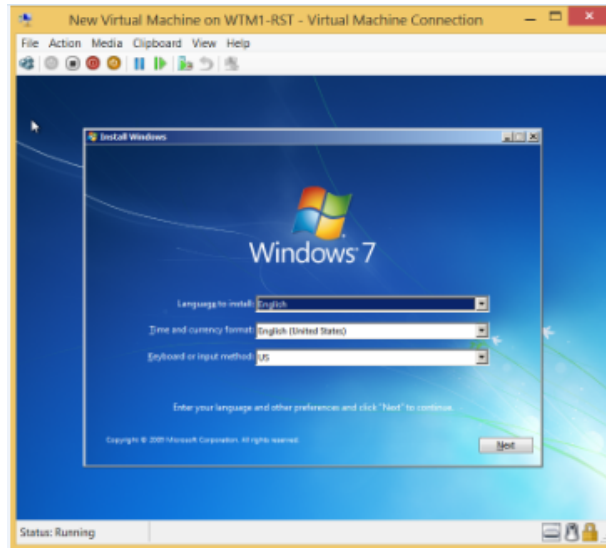


11. Click on the green **Start** button to run Virtual Machine

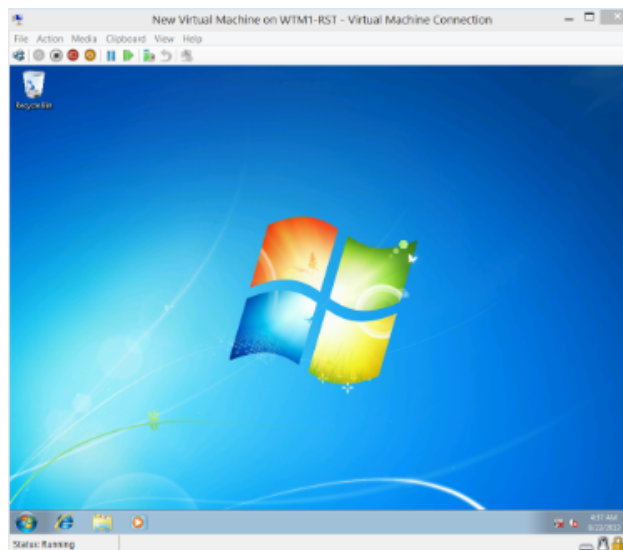




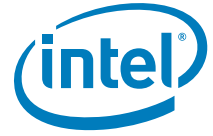
12. **Follow** normal OS Installation Instructions, this depends on OS you have chosen.



13. Once this is complete your Virtual Machine will look like a normal System inside the Virtual Machine Window.



17.3.2



(This page intentionally left blank.)





18 ISH Firmware (FW) Compliance

This section provides the ISH FW testing (performed by 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:

- The PDT Editor tool can be found in the ISH FW Kit.
- The Sensor Viewer Tool can be found in the ISH FW Kit.



18.1 Intel® ISH Firmware (FW) Compliance Test Coverage Summary

Test ID	Test Case Title	Target OS	Automated/ Manual	Mandatory/ Optional
ISS_TST_01	Sensor communication test	Windows*	PETS	Mandatory
ISH_TST_02	Sensor data check	Windows*	Manual	Mandatory
ISH_TST_03	ISH FW loading and execution	Windows*	Manual	Mandatory
ISH_TST_04	Intel® SensorViewer 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	Barometer (pressure) sensor sanity test	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 accuracy test with Second Accelerometer	Windows*	Semi-Automated (PETS)	Mandatory only if the second accelerometer is present
ISS_TST_12A	PLM functionality verification in S0	Windows*	Manual	Mandatory only if the second accelerometer is present
ISS_TST_12B	PLM functionality verification with power transitions	Windows*	Manual	Mandatory only if the second accelerometer is present
ISS_TST_13	Heading sensor accuracy and drift test	Windows*	Semi-Automated (PETS)	Mandatory only if a magnetometer sensor is present.
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_16	Sensor terminal 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



18.2 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 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 ISSUtil Tool: "ISSUtil.exe -BIST -test 0 -verbose" "ISSUtil.exe -BIST -test 1 -verbose" "ISSUtil.exe -BIST -test 2 -verbose" "ISSUtil.exe -BIST -test 3 -verbose"
Test Pass/Fail Criteria:	Test will pass if each of the tests were completed successfully without any errors.

