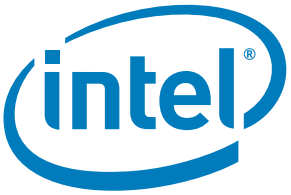


Tiger Lake Platform Intel® Converged Security and Management Engine (Intel® CSME) 15.0 and Intel® Sensor Solution Consumer Firmware

Compliance and Testing Guide

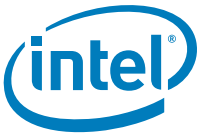
Revision 0.8

April 2020

Intel Confidential

Document Number: 613800

Contents



Figures

Tables

Revision History

Document Number	Revision Number	Description	Revision Date
613800	0.5	• Initial release.	July 2019
	0.6	• **Removed Intel® SGX Compliancy Chapter** • **Intel® Trace Hub Compliancy** — Removed test ITH_003 "BIOS - DCI Enable Post EOM" • **Intel® CSME BIOS Compliancy** — Updated terminology for the manufacturing/re-manufacturing environment. • **Intel® CSME Manufacturing or Re-Manufacturing Environment Compliancy—Consumer** — Updated terminology for the manufacturing/re-manufacturing environment. • **Intel® CSME Power Management for Consumer Designs** — Updated XML needed for test ME_PM_27 — Updated FWSTS value in test ME_PM_26.9 • **Intel® CSME Power Management for Consumer Designs—Stress Testing** — Added additional step in stress flow compliance guide test cases to check if there is any flash log in system. • **Intel® ICC Compliancy** — removed Intel® CCT usage and updated with Intel® ICC SDK usage.	November 2019
	0.7	• **Added Chapter 8, "Intel® CSME Resiliency Compliancy".** • **Chapter 11, "Intel® CSME Power Management for Consumer Designs Stress Testing":** — Updated tests PM_ST_31,32. • **Intel® ICC Compliancy:** — Added a note for the support of Over Clocking Profiles. • **Platform Controller Hub (PCH) SoftStrap Configuration:** — Added additional offset changes for A1 stepping PCH. — Corrected offset for USB3 / PCIe* Combo Port 3.	January 2020
	0.8	• **Added Chapter 21, "Platform SKU Emulation Check"** • **Chapter 10, "Intel® CSME Power Management for Consumer Designs":** — Decreased PG check time from 3 minutes to 1 minute. • **Chapter 18, "Platform Controller Hub (PCH) Soft Strap Configuration":** — Removed Test PSS_005. — Added USB3 and SATA combo port tests for static disable. — Updated TPM frequency encoding to 48 MHz value.	April 2020

§ §

1 Introduction

1.1 Purpose and Scope

The Intel® Converged Security and Management Engine (Intel® CSME) and Intel® Sensor Solution Consumer Compliance Guide for Tiger Lake Platforms are designed to provide original equipment and device manufacturers with the compliancy requirements for the platform implementation. 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, and AIO **form factors** only, and supports Windows* 10 Operating System.

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 Intel® CSME Firmware General Notes

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 guarantied, 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* 8.1/10 Fast Startup (Partial Hibernate)

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

1.3.3 Environment Networking Recommendations

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. For example—If your 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.

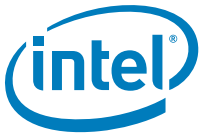
1.5 Acronyms, Definitions, and Terminology

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 KBC (Keyboard Controller)
USB-R	Integrated Device Electronics-Redirect
Intel® MEI	Intel® Management Engine Interface
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
SPI Flash Programming Guide	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 and http://xen.org/download/index.html
Intel® TXT – Trusted Boot Checkout Kit	TBD
EFI shell (DUET – FAT32)	http://developer.intel.com/technology/efi/agreesource.htm
Cannon Lake Platform Controller Hub (PCH) LP External Design Specification (EDS)	TBD
Intel® Trusted Execution Technology (Intel® TXT) - Trusted Platform Module (TPM) Nonvolatile (NV) Storage Interface Usage – Application Note	420735
Intel® CSME 15 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® Platform Enablement Test Suite User Guide	Located in Intel® Compliancy Kit
Intel® APS Setup and Configuration Guide for OEMs	Located in Intel® Compliancy Kit
Intel® Automated Power and System State Test Device (Intel® APS) User's Guide for OEMs	Located in Intel® Compliancy Kit
Intel® AMT Tools User Guide	Located in Intel® Compliancy Kit

1.7 External References

Document	Location
IEEE 802.11a Specification	http://standards.ieee.org/wireless
IEEE 802.11b Specification	http://standards.ieee.org/wireless
IEEE 802.11g Specification	http://standards.ieee.org/wireless
IEEE 802.11d Specification	http://standards.ieee.org/wireless
IEEE 802.11e Specification	http://standards.ieee.org/wireless
IEEE 802.11h Specification	http://standards.ieee.org/wireless
IEEE 802.11i Specification	http://standards.ieee.org/wireless

Document	Location
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 testing 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 Control Panel -> System -> Hardware -> Device Manager -> (select network adapter) -> Properties –> Advanced. Change **Enable PME** to **enabled.**

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

The following table shows the configuration information for the Intel® 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 Intel® Boot Guard and Intel® PTT chapter for actual compliancy tests.

Definitions:

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

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

Platform 2016[1]	Intel® Active Client Manager (Intel® ACM)	Intel® CSME Firmware	Intel® PTT	TPM 1.2	TPM 2.0
TGL Based (1-Chip and 2-chip)	Intel® ACM 3.x	Consumer	Yes	Yes	Yes
		Corporate Intel® vPro®	Yes[2]	Yes	Yes

Notes:
1. Refer to platform dashboard for POR configurations.
2. Refer to Intel® PTT documentations for vPro® compatibility.

§ §

2 Intel® Trace Hub (Intel® TH)

This chapter serves as a checklist for the environment setup of Intel® 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 Get started html , System Trace User Guide and DCI user guide located at *"C:\IntelSWTools\system_studio_2019_nda_xxxx\documentation_2019\en\debugger\system_studio_2019_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 Bringup Guide for more details on image creation.

2.1 Intel® Trace Hub Compliancy Test Coverage Summary

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

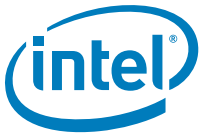
Test ID	Test Case Title	PETS/Manual	Form Factor
ITH_001	Intel® CSME FW - DCI Enable (MEEN)	Manual	D M A W
ITH_002	BIOS - DCI Enable (HEEN)	Manual	D M A W
ITH_004	Capture ITH BIOS/ME Tracing Via CCA	Manual	D M A W

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 or re-manufacturing environment, DCI interface can be enabled through Intel® CSME FW (MEEN).
Objective	To enable DCI through Intel® CSME
Procedure	1. Install Intel® System Debugger which supports your platform on your console. 2. Flash the full DCI enabled image on to the platfom 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. Open Intel® System Debugger. Use a fresh workspace and open a new Intel system trace project to configure the trace project for SUT. Refer to System Trace user Guide for more details. 7. Click **Connect** and ensure that DCI is connected without errors
Test Pass/Fail Criteria	Test passes if we are able to connect to the target over DCI and the following message is displayed in the console: 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

2.3 BIOS - DCI Enable (HEEN)

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



Test ID	ITH_002
Objective	To enable DCI through BIOS
Procedure	1. Install Intel® System Debugger which supports your platform on your console. 2. Flash the full DCI disabled image on to the platform. 3. Boot to BIOS and ensure that Host DCI Enable (HEEN) is set to Enabled, Refer to Document# 558380 for BIOS implementation details. 4. Connect the target end of the CCA to a USB3 port on the target and connect the host end of the CCA to a host with Intel® System Studio NDA software installed. 5. Open Intel® System Debugger. Use a fresh workspace and open a new Intel system trace project to configure the trace project for SUT. Refer to System Trace user Guide for more details. 6. Click **Connect** and ensure that DCI is connected without errors
Test Pass/Fail Criteria	Test passes if we are able to connect to the target over DCI and we are able to see the following message in the console: 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