18.3 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 those sensors information were configured correctly in PDT table.
Objective:	Check the sensor data in the PDT editor to make sure it is compliant with the board.
Windows* Procedure:	<p>Verify the sensors information in the PDT Editor:</p> <ol style="list-style-type: none"> 1. Open the full SPI image in the FITC tool. (Decompose it) 2. In the FITC tool folder, a folder will be 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 will be located under: FITC\image_name\Decomp\PdtBinary.bin. 4. In the PDT Editor, verify that each of the sensors configured with the rights settings.
Test Pass/Fail Criteria:	Test will pass if the sensors information were configured correctly in the PDT Editor.



18.4 ISH FW 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 the ISH FW can be read.
Objective:	Verify that ISH is responsive and that ISH FW can be read
Windows* Procedure:	<ol style="list-style-type: none">1. Boot the platform to AOS/WOS shell.2. From elevated command line run the ISSUtil Tool: ISSUtil.exe -INFO3. In the tool output check that:<ol style="list-style-type: none">a. ISH Status is "responding"b. ISH FW Version can be read and is as follow: "5.x.x.XXXX" (X- Stand for do not care)
Test Pass/Fail Criteria:	Test will pass if ISH status is "responding" and ISH FW can be read.

18.5 Intel® SensorViewer Test

Test ID:	ISS_TST_04
Test Case Title:	Intel® SensorViewer 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:	<ol style="list-style-type: none">1. Boot the platform to Windows*2. Open the Intel® SensorViewer and switch to "Desktop API" in Settings.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 Intel® SensorViewer.
Test Pass/Fail Criteria:	Test will pass if in the sensor viewer, all of the sensors state is "Ready" and the data is received for each of the sensors



18.6 Test System Sensors

18.6.1 Sensor Noise and Error Levels

Following is a table of sensor noise and error levels that will be monitored by some tests within the compliance guide. These numbers should be measured after calibration has been applied.

Table of measured values 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

Table of measured values from the IISS algorithms (static—no movement):

	Maximum Error	Average Error	STD
Inclinometer	2 deg	2 deg	0.75
3D Compass	2 deg	2 deg	0.75
3D Gyro	1.0 dps	1.0 dps	0.2 dps
3DAccelerometer	40 mg	40 mg	

Note: 3D Gyroscope and 3D Accelerometer values are "per axis"



18.6.2 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) will perform the following steps:</p> <ol style="list-style-type: none">1. Gather RAW and virtual sensor data over a designated period (i.e. 10s). Data will be 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 will pass 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 will refer 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 will raise a "warning" to the user.</p>



18.6.3 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) will perform the following steps:</p> <ol style="list-style-type: none"> The system will exercise known interference sources to see if they will 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 will gather 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"> The system will exercise known interference sources to see if they will have influences on the system. Data Should be gathered at each step. 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 will pass if all sequences show:</p> <ol style="list-style-type: none"> RAW sensor statistical data shows noise levels within acceptable ranges. Data output from sensor algorithms do not show movement or other performance issues when the system is at rest. <p>Note: For #1 and #2 - the tool will refer to the pass/fail levels placed in the section "Sensor Noise and Error Levels".</p> <p>Note: In the case that the test results are above the pass/fail limits - the tests will raise a "warning" to the user.</p>

18.7 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:	Optional. Mandatory if motion sensors are present
Description:	The data quality of the sensor algorithms can be impacted by a number of factors (e.g. 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)</p> <p>Initial state of the SUT should be S0.</p> <p>The system should have run through the ISS sensor calibration procedure with the calibration data stored and used on the system.</p> <p>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.</p> <p>The user will be 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 will pass if all sequences show for the gyroscope:</p> <p>The correct direction was recorded from the gyroscope when moving the system.</p> <p>Test will pass if all sequences show for the accelerometer:</p> <p>The accelerometer reading was correct within a 5 degree error.</p>



18.8 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 will confirm 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) 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"> Lift the system to a height of 1.5-2.0 meters. Wait 10 seconds. Place the system on the ground. Wait 10 seconds. <p>For each sample data sample - the system will gather RAW and virtual sensor data.</p>
Test Pass/Fail Criteria:	Test will pass if all sequences show: The pressure sensor recorded a change in altitude relative.

18.9 Light Sensor (ALS) Accuracy Test

Test ID:	ISS_TST_09
Test Case Title:	Light sensor (ALS) accuracy test
Mandatory/Optional:	Mandatory
Description:	This test will review the accuracy of the ambient light sensor after it has been characterized.
Objective:	<p>The ALS 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) 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"> Tunable light source that can emit halogen light. 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"> 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. 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. 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. (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:	Test will pass if all sequences show: For all light levels tested - the ALS is correct within +/- 10%.