2.4 Capturing 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	1. Flash image that has DCI and Intel® 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 OpenIPC software installed. 3. Open Intel® System Debugger. Use a fresh workspace and open a new Intel system trace project to configure the trace project for SUT. Refer to System Trace user Guide for more details. 4. Check CSME and BIOS for the trace source. ***Note:*** Selecting BIOS is optional, if the BIOS does not support trace messages over Intel® Trace Hub. 5. Click the green button to connect to the target on the Target Connection tab. 6. Click Play to start the trace in the Trace Capture tab. 7. Restart the target with the restart option from windows* menu. 8. check if we are able to collect BIOS and Intel® CSME logs in the STT and the messages are time correlated. 9. Shut down target by selecting shutdown option from windows* menu 10. Power on the target to boot from S5 to S0 state 11. check if we are able to collect BIOS and Intel® CSME logs in the STT and the messages are time correlated. 12. Put the target to standby mode (S3) 13. Resume the target to boot from standby by pressing the Power Button 14. check if we are able to collect BIOS and Intel® CSME logs in the STT and the messages are time correlated. 15. Execute a cold reset by writing 0xE to CF9 register (mm CF9 0xE -io) 16. check if we are able to collect BIOS and Intel® CSME logs in the STT and the messages are time correlated. 17. Execute a warm reset by writing 0x6 to CF9 register (mm CF9 0x6 -io) 18. check if we are able to collect BIOS and Intel® CSME logs in the STT and the messages are time correlated.
Test Pass/Fail Criteria	The test passes, if user is able to collect BIOS and Intel® CSME logs in the STT and the messages are time correlated.

§ §

3 Signing and Manifesting Compliance

This chapter includes tests to verify that OEMs are able to sign and manifest OEM components part of the SPI images. This involves creating OEM KM and placing the appropriate Public Key hashes.

3.1 Test Environment Setup

ICL Signing and Manifesting documentation can be found in Intel® CSME FW kit that contains all the necessary details pertaining to OEM component signing.

3.2 Tools for Testing

Intel® MEU (Intel® Manifest Extension Utility): Tool used to manifest OEM Components

OpenSSL: Freeware, can be found in Open source community. This tool integrates with MEU for signing the manifested components.

Intel® FIT (Intel® Flash Image Tool): Tool used to stitch FW image, can be found in Intel® CSME FW kit.

Intel® FPT (Intel® Flash Programming Tool): Used to burn images on SPI platforms, and set EOM state.

3.3 Signing and Manifesting Coverage Summary

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

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

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

Test ID	Test Case Title	PETS Package Name	OS Support	Platform	Form Factor	How?
SIGN_01	OEM KM not enabled	N/A	W WI	TGL	All	M
SIGN_02	OEM KM enabled	N/A	W WI	TGL	All	M

3.4 Non-Signed Image Creation

Test ID	**SIGN_01**
Test Case Title	OEM KM not enabled
Objective	This test verifies that OEMs are able to create a non-signed IFWI image (i.e. not enabling OEM KM), and successfully bring up the platform.
Test Pass Criteria	Platform boots to OS and ISH/iUnit/aDSP (Audio) are enabled and operational if used. For example on ISH, this could be achieved by confirming the following test passes: ISS_FW_02 (refer section 20.4 ISH FW Loading and Execution)
Mandatory/ Optional	Optional
Description	OEM would not sign OEM-provided binaries in the IFWI image nor input OEM KM binary. **Important Note**: The OEM KM is optional. OEMs who do not wish to use the OEM KM may keep out the OEM KM binary. By excluding or including OEM KM binary, the given platform is **permanently** set to require/not-require OEM KM per the configuration set in FIT. This choice is **permanently committed** to FPF HW at the time the platform undergoes closemnf/end-of-manufacturing process. This cannot be reversed after closemnf/EOM. This is done by an FPF value called OEM_KM_Presence. This FPF value can be viewed by MEInfo.
Windows* Procedure	***Note:*** For below procedure, if you are not building image from scratch but decomposing already built image, refer to System Tools User Guide found in Intel® CSME FW kits (Decomposing an Existing Flash Image). Once image is decomposed, follow the below procedure in FIT: Manual procedure. 1. Using CSME FW Bring Up guide (found in CSME FW kit), create and SPI image with ISH, iUnit and aDSP Intel signed binaries. a. Do not create OEM KM binary and do not include in Intel® FIT: In Intel® FIT, under Platform Protection tab/xml, do not include the following: — OEM Key Manifest Binary 2. Burn SPI image on the platform. 3. Verify that the platform boots to the OS and confirm ISH/iUnit/aDSP are enabled and operational.

3.5 Signed Image Creation

Test ID	**SIGN_02**
Test Case Title	OEM KM enabled
Objective	This test verifies that OEMs are able to sign and manifest OEM components that are authenticated by OEM KM
Test Pass Criteria	Platform boots to OS and the enabled OEM components (ISH/iUnit/Audio) are verified and operational. For example on ISH, this could be achieved by confirming the following test passes: ISS_FW_02 (refer section 20.4 ISH FW Loading and Execution)
Mandatory/ Optional	Optional
Description	OEM sign all OEM binaries such as ISH, iUnit, aDSP (Audio FW) and create SPI image with OEM KM containing all the necessary keys that authenticate these components. **Important Note**: The OEM KM is optional. OEMs who do not wish to use the OEM KM may keep out the OEM KM binary. By excluding or including OEM KM binary, the given platform is **permanently** set to require/not-require OEM KM per the configuration set in FIT. This choice is **permanently committed** to FPF HW at the time the platform undergoes closemnf/end-of-manufacturing process. This cannot be reversed after closemnf/EOM. This is done by an FPF value called OEM_KM_Presence. This FPF value can be viewed by MEInfo.

Windows* Procedure	Manual procedure:
	
	1. Create pairs of keys for signing OEM-provided binaries, using OpenSSL. Details of procedure are in the TGL Signing and Manifesting Guide, chapter 5.
	2. Create OEM KM with the appropriate OEM components per the platform design, refer chapter 7 of ICL Signing and Manifesting Guide.
	  a. 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.
	3. Use MEU to manifest and sign the OEM Key Manifest. Details of procedure are in the TGL Signing and Manifesting Guide, chapter 7.
	4. Use MEU to sign (or resign if necessary) each OEM binary whose hash has been entered into the OEM Key Manifest.
	5. In FIT, enter the following:
	  a. The public key hash of the OEM Key Manifest key
	  b. The OEM Key Manifest binary
	6. Use FIT to build an SPI image including the OEM Key Manifest. Details of procedure are in the TGL Signing and Manifesting Guide, chapter 8.
	7. Burn the IFWI image to the platform.
	8. Verify that the platform boots to the OS and confirm ISH/iUnit/aDSP are enabled and operational.

§ §

4 Intel® CSME BIOS Compliancy

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

Test Environment for Intel® CSME BIOS Compliancy Section:

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

Tools for testing:

- **Intel® Platform Enablement Test Suite**: Latest version of the tool is available in Intel® CSME Compliancy kit release. Refer to the *Intel® Platform Enablement Test Suite User Guide* available in the Intel® CSME Compliancy Kit for exact instructions on how to load and setup the Intel® Platform Enablement Test Suite software.

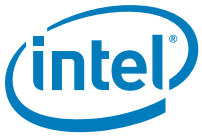
4.1 BIOS Compliancy Test Coverage Summary

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

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

Test ID	Test Case Title	PETS/Manual	Form Factor	Network
BIOS_01	End of POST	PETS/Manual	D M A	LAN+WLAN; WLAN only
BIOS_02	CF9GR locking/unlocking— non Manufacturing/Re-manufacturing Environment	PETS/Manual	D M A	LAN+WLAN; WLAN only
BIOS_03	DRAM INIT Done	PETS/Manual	D M A	LAN+WLAN; WLAN only

Note: BIOS_04 belongs to "Intel® CSME Manufacturing or Re-manufacturing Environment" Compliance Chapter.



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

Test ID	**BIOS_01**
Test Case Title	End of POST
Mandatory/Optional	Mandatory
Description	When the system completes POST that BIOS is required to send an "End of POST" message to the Intel® CSME by means of the Intel® MEI when the system is transitioning from S4/S5 to S0.
Objective	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. If the system is in the Intel® CSME flash protection mode, END_OF_POST message is optional. ***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 flash protection mode. For shipping machine, HFSTS at PCI address space at PCH B0:D22:F0 register offset 40h [bit 4] has to be '0'.
Procedure	1. Boot the system under test to OS. 2. Intel® Platform Enablement Test Suite performs the following: a. For each of the following system transitions: 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]. i. If [bit 4] is equal to '0', it means it's not in the Intel® CSME flash protection mode. ii. If [bit 4] is equal to '1', it means it's in the Intel® CSME flash protection 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 flash protection mode. If the system is in the Intel® CSME flash protection 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/Re-manufacturing Environment
Mandatory/Optional	Mandatory
Description	When the system is not in the manufacturing/re-manufacturing environment, 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 flash protection mode). ***Note:*** The recommended allocation of PWRMBASE is 0xFE000000 in PCH BIOS Specification.
Procedure	1. Manually read the PCI address space to verify the Intel® CSME Flash Protection 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 Flash Protection 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	For each of the following system transitions: G3 -> S0 (CM-Off->CM0) S5 -> S0 (CM-Off->CM0) S4 -> S0 (CM-Off->CM0) 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.
Test Pass/Fail Criteria	Test passes if the Intel® CSME transitions to CM0 with UMA for the system transitions listed above[1].

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

§ §

5 Intel® CSME Manufacturing or Re-Manufacturing Environment Compliancy

This 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 Flash Protection Mode.

The tests in this section verify that certain BIOS operations are *not* performed when the Intel® CSME is in Manufacturing/ Re-manufacturing Environment.

Test Environment for Intel® CSME BIOS Compliancy section:

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

Tools for Testing:

- **Intel® Platform Enablement Test Suite (Intel® PETS)**: Latest version of the tool is available in 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.
- Compliance_MeBios_ManufacturingMode.xml package should be loaded to Intel® Platform Enablement Test Suite in order to complete this section.

5.1 Manufacturing Mode Compliancy Test Coverage Summary

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

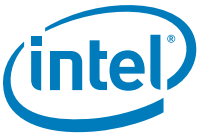
Network:
LAN = systems with LAN interface and test is performed using LAN interface
WLAN = systems with WLAN interface and test is performed using the WLAN interface

Test ID	Test Case Title	PETS/ Manual	Form Factor	Network Factor
BIOS_04	CF9GR locking/unlocking - Manufacturing/ Re-Manufacturing Environment	PETS	D M A	LAN+WLAN; WLAN only

5.2 CF9GR Locking/Unlocking

Test ID	**BIOS_04**
Test Case Title	CF9GR locking/unlocking—Manufacturing/ Re-Manufacturing Environment
Mandatory/Optional	Mandatory
Description	When the system is in the Intel® CSME Manufacturing/ Re-Manufacturing Environment, 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/re-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	1. Boot the system under test to OS. 2. Intel Platform Enablement Test Suite performs the following: a. Manually read the PCI address space at PCH B0:D22:F0 register offset 40h [bit 4] to verify the Intel® CSME Flash Protection 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 Flash Protection Mode.

§ §



6 SPI Flash Interface

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

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

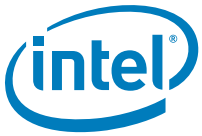
Test ID	Test Case Title	PETS/Manual	Form Factor	Network Factor
SPI_001	Descriptor Mode Test	PETS	DT/MB	LAN+WLAN; WLAN only
SPI_002	Serial Flash Discoverable Parameter Test	PETS	DT/MB	LAN+WLAN; WLAN only
SPI_003	4 Kbytes Erasable Blocks Test	PETS	DT/MB	LAN+WLAN; WLAN only
SPI_004	SPI Flash Size Test	PETS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

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	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	1. Boot to target OS. 2. Does flash device 0 in the SUT supports SFDP? a. If Yes, — Verify that the Component Property Parameter Table Valid (CPPTV) bit 31 of the Vendor Specific Component Capabilities 0 register (VSCC0[4]) is set to 1b. b. If No, — 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 Read[3]. 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). a. 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? a. If Yes, — Verify that the Component Property Parameter Table Valid (CPPTV) bit 31 of the Vendor Specific Component Capabilities 1 register (VSCC1[4]) is set to 1b. b. If No, — 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 Read[3]. ***Notes:*** 1. VSCC0 register is located at (VTBA[4] + C4h). 2. VSCC1 register is located at (VTBA[4] + 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	Part 1: Verify registers. 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. Part 2: Check against SPI flash device datasheet. 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.bin[2] SPI part registry cached in Intel® PETS. ***Notes:*** 1. The "MEInfo" tool is part of the Intel® CSME 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.

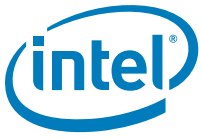
6.5 SPI Flash Size Test

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.

Test ID	SPI_004
Objective	Verify the correct SPI flash size is used for a given PCH SKU contained in the SUT.
Procedure	1. Boot to target OS. 2. Read following information from SPI Flash Descriptor in the SUT: • 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 (C0DEN) 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: • SPI flash device manufacturer datasheet[1]. ***Note:*** 1. Intel® PETS maintains a list of SPI flash device sizes.
Test Pass/Fail Criteria	The test passes if the following conditions is true: 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 programed by BIOS. Incorrect VSCCn registers configuration may affect SPI flash functionality and also may lead to premature flash device wear out.
Objective	To verify VSCCn registers in memory mapped space and VSCC table in SPI Flash Descriptor is configured correctly.
Procedure	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 (FDBAR[1] + 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. ***Note:*** FDBAR is located at address 0 of the SPI flash device chip select 0.
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	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. PETS helps automate testing of this capability. Perform the test by enabling "State after G3 to S5" at BIOS setting. **Alternate Procedure** 1. Configure the platform with Intel® CSME Firmware. 2. Use FPT /d to dump the image. 3. Use Flash Programming Tool (FPT) to lock the image down using the -closemnf. Boot system from a G3 state. 4. Use FPT /d to dump the image. This test should fail. 5. Use the physical jumper to override the protection (asserts HDA_SDO high during rising edge of PWROK). 6. Use FPT /d to dump the image. This test should now pass.
Test Pass/Fail Criteria	Test passes if FDOPSS bit is set to '1' by default and set to '0' when intending to enter Intel® CSME Test Mode.

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

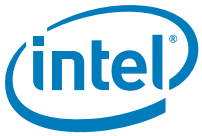
Test ID	SPI_007
Test Case Title	Single Input, Dual or Quad Output Fast Read Test
Mandatory/Optional	Mandatory
Description	This test is to verify that the flash parts supports Single Input, Dual, or Quad Output fast read if selected. This is a new mode of operation for serial flash that increases the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

Test ID	SPI_007
Objective	This test is to verify that the flash parts supports Single Input, Dual, or Quad Output fast read if selected.
Procedure	PETS asks the user whether 'Single Input Dual or Quad Output Fast Read' is supported. **If Yes,** 1. PETS verifies that FLCOMP bit 20 is set to 1b. 2. PETS then uses Serial Flash Discovery Parameters to verify that all flash parts in the system support 'Single Input, Dual or Quad Output Fast Read'. 3. PETS checks whether softstraps are enabled to support Dual or Quad Output Fast Read Function. a. For Dual Output Read, PETS checks if FLCOMP bit 12 is set to 1 b. For Quad Output Read. PETS checks if FLCOMP bit 14 is set to 1 ***Note:*** Quad Output Fast Read is not supported if the Flash device does not have SFDP.. **If No,** 1. PETS verifies that FLCOMP bit 20 is set to 0b.
Test Pass/Fail Criteria	Test fails if there is an invalid configuration with single input, dual, or quad output fast read. Test results passes if settings are not invalid, and if single input, dual output fast read is verified by SFDP.