18.10 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 will fall 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>
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. 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:	<p>Test will pass if all sequences show:</p> <p>The recorded light level of the ALS does not fall more than 50%.</p>



18.11 360 Hinge Accuracy Test with Second Accelerometer

Test ID:	ISS_TST_11
Test Case Title:	360 hinge accuracy test with 2nd accelerometer
Mandatory/Optional:	Optional. Mandatory if the 2nd accelerometer is present.
Description:	<p>Placing an accelerometer both in the base and lid of the system design will enable the system to determine the angle between the lid and base. This algorithm (also called a virtual protractor) will 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"> 0 degrees. Lid closed (screen facing keyboard). 90deg. Screen open and facing the user. Screen and keyboard are orthogonal with user seeing screen and keyboard at the same time. 180 degrees. Screen and keyboard both facing up. 270 degrees. Screen and keyboard are orthogonal. The user cannot see the screen and keyboard at the same time. 360 degrees. System flat on table. The screen is facing up and the keyboard is facing down.
Test Pass/Fail Criteria:	<p>Test will pass if all sequences show:</p> <p>The detected angle should be within a ± 10 degrees of accuracy.</p> <p>Over the 5 seconds, the variance of the angle should have been less than ± 5 degrees.</p>

18.12 PLM Functionality Verification

Test ID:	ISS_TST_12A
Test Case Title:	PLM functionality verification without system power transitions
Mandatory/Optional:	Optional. Mandatory if PLM is implemented
Description:	<p>Test will require 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.</p> <p>Note: PETS will read the PLM table configuration from the PDT Config file and will prompt the user to set system position according to the defined modes (First mode to test should be the last one that is configured in the PLM table)</p>



Test ID:	ISS_TST_12A
Objective:	To verify proper configuration and functionality of the PLM algorithm on customer system in S0
Procedure:	<ol style="list-style-type: none">1. PETS will ask the user to boot the system to OS.2. PETS prompt user to set the system in a first position according to the last PLM Mode configured in the PDT Config file. <p>Note: The following should be included in the message to the user: <i>a) Angle Range b) LCD Direction and its nick name (if implemented)</i></p> <ol style="list-style-type: none">3. User should manually acknowledge when the system is placed in the position as requested in previous step4. PETS will read PLM data and 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 will pass 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:	Optional. Mandatory if PLM is implemented
Description:	<p>Test will require to make system power transitions while going through the system modes as configured in the PDT Config file. User will be 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.</p> <p>Note: PETS will read the PLM table configuration from the PDT Config file and will prompt the user to set system position according to the defined modes (First mode to test should be the last one that is configured in the PLM table).</p>
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. PETS will ask the user to boot the system to OS.2. PETS prompt user to set the system in a first position according to the last PLM Mode configured in the PDT Config file. <p>Note: The following should be included in the message to the user: <i>a) Angle Range b) LCD Direction and its nick name</i></p> <ol style="list-style-type: none">3. User should manually acknowledge when the system is placed in the position as requested in previous step4. PETS will read PLM data and verify if the actual system position reported by the PLM algorithm is aligned to what user confirmed.5. PETS will ask the user to change the system state to S36. PETS prompt user to set the system in the next position according to the last PLM Mode configured in the PDT Config file. <p>Note: the following should be included in the message to the user: <i>a) Angle Range b) LCD Direction and its nick name (if Implemented)</i></p> <ol style="list-style-type: none">7. User should manually acknowledge when the system is placed in the position as requested in previous step8. PETS will ask the user to wake the system to OS/S09. PETS will read PLM data and 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 will pass only if all PLM Modes are matching the actual system position. i.e. all PLM Modes are successfully matched.



18.13 Heading Sensor Accuracy and Drift Test

Test ID:	ISS_TST_13
Test Case Title:	Heading sensor accuracy and drift test
Mandatory/Optional:	Optional. Mandatory if a magnetometer sensor is present.
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)</p> <p>Initial state of the SUT should be S0 (OS up). The ISS should be configured in the system FW.</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>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) will perform the following steps:</p> <p>Test System Flat on Table (Z-UP)</p> <p>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 90 degrees from north 3. Rotate the system to 180 degrees from north 4. Rotate the system to 270 degrees from north 5. Rotate the system to face 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:	<p>Test will pass if all sequences show:</p> <p>System heading error should not exceed 10 degrees at any rest position.</p>



18.14 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.
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 + DC2. Resume from S3 on DC3. Resume from S4 on AC + DC4. Resume from S4 on DC5. Resume from S5 on AC + DC6. Resume from S5 on DC7. Resume from DeepS3* (Optional if FW image supports DeepSx)8. Resume from DeepS4* (Optional if FW image supports DeepSx)9. Resume from DeepS5* (Optional if FW image supports DeepSx)10. Resume from G3 on AC + DC11. Resume from G3 on DC12. Resume from G3 with no coin battery (if coin battery exists)13. Resume after system reset (cold reset, HW RST button)14. 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 ISSUtil tool ("ISSUtil.exe -BIST -test 3").</p>
Test Pass/Fail Criteria:	<p>Test will pass 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 will return a warning to the user.</p>



18.15 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 will confirm if the sensor activity contexts algorithms within the IISS are working properly.</p>
Objective:	Confirm that the system will detect the system user activity contexts.
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. If the system is a 2-in-1 system start in the tablet form factor.</p> <ol style="list-style-type: none"> 1. Leave the SUT on desktop and wait for 5 minutes. The system should detect that the system is sedentary. 2. Pick up the SUT and begin walking with it. The system should detect that you are walking with the system. 3. Start lightly running with the SUT. The system should detect that you are running with the system.
Test Pass/Fail Criteria:	<p>Test will pass if all sequences show:</p> <p>The system accurately detected the user contexts.</p>

18.16 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:	<p>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 will confirm if the sensor terminal contexts algorithms within the IISS are working properly.</p>
Objective:	Confirm that the system will detect the terminal contexts.
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. 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:	<p>Test will pass if all sequences show:</p> <p>The system accurately detected the terminal contexts.</p>

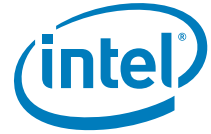


18.17 Sensor Gesture Contexts

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 will confirm if the sensor gesture contexts algorithm within the IISS are working properly.
Objective:	Confirm that the system will detect the system user gesture contexts.
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. If the system is a 2-in-1 system start in the tablet form factor.</p> <ol style="list-style-type: none">1. Lift the system from the table and look at the system.
Test Pass/Fail Criteria:	<p>Test will pass if all sequences show:</p> <p>The system accurately detected the terminal contexts.</p>

18.18 Wake on Shake Test

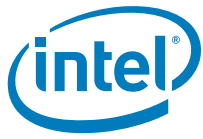
Test ID:	ISS_TST_18
Test Case Title:	Wake on shake test
Mandatory/Optional:	Mandatory
Description:	Wake on different events is a mandatory feature in Win10. As such a test that will focus on the ability to wake the system from S0i3 (CS) is a must.
Objective:	Test that ISH can send a wake event to Win OS and the OS waken 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 will go 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:	Test will pass if Windows* awakes all 3 times



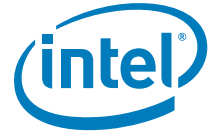
18.19 Step Counting Test

Test ID:	ISS_TST_19
Test Case Title:	Step counting test
Mandatory/Optional:	Optional, 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
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 will start acting of 10 seconds of stepping, so tests that will take 10 seconds or will 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.

§ §



(This page intentionally left blank.)



19 Intel® Software Guard Extension (Intel® SGX)

19.1 Introduction

Intel® Software Guard Extension (Intel® SGX) Technology is a CPU based capability that allows applications 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 on [CCL](#). 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.

19.2 Intel® Software Guard Extension (Intel® SGX) Compliance Test Coverage Summary

OS Support', and 'How?' Columns 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.

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

Network Factor: 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	How?	Intel® PETS Package Name	OS Support	Form Factor
SGX_001	SGX Enabled	I	Compliance_SGX.xml	W WI	D M HEDT
SGX_002	SGX Disabled	I	Compliance_SGX.xml	W WI	D M HEDT
SGX_003	SGX SW Controlled	I	Compliance_SGX.xml	W WI	D M HEDT
SGX_004	Memory Allocation	I	Compliance_SGX.xml	W WI	D M HEDT
SGX_005	SGX Functionality	I	Compliance_SGX.xml	W WI	D M HEDT
SGX_006	EPID/PSE Provisioning	I	Compliance_SGX.xml	W WI	D M HEDT

19.3 SGX Tests

19.3.1 SGX Enabled

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"> In BIOS, Select SGX Enabled option. Boot to Windows 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. Verify in file "SgxBIOSInfoToolOutput.txt" (under same directory) result as SGX enabled. Reboot. Perform b-d again. Perform S3, resume. Run c-d again. Perform S4, S5. Run b-d again.
Test Pass/Fail Criteria	Result is verified as SGX enabled in the "SgxBIOSInfoToolOutput.txt" file.



19.3.2 SGX Disabled

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:	a. In BIOS, Select SGX Disabled option. b. Boot to Windows c. 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. d. Verify in file "SgxBIOSInfoToolOutput.txt" (under same directory) result as SGX disabled. e. Reboot. f. Perform b-d again. g. Perform S3, resume h. Run c-d again. i. Perform S4, S5. j. Run b-d again.
Test Pass/Fail Criteria:	Result is verified as SGX disabled in the "SgxBIOSInfoToolOutput.txt" file.