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 supports Dual or Quad I/O Fast Read. This is a new mode of operation for serial flash that increases the read speed of SPI flash. If incorrectly configured there could be undesired operation.
Objective	This test is to verify that the flash parts supports Dual or Quad I/O Fast Read
Procedure	PETS asks the user whether 'Dual or Quad I/O Fast Read' is supported. **If Yes,** 1. PETS uses Serial Flash Discovery Parameters (SFDP) to verify that all flash parts in the system support 'Dual or Quad I/O Fast Read. 2. PETS then check if a. if FLCOMP bit 13 is set to 1 if Dual I/O fast read is supported; or b. FLCOMP bit 15 is set to 1 if Quad I/O fast read is supported. 3. PETS verifies that FLCOMP bit 20 set to 1. **If No,** 1. PETS then check if a. offset FLCOMP bit 13 is set to 0 if Dual I/O Fast Read is not supported; or b. FLCOMP bit 15 is set to 0 if Quad I/O Fast Read is not supported.
Test Pass/Fail Criteria	Test fails if there is an invalid configuration with single input, Dual or Quad I/O Fast Read and if serial flash part does not support Serial Flash Discovery Parameters, Dual and Quad I/O Fast Read would not be supported. Test results passes if settings are not invalid, and if single input, Dual or Quad I/O Fast Read is verified by SFDP..

§ §



7 Enhanced Serial Peripheral Interface (eSPI)

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 it's MAF and SAF configurations, allocate low voltage of 1.8V to I/O buffers, reduces pin count, and allows for higher bandwidth.

7.1 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.

7.2 Tools for Testing

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

7.3 eSPI Compliancy Test Coverage Summary

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

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

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

Test ID	Test Case Title	PETS Package Name	OS Supported	How?
eSPI_001	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
eSPI_010	Platform boots with EC Read-Only permission to BIOS region and BIOS with RW permissions to EC	N/A	W	M

Test ID	Test Case Title	PETS Package Name	OS Supported	How?
eSPI_011	Perform FWUpdate with MAF configurations	N/A	W	M

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

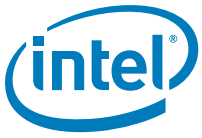
Test ID	**eSPI_001**
Test Case Title	Booting with MAF configurations (straps set to MAF defaults)
Platform	Platforms with MAF configuration
Mandatory/Optional	Mandatory
Objective	Verify that the platform boots with default MAF configuration
Test Pass Criteria	Test passes if platform boots to OS
Description	Platform should boot to OS with all MAF straps set to default
Procedure	1. Follow Intel® SPI Programming Guide and review all soft straps applicable to MAF. 2. Build IFWI with default straps for MAF using Intel® FIT. 3. Flash IFWI onto the platform. 4. Check that platform boots to OS.

7.5 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	1. Create and IFWI in Intel® FIT with EC region. 2. Flash IFWI onto the platform. 3. Check that platform boots to OS.

7.6 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 ID	**eSPI_004**
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:	1. Create IFWI in Intel® FIT with EC region at a different location. 2. Flash IFWI onto the platform. 3. Check that the platform is booting to OS.

7.7 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	1. Create IFWI in Intel® FIT with EC region disabled. 2. Make sure Intel® FIT tool does not return any errors. 3. Flash IFWI onto the platform. 4. Check that the platform is booting to OS.

7.8 IFWI with Empty EC Region

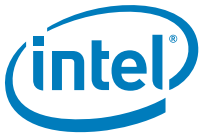
Test ID	**eSPI_006**
Test Case Title	IFWI with empty EC region
Platform	Platforms with SAF/MAF configuration
Mandatory/Optional	Mandatory
Objective	Ensure that Intel® FIT tool prevents building an image with empty EC region
Test Pass Criteria	Intel® FIT does not build IFWI with empty EC region
Description	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	1. Enable EC region in Intel® FIT. 2. Create IFWI without providing EC region. 3. Check that Intel® FIT does not build IFWI successfully.

7.9 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	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.

7.10 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	1. Create IFWI with default descriptor permissions in Intel® FIT. 2. Flash IFWI onto the platform. 3. Boot platform to OS. 4. Run Intel® FPT -closemnf EC. 1. Run Intel® MEManuf -EOL. 2. Make sure that Intel® MEManuf -EOL check passes.



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

Test ID	**eSPI_009**
Test Case Title	Platform boots with EC Read-Only permission to BIOS region
Platform	Platforms with MAF configuration **(Requires EOM for EC region)**
Mandatory/Optional	Mandatory
Objective	This test is to verify that the platform is boot successfully to OS with EC having only read permission to BIOS region and with default permission for the other regions
Test Pass Criteria	Test passes if platform boots to OS, EOM is set, and Intel® MEManuf -EOL check passes
Description	EC region can be configured to Read-Only from BIOS region.
Procedure	1. Create IFWI with EC Read-Only access to BIOS region in descriptor permissions in Intel® FIT. They should be as follows: a. EC read access should have a value of 0x103 in Intel® FIT. 2. Flash IFWI onto the platform. 3. Boot platform to OS. 4. Run Intel® FPT -closemnf EC. 5. Run Intel® MEManuf -EOL. 6. Make sure that Intel® MEManuf -EOL check passes.

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

Test ID	**eSPI_010**
Test Case Title	Platform boots with EC Read-Only permission to BIOS region and BIOS with RW permissions to EC
Platform	Platforms with MAF configuration **(Requires EOM for EC region)**
Mandatory/Optional	Mandatory
Objective	This test is to verify that the platform is boot successfully to OS with EC having only read permission to BIOS region and with BIOS have RW permissions to EC region
Test Pass Criteria	Test passes if platform boots to OS, EOM is set, and Intel® MEManuf -EOL check passes
Description	EC region can be configured to Read-Only from BIOS region as well as having BIOS with RW permissions to EC region
Procedure	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: a. EC read access should have a value of 0x103 in Intel® FIT b. Host CPU/BIOS read access should have a value of either 0x10F or 0x11F c. 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 -closemnf EC. 5. Run Intel® MEManuf -EOL. 6. Make sure that Intel® MEManuf -EOL check passes.

7.13 Perform FWUpdate with MAF Configurations

Test ID	**eSPI_011**
Test Case Title	Perform FWUpdate with MAF configurations
Platform	Platforms with MAF configurations
Mandatory/Optional	Mandatory
Objective	This test is to verify that the FWupdate flow works properly with MAF configurations and platform boots to OS
Test Pass Criteria	Test passes if FWupdate flow is successfully completed with MAF configurations in place.
Description	Ensuring that the platform would successfully boot with MAF configurations after performing a FWUpdate flow
Procedure	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.