19.3.3 SGX SW Controlled

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:	a. In BIOS, Select SGX SW Controlled option. b. Boot to Windows c. 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. d. Verify in file "SgxBIOSInfoToolOutput.txt" (under same directory) result as SGX disabled. e. Reboot. f. Perform b-d again. g. Perform S3, resume. h. Run c-d again. i. Perform S4, S5. j. Run b-d again.
Test Pass/Fail Criteria:	Result is verified as Intel® SGX SW Controlled in the "SgxBIOSInfoToolOutput.txt" file.



19.3.4 Memory Allocation

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:	<ul style="list-style-type: none">a. boot to UEFI shellb. run memmapc. check that the range reported in the MSR is marked as reserved/hardware reserved.d. 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.

19.3.5 SGX Functionality

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:	<ul style="list-style-type: none">a. set SGX as enabled in BIOSb. Install the SGX SW (if not already installed, can be found on VIP)c. Install the full MEI SW package. (if not already installed, can be found on VIP)d. 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 will be necessary to run the command several timese. check the SgxFunctionalValidationToolOutput.txt for failures
Test Pass/Fail Criteria:	SgxFunctionalValidationToolOutput.txt should give a 'pass/fail/' result.



Figure 19-1. Intel® SGX Functional validation tool pass result example

```

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
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

SGX functionality has been verified.
-----

```

19.3.6 EPID/PSE Provisioning

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:	<ul style="list-style-type: none"> a. set SGX as enabled in BIOS b. Connect platform to the Internet via LAN/WiFi c. 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". d. check the CMD for failures
Test Pass/Fail Criteria:	SgxFunctionalValidationToolOutput.txt should give a 'pass/fail/ result.

**Figure 19-2. Functional validation tool provisioning pass result example**

```
C:\> 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

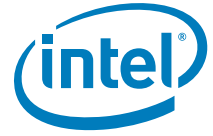
Starting PSE provisioning.....
Successfully completed PSE provisioning.

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 t
SUCCESS: Tried to Provision the PSE in the system under test (Note: Internet connectivity is required
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.
-----
```

§ §



(This page intentionally left blank.)



20 Enhanced Serial Peripheral Interface (eSPI)

20.1 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.

20.2 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.

20.3 Tools for Testing

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

20.4 eSPI Compliancy Test Coverage Summary

Operating System Support and How? Columns 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?
eSPI_001	Booting 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 Support	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

20.5 Booting with MAF Configurations (Straps set to MAF Defaults)

Test ID:	eSPI_001
Test Case Title:	Booting 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"> 3. Follow Intel® SPI Programming Guide and review all soft straps applicable to MAF 4. Build IFWI with default straps for MAF using Intel® FIT 5. Flash IFWI onto the platform 6. Check that platform boots to OS

20.6 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

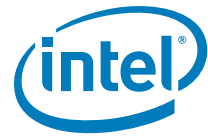


20.7 Platform Boots with EC Region in Different Place

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

20.8 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



20.9 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 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

20.10 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

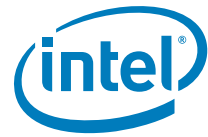


20.11 Platform Boots with Default EC Region Permissions

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® FIT2. Flash IFWI onto the platform3. Boot platform to OS4. Run Intel® FPT -closemnf EC5. Run Intel® MEManuf -EOL6. Make sure that Intel® MEManuf -EOL check passes

20.12 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 will be 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:<ul style="list-style-type: none">• EC read access should have a value of 0x103 in Intel® FIT2. Flash IFWI onto the platform3. Boot platform to OS4. Run Intel® FPT -closemnf EC5. Run Intel® MEManuf -EOL6. Make sure that Intel® MEManuf -EOL check passes



20.13 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 will be 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: <ul style="list-style-type: none"> • EC read access should have a value of 0x103 in Intel® FIT • Host CPU/BIOS read access should have a value of either 0x10F or 0x11F • Host CPU/BIOS write access should have a value of either 0x10A or 0x11A 2. Flash IFWI onto the platform 3. Boot platform to OS 4. Run Intel® FPT -closemfn EC 5. Run Intel® MEManuf -EOL 6. Make sure that Intel® MEManuf -EOL check passes

20.14 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 will work 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 to the System Tools User Guide for more information on the FWUpdate flow. 3. Verify that platform can boot to OS after FWUpdate is completed.

§ §



(This page intentionally left blank.)