§ §

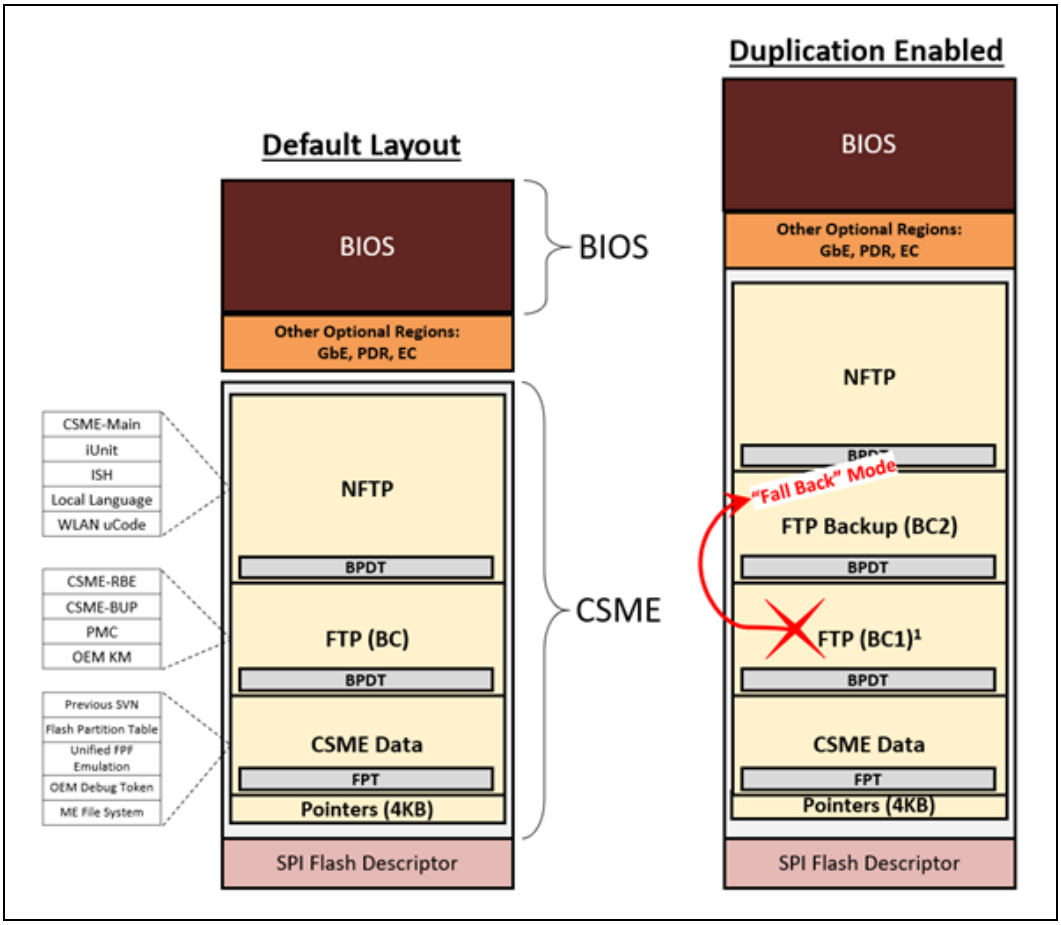
8 Intel® CSME Resiliency Compliancy

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

8.1 Intel® CSME Layout Overview with Boot Critical Redundancy

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

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



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

8.1.1 Intel® CSME Layout Pointers

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

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

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

8.1.2 Boot Partition Descriptor Table (BPDT)

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

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

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

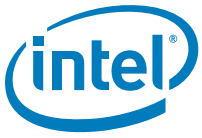


Table 8-1. BPDT Layout in Intel® CSME Region

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

8.1.3 Intel® CSME High-Level Flow

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

8.1.4 Intel® CSME Firmware Status (FWSTS1) Register Indication Scenarios

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

8.2 Test Environment

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

8.3 Intel® CSME Resiliency Compliancy Test Coverage Summary

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

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

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

8.4 Boot Critical Redundancy Enabled

Test ID	**Resilience_01**
Test Case Title	Boot Critical Redundancy Enabled
Mandatory/Optional	Optional
Description	The system is not in the Intel® ME Manufacturing Mode—when the system completes this test. This test is to confirm Boot Critical Redundancy Resiliency Feature is properly enabled and recognized by CSME. Do not perform any image corruption in this test.
Objective	Verify "Boot Critical Code Redundancy" is properly enabled and system normally booting to primary partition
Procedure	1. Build image using FIT with redundancy enabled: Build -> Build Settings -> under "Image Build Settings", set "Redundancy Enabled" to "True". 2. Boot system at least once to OS. 3. Confirm MEInfo output shows "Boot critical code redundancy" as "Enabled" 4. Confirm "Current Boot Partition" is "1" 5. Confirm FWSTS1.bit10 = "0" also indicating "Current Boot Partition" is Primary FTP/BC1 where "0" means no failure in booting BC1.
Test Pass/Fail Criteria	Pass: "Boot critical code redundancy" = "Enabled" AND "Current Boot Partition" = "1" Fail: "Boot critical code redundancy" = "Disabled"

8.5 Critical Code Corruption - BPDT1

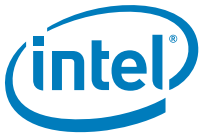
Test ID	**Resilience_02**
Test Case Title	Critical Code Corruption – BPDT
Mandatory/Optional	Optional
Description	The system is not in the Intel® ME Manufacturing Mode—when the system completes this test. This test is to confirm CSME can fallback to Backup copy of FTP (BC2) when BC1 is corrupted.
Objective	Verify Intel® CSME automatically falls back to BC2 when BC1 is corrupted.
Procedure	1. Build image using FIT with redundancy enabled: Build -> Build Settings -> under "Image Build Settings", set "Redundancy Enabled" to "True". 2. Boot system at least once to OS. 3. Place system in G3 and dump full SPI image. 4. From Layout Pointers, retrieve offset of "Boot Partition 1 (BP1)" (offset value located @ 35:32 within layout pointers). 5. "Boot Partition 1" starts with BPDT structure, manually corrupt structure writing "0xffffffff" at its offset 0 and save as "Corrupted_BPDT1.bin" 6. While system is in G3, flash Corrupted_BPDT1.bin image to SPI 7. Power up SUT and boot to OS 8. Confirm the following: a. MEInfo shows: "Current Boot Partition" = "2". b. FWSTS1.bit0-3 (Current State): Normal [5]. c. FWSTS1.bit10 (BC1 Boot Failed): Yes [1].
Test Pass/Fail Criteria	Pass: All below conditions must be met to pass the test: 1. MEInfo shows: "Current Boot Partition" = "2". 2. FWSTS1.bit0-3 (Current State): Normal [5]. 3. FWSTS1.bit10 (BC1 Boot Failed): Yes [1]. Fail: No Boot

8.6 Critical Code Corruption - BUP

Test ID	**Resilience_03**
Test Case Title	Critical Code Corruption – BUP
Mandatory/Optional	Optional
Description	The system is not in the Intel® ME Manufacturing Mode—when the system completes this test. This test is to confirm CSME can fallback to Backup copy of FTP (BC2) when BC1 is corrupted.
Objective	Verify Intel® CSME automatically falls back to BC2 when BC1 is corrupted.
Procedure	1. Build image using FIT with redundancy enabled: Build -> Build Settings -> under "Image Build Settings", set "Redundancy Enabled" to "True". 2. Boot system at least once to OS. 3. Place system in G3 and dump full SPI image. 4. From Layout Pointers, retrieve offset of "Boot Partition 1 (BP1)" (offset value located @ 35:32 within layout pointers). 5. "Boot Partition 1" starts with BPDT structure. Within BPDT1 find the BPDT Entry for "CSME BUP" (type 2) and manually Corrupt partition content at offset 700KB [do 4 KB erase] and save as "Corrupted_BUP.bin" (See BPDT details above). 6. While system is in G3, flash Corrupted_BUP.bin image to SPI 7. Power up SUT and boot to OS (expect to see global reset) 8. Confirm the following: a. MEInfo shows: "Current Boot Partition" = "2". b. FWSTS1.bit0-3 (Current State): Normal [5] c. FWSTS1.bit10 (BC1 Boot Failed): Yes [1].
Test Pass/Fail Criteria	Pass: All below conditions must be met to pass the test: 1. MEInfo shows: "Current Boot Partition" = "2". 2. FWSTS1.bit0-3 (Current State): Normal [5]. 3. FWSTS1.bit10 (BC1 Boot Failed): Yes [1]. Fail: No Boot

8.7 Critical Code Corruption - PMC

Test ID	**Resilience_04**
Test Case Title	Critical Code Corruption – PMC
Mandatory/Optional	Optional
Description	The system is not in the Intel® ME Manufacturing Mode—when the system completes this test. This test is to confirm CSME can fallback to Backup copy of FTP (BC2) when BC1 is corrupted.
Objective	Verify Intel® CSME automatically falls back to BC2 when BC1 is corrupted.
Procedure	1. Build image using FIT with redundancy enabled: Build -> Build Settings -> under "Image Build Settings", set "Redundancy Enabled" to "True". 2. Boot system at least once to OS. 3. Place system in G3 and dump full SPI image. 4. From Layout Pointers, retrieve offset of "Boot Partition 1 (BP1)" (offset value located @ 35:32 within layout pointers). 5. "Boot Partition 1" starts with BPDT structure. Within BPDT1 find the BPDT Entry for "PMC" (type 14 or 0xE) and manually Corrupt the 4KB pointed by sub-partition offset [do 4 KB erase] and save as "Corrupted_PMC.bin" (See BPDT details above). 6. While system is in G3, flash Corrupted_PMC.bin image to SPI 7. Power up SUT and boot to OS (expect to see global reset) 8. Confirm the following: a. MEInfo shows: "Current Boot Partition" = "2". b. FWSTS1.bit0-3 (Current State): Normal [2]. c. FWSTS1.bit10 (BC1 Boot Failed): Yes [1].
Test Pass/Fail Criteria	Pass: All below conditions must be met to pass the test: 1. MEInfo shows: "Current Boot Partition" = "2". 2. FWSTS1.bit0-3 (Current State): Normal [5] 3. FWSTS1.bit10 (BC1 Boot Failed): Yes [1]. Fail: No Boot



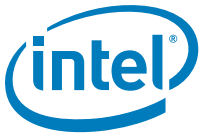
8.8 Critical Code Corruption - TypeC

Test ID	**Resilience_05**
Test Case Title	Critical Code Corruption – TypeC
Mandatory/Optional	Optional
Description	The system is not in the Intel® ME Manufacturing Mode—when the system completes this test. This test is to confirm CSME can fallback to Backup copy of FTP (BC2) when BC1 is corrupted.
Objective	Verify Intel® CSME automatically falls back to BC2 when BC1 is corrupted.
Procedure	1. Build image using FIT with redundancy enabled: Build -> Build Settings -> under "Image Build Settings", set "Redundancy Enabled" to "True". 2. Boot system at least once to OS. 3. Place system in G3 and dump full SPI image. 4. From Layout Pointers, retrieve offset of "Boot Partition 1 (BP1)" (offset value located @ 35:32 within layout pointers). 5. "Boot Partition 1" starts with BPDT structure. Within BPDT1 find the BPDT Entry for "IOM FW (TypeC)" (type 23 or 0x17) and manually Corrupt the 4KB pointed by sub-partition offset [do 4 KB erase] and save as "Corrupted_TypeC.bin" (See BPDT details above). 6. While system is in G3, flash Corrupted_TypeC.bin image to SPI 7. Power up SUT and boot to OS (expect to see global reset) 8. Confirm the following: a. MEInfo shows: "Current Boot Partition" = "2". b. FWSTS1.bit0-3 (Current State): Normal [5] c. FWSTS1.bit10 (BC1 Boot Failed): Yes [1].
Test Pass/Fail Criteria	Pass: All below conditions must be met to pass the test: 1. MEInfo shows: "Current Boot Partition" = "2". 2. FWSTS1.bit0-3 (Current State): Normal [5]. 3. FWSTS1.bit10 (BC1 Boot Failed): Yes [1]. Fail: No Boot

8.9 Recovery of Corrupted Primary Boot Critical (BC1) Partition

Test ID	**Resilience_06**
Test Case Title	Recovery of Corrupted Primary Boot Critical (BC1) Partition
Mandatory/Optional	Optional
Description	The system is not in the Intel® ME Manufacturing Mode—when the system completes this test. This test is to confirm CSME can boot from primary FTP (BC1) after FWupdate repaired corruption
Objective	Verify Intel® CSME boot normally form BC1 after a successful FWUpdate repair BC1 corruption
Procedure	1. Perform Resilience_03 test above 2. Perform CSME FW Update (using FWUpdLcl or OEM Capsule update) 3. Confirm the following: a. MEInfo shows: "Current Boot Partition" = "1" b. FWSTS1.bit0-3 (Current State): Normal [5] c. FWSTS1.bit10 (BC1 Boot Failed): No [0]
Test Pass/Fail Criteria	Pass: All below conditions must be met to pass the test: 1. MEInfo shows: "Current Boot Partition" = "1" 2. FWSTS1.bit0-3 (Current State): Normal [5] 3. FWSTS1.bit10 (BC1 Boot Failed): No [0] Fail: Any of below conditions can fail this test: 1. MEInfo shows: "Current Boot Partition" = "2" 2. FWSTS1.bit0-3 (Current State): Recovery [2] 3. FWSTS1.bit10 (BC1 Boot Failed): Yes [1]

§ §



9 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

9.1 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
☑ Desktop ☑ Mobile	☑ Standard ☑ 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 S3 resting system state. Systems that support Modern Standby or Microsoft* Windows* InstantGo* moves to S0 Low Power Idle state upon being sent to Sleep. This is usually defined by feature support relative to the operating system in conjunction with BIOS and system device support, but may also be due to the nature of the operating system itself relative to the goals of the test.

9.2 Test Coverage Summary

The following describes columns in the test coverage summary below. The **Test ID** is the reference identifier for the test in this document and any related tools which reference this document. The **Title** is the name of the test. The **Req.** (Requirement) column describes the requirement for test execution. The **Form Factor**, **OS** (Operating System), and **Net** (network) indicate the applicable test system configuration. **How?** column describes the test methodology.

Req.: M = Mandatory, C = Conditional[1], and O = Optional

[1]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 9-2. Intel® AMT Test Coverage Summary

Test ID	Title	Req.	Form Factor D M W	Power Model S M/I	Net	How?
Intel® ME Firmware Update						
CS_020	Intel® ME Firmware Update	C	☑ ☑ ☑	☑ ☑	N	M

9.3 Intel® ME Firmware Update

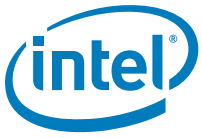
The section serves as a checklist for the environment setup and testing of Intel® ME firmware update feature support.

9.3.1 Tools for Testing

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

9.3.2 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	**Form Factor**: ☑ Desktop, ☑ Mobile **System Power Model**: ☑ Standard, ☑ 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	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)	12. Run the Intel® FWUpdLcl tool on the SUT to restore the firmware to the original image extracted earlier from the SUT. 13. Restart the SUT. 14. Verify the SUT has booted to the Host OS. 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.
Pass Criteria	The test passes if the firmware update is successful, and the original firmware can be restored for each of the following conditions: • 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. 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.
References	For details on Intel® ME firmware tools, refer to the *Intel® ME System Tools User Guide*.

§ §

10 Intel® CSME Power Management for Consumer Designs

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

10.1 System Power States

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

10.1.1 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:

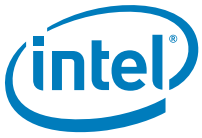
Intel® ME must be in CM-Off AND either a OR b as defined below:

1. ((DPS4_EN_AC AND S4) OR (DPS5_EN_AC AND S5)) (desktop only)
2. ((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 10-1. 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.

10.1.1.1 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#.

10.1.2 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.

10.2 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.

10.2.1 Test Parameters

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

Example 10-1.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 10-2.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.

10.2.2 Tools for Testing

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

- Intel® PETS: The latest version of the tool from the Intel® ME Compliancy and Debug kit release. Refer 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.

10.2.3 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.

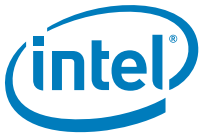
When completing tests within this chapter, especially those which send the system to a specific S-state (S3, S4, S5, Deep Sx, etc.), it is important to ensure that the network wake events are properly configured for each applicable device (LAN and/or WLAN).

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 helps to ensure System resumed from S4 state only and no other Sx state. Verify that windows booted from hibernate, i.e., value should be 0x02. “Run the following power shell command” Get-WinEvent-ProviderName Microsoft-windows-Kernel-boot-MaxEvents 10| where-Object{$_.message -like “The Boot type*”}

10.2.4 Test Step Execution and Verification

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

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 TGL. 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.
   a. CF9GR bit is located at 0xFE001048 (BIT20) in PMC PWRM space on TGL. Confirm that CF9 Lock down (CF9LOCK) bit 31 is set to **0**b. Information describing how to access this value may be found in the PCH EDS.
2. Verify that the SUT is in S0.
   a. 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]).
   a. 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**:

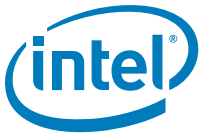
State	SLP_S3#	SLP_S4#	SLP_S5#	SLP_A#	VccSUS3_3	VccDSW3_3
S0	1	1	1	N/A	Powered	Powered
S3	0	1	1	N/A	Powered	Powered
S4	0	0	1	N/A	Powered	Powered
S5	0	0	0	N/A	Powered	Powered
MeOn	N/A	N/A	N/A	1	Powered	Powered
MeOff	N/A	N/A	N/A	0	Powered	Powered
Deep S4	0	0	1	0	Off	Powered
Deep S5	0	0	0	0	Off	Powered
G3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

   b. In S0, the CM0-PG and CM0 Intel® ME 'MeOn' states appears the same in the table above. Follow the procedure below via the Host OS on the SUT to confirm if the Intel® ME is Power Gated (CM0-PG):
      i. 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.
      ii. 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).



a. 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.

b. 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. 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.

   a. 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.

   a. 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.

   a. 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.

   a. The battery information on SUT can be queried via the Microsoft* Windows* Management Instrumentation Command (WMIC) tool.

   ```
   $> WMIC PATH Win32_Battery Get EstimatedChargeRemaining
   ```

   b. 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.

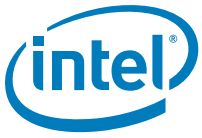
10.2.5 Setup Environment Tests

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** ☑ Modern Standby and InstantGo systems

ID	**Check S3**
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	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. 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	1. Suspend the SUT via the Host OS. 2. Verify that the SUT is in S3/MeOff (CM-Off). 3. Briefly press the Power Button on the SUT. 4. Verify that the SUT is in S0/MeOn (CM0,CM0-PG).
Pass Criteria	The test passes if the SUT moves to 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, please confirm the following: • 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	1. Hibernate the SUT via the Host OS. 2. Verify that the SUT is in S4,S5,Deep S4,Deep S5,G3/MeOff (CM-Off). 3. Briefly press the Power Button on the SUT. 4. Verify that the SUT is in S0/MeOn (CM0,CM0-PG). 5. Verify that windows booted from hibernate i.e. value should be 0x02. "run the following power shell command": Get-WinEvent -ProviderName Microsoft-Windows-Kernel-boot -MaxEvents 10 | Where-Object {$_.message -like "The boot type*"}
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).



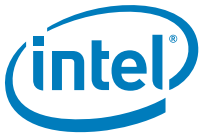
ID	Check S5		
Title	S0/CM0 to S5/CM-Off to S0/CM0 via Host OS shutdown cycle (AC-only)		
Requirement	Optional		
Method	Automated by Intel® PETS		
Objective	This test checks the SUT power flow from S0/CM0 to S5/CM-Off to S0/CM0 via Host OS shutdown cycle with the parameters outlined below.		
Configuration	If Deep S5 and/or G3 are supported on the SUT, please confirm the following: • 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	1. Shutdown the SUT via the Host OS. 2. Verify that the SUT is in S5,Deep S5,G3/MeOff (CM-Off). 3. Briefly press the Power Button on the SUT. 4. Verify that the SUT is in S0/MeOn (CM0,CM0-PG).		
Pass Criteria	The test passes if the SUT moves to S5, 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	☑ 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: • 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.		

ID	Check Deep S4
Procedure	1. Request the test operator to confirm the SUT is properly configured to enter Deep S4 upon Host OS hibernate. 2. Hibernate the SUT via the Host OS. 3. Verify that the SUT is in Deep S4/MeOff (CM-Off). 4. Briefly press the Power Button on the SUT. 5. Verify that the SUT is in S0/MeOn (CM0,CM0-PG).
Pass Criteria	The test passes if the SUT moves to Deep 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	☑ 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: • 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.		
Procedure	1. Request the test operator to confirm the SUT is properly configured to enter Deep S5 upon Host OS shutdown. 2. Shutdown the SUT via the Host OS. 3. Verify that the SUT is in Deep S5/MeOff (CM-Off). 4. Briefly press the Power Button on the SUT. 5. Verify that the SUT is in S0/MeOn (CM0,CM0-PG).		
Pass Criteria	The test passes if the SUT moves to Deep S5 and then to S0, and the Intel® 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: • The SUT and/or BIOS are properly configured to permit Deep S5 or G3 entry. • The correct Deep Sx policy is applied to the SUT profile in Intel® PETS.



ID	Check Intel® ME		
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	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	1. Shutdown the SUT via the Host OS. 2. Verify that the SUT is in S5,Deep S5,G3/MeOff (CM-Off). 3. Briefly press the Power Button on the SUT. 4. Verify that the SUT is in S0/MeOn (CM0,CM0-PG).		
Pass Criteria	The test passes if the SUT moves to S5 (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	☑ 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	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.		
Procedure	1. Set the SUT power source to **DC-only**. 2. Wait for **5 seconds** before proceeding to allow the test environment to stabilize. 3. 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	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.		

ID	Check AC Power
Procedure	1. Set the SUT power source to **AC-only**. 2. Wait **5 seconds** before proceeding to allow the test environment to stabilize. 3. 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.

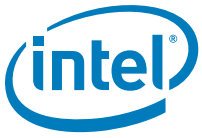
ID	Check G3 State	
Title	S0/CM0 to G3/CM-Off via Power loss (AC+DC, AC-only)	
Requirement	Optional	
Method	Automated by Intel® PETS	
Objective	This test checks the SUT power flow from S0/CM0 to G3/CM-Off via Power loss with the parameters outlined below.	
Configuration	If Deep S5 and/or G3 are supported on the SUT, please confirm the following: • 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)
	Power States – Final	G3/MeOff (CM-Off)
	Power States – 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. 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	1. Shutdown the SUT via the Host OS. 2. Verify that the SUT is in S5,Deep S5,G3/MeOff (CM-Off). 3. Remove power from the SUT via AC-detach, and if necessary also via DC-detach. Wait for **10 seconds** before continuing to allow full power drain from the SUT. 4. Verify that the SUT is in G3/MeOff (CM-Off).	
Pass Criteria	The test passes if the SUT moves to G3, and the Intel® ME moves to MeOff (CM-Off).	

10.3 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 would not support Modern Standby or Microsoft* Windows* InstantGo. Refer the test Requirement section for Exemption details.



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

Test ID	Test Case Title	Test Method
ME_PM_1	S0/CM0 to S3/CM-Off	Intel® PETS Package: Compliance_Power_G3-S5.xml
ME_PM_2	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_RST.xml
ME_PM_44	S0/CM0-PG, CM0 to S4–S5/CM-Off	Intel® PETS Package: Compliance_ME_Power_Gating.xml
ME_PM_45	G3 or S4–S5/CM-Off to S0/CM0_PG, CM0	Intel® PETS Package: Compliance_ME_Power_Gating.xml Compliance_ME_Power_Gating_Network_Wake.xml
ME_PM_46	S0/CM0-PG, CM0 to S0/CM0-PG, CM0	Intel® PETS Package: Compliance_ME_Power_Gating.xml Compliance_Power_RST.xml

Notes:

1. All the tests which use wake on LAN (WOL) as a trigger require SUSPEND well (SUS well) to be powered up. Hence platforms which implement and support DeepSx cannot run WOL tests. PETS includes all the WOL tests under a single package named Compliance_Power_WOL.xml.
2. Some tests defined in this chapter perform a non-graceful system shutdown or restart. In cases where the Host OS used on the SUT during the test is Microsoft* Windows*, the test may cause the Host OS to enter into recovery mode due to non-graceful power state transition. **Test operators should be aware of the Host OS boot state during these tests to avoid impact to the Host OS on the SUT or invalid test result collection.** The following is a list of tests which may have impact on subsequent Host OS boot: ME_PM_17.6, ME_PM_18.1/2, 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.

10.4 ME_PM_1: S0/CM0 to S3/CM-Off

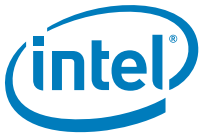
ID	**ME_PM_1.1**		
Title	S0/CM0 to S3/CM-Off via Host OS suspend (DC-only)		
Requirement	Mandatory	**Exemptions**	☑ Non-Mobile (AC-only) systems ☑ Modern Standby and InstantGo systems
Method	Automated by Intel® PETS		

ID	**ME_PM_1.1**
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	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	1. Suspend the SUT via the Host OS. 2. Verify that the SUT is in S3/MeOff (CM-Off).
Pass Criteria	The test passes if the SUT moves to S3 and the Intel® 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**: ☑ 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	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	1. Suspend the SUT via the Host OS. 2. Verify that the SUT is in S3/MeOff (CM-Off).
Pass Criteria	The test passes if the SUT moves to S3 and the Intel® ME moves to MeOff (CM-Off).

10.5 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**: ☑ Systems without WoL and/or WoWLAN support ☑ Modern Standby and InstantGo systems
Method	Automated by Intel® PETS

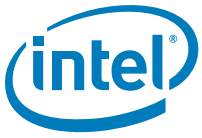


ID	ME_PM_2.1		
Objective	This test checks the SUT power flow from S3/CM-Off to S0/CM0 via magic packet with the parameters outlined below.		
Configuration	This test assumes that either LAN-only, WLAN-only, or both LAN and WLAN network interfaces are available on the SUT. Where both network interfaces are available, LAN is the initial active network interface in the test, and WLAN is the secondary network interface.		
Parameters	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	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. Record the Host OS last boot time on the SUT (to verify successful return from S3). 5. Ensure that yellow bang is not seen on Drivers in Device Manager		
Procedure	1. Suspend the SUT via the Host OS. 2. Verify that the SUT is in S3/MeOff (CM-Off). 3. Send three magic packets, at **2 second** intervals, by means of the active network interface. 4. Verify that the SUT is in S0/MeOn (CM0,CM0-PG). 5. Verify that the Host OS on the SUT is available.Verify that the second nibble of the FWSTS2 register on the SUT have a value of 0x6**0**xxxxxx. 6. Verify the Host OS last boot time on the SUT matches the boot time recorded before entry into S3. 7. Verify that the second nibble of the FWSTS2 register on the SUT have a value of 0x6**0**xxxxxx. 8. 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: • 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	☑ Non-Mobile (AC-only) systems ☑ Modern Standby and InstantGo systems
Method	Automated by Intel® PETS		
Objective	This test checks the SUT power flow from S3/CM-Off to S0/CM0 via Power Button press with the parameters outlined below.		
Configuration	This test assumes that either LAN-only, WLAN-only, or both LAN and WLAN network interfaces are available on the SUT.		
Parameters	System Power Source		DC-only
	Power States	Initial	S3/MeOff (CM-Off)
		Final	S0/MeOn (CM0,CM0-PG)
		Trigger	Power Button press

ID	ME_PM_2.2
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. 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 8. Suspend the SUT via the Host OS. 9. Verify that the SUT is in S3/MeOff (CM-Off).
Procedure	1. Briefly press the Power Button on the SUT. 2. Verify that the SUT is in S0/MeOn (CM0,CM0-PG). 3. Verify that the Host OS on the SUT is available. 4. Verify the Host OS last boot time on the SUT matches the boot time recorded before entry into S3. 5. Verify that the second nibble of the FWSTS2 register on the SUT have a value of 0x6**0**xxxxxx. 6. Ensure that yellow bang is not seen on Drivers in Device Manager
Pass Criteria	The test passes if: • 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** ☑ 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	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. 4. Record the Host OS last boot time on the SUT (to verify successful return from S3). 5. Ensure that yellow bang is not seen on Drivers in Device Manager 6. Suspend the SUT via the Host OS. 7. Verify that the SUT is in S3/MeOff (CM-Off).		
Procedure	1. Briefly press the Power Button on the SUT. 2. Verify that the SUT is in S0/MeOn (CM0,CM0-PG). 3. Verify that the Host OS on the SUT is available. 4. Verify the Host OS last boot time on the SUT matches the boot time recorded before entry into S3. 5. Verify that the second nibble of the FWSTS2 register on the SUT have a value of 0x6**0**xxxxxx. 6. Ensure that yellow bang is not seen on Drivers in Device Manager		



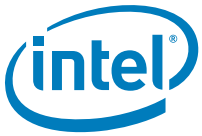
ID	ME_PM_2.3
Pass Criteria	The test passes if: • The SUT moves from S3 to S0. • The Intel® ME moves to MeOn (CM0, CM0-PG). • The Host OS last boot time has not changed.

ID	ME_PM_2.7		
Title	S3/CM-Off to S0/CM0 via magic packet (DC-only)		
Requirement	Optional	Non-Support	☑ Non-Mobile (AC-only) systems ☑ Systems without WoL and/or WoWLAN support ☑ Modern Standby and InstantGo systems
Method	Automated by Intel® PETS		
Objective	This test checks the SUT power flow from S3/CM-Off to S0/CM0 via magic packet with the parameters outlined below.		
Configuration	This test assumes that either LAN-only, WLAN-only, or both LAN and WLAN network interfaces are available on the SUT. Where both network interfaces are available, LAN is the initial active network interface in the test, and WLAN is the secondary network interface.		
Parameters	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	1. Suspend the SUT via the Host OS. 2. Verify that the SUT is in S3/MeOff (CM-Off). 3. Send three magic packets, at **2 second** intervals, by means of the active network interface. 4. Verify that the SUT is in S0/MeOn (CM0,CM0-PG). 5. Verify that the Host OS on the SUT is available. 6. Verify the Host OS last boot time on the SUT matches the boot time recorded before entry into S3. 7. Verify that the second nibble of the FWSTS2 register on the SUT have a value of 0x6**0**xxxxxx. 8. 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: • 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.		

10.6 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** ☑ 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 S5 and/or G3 are supported on the SUT, confirm the following: • 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) **Power States** — **Final**: S4, S5, Deep S4, Deep S5, G3/MeOff (CM-Off) **Power States** — **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 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	1. Hibernate the SUT via the Host OS. 2. Verify that the SUT is in S4,S5,Deep S4,Deep S5,G3/MeOff (CM-Off).
Pass Criteria	The test passes if the SUT moves to S4, S5, Deep S4, Deep S5, or G3, and the Intel® 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 S5 and/or G3 are supported on the SUT, confirm the following: • 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) **Power States** — **Final**: S4, S5, Deep S4, Deep S5, G3/MeOff (CM-Off) **Power States** — **Trigger**: Host OS hibernate



ID	ME_PM_8.2
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	1. Hibernate the SUT via the Host OS. 2. Verify that the SUT is in S4,S5,Deep S4,Deep S5,G3/MeOff (CM-Off).
Pass Criteria	The test passes if the SUT moves to S4, S5, Deep S4, Deep S5, or G3, and the Intel® ME moves to MeOff (CM-Off).

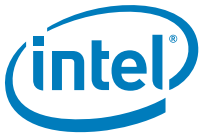
ID	ME_PM_8.3		
Title	S0/CM0 to S5/CM-Off via Host OS shutdown (DC-only)		
Requirement	Mandatory **Exemptions** ☑ Non-Mobile (AC-only) systems		
Method	Automated by Intel® PETS		
Objective	This test checks the SUT power flow from S0/CM0 to S5/CM-Off via Host OS shutdown with the parameters outlined below.		
Configuration	If Deep S5 and/or G3 are supported on the SUT, confirm the following: • The SUT and/or BIOS are properly configured to permit Deep S5 or G3 entry. • The correct Deep Sx policy is applied to the SUT profile in Intel® PETS. This test assumes that either LAN-only, WLAN-only, or both LAN and WLAN network interfaces are available on the SUT.		
Parameters	**System Power Source**		DC-only
	Power States	**Initial**	S0/MeOn (CM0,CM0-PG)
		Final	S3/MeOff (CM-Off)
		Trigger	Host OS shutdown
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.		
Procedure	1. Shutdown the SUT via the Host OS. 2. Verify that the SUT is in S5,Deep S5,G3/MeOff (CM-Off).		
Pass Criteria	The test passes if the SUT moves to S5 (or Deep S5 or G3), and the Intel® 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	If Deep S5 and/or G3 are supported on the SUT, confirm the following: • 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.

ID	**ME_PM_8.4**		
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	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	1. Shutdown the SUT via the Host OS. 2. Verify that the SUT is in S5,Deep S5,G3/MeOff (CM-Off).		
Pass Criteria	The test passes if the SUT moves to S5 (or Deep S5 or G3), and the Intel® ME moves to MeOff (CM-Off).		

10.7 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** ☑ 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 S5 and/or G3 are supported on the SUT, confirm the following: • 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	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. Hibernate the SUT via the Host OS. 8. Verify that the SUT is in S4,S5,Deep S4,Deep S5,G3/MeOff (CM-Off).		



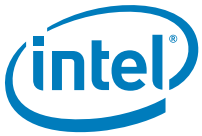
ID	ME_PM_9.1
Procedure	1. Briefly press the Power Button on the SUT. 2. Verify that the SUT is in S0/MeOn (CM0,CM0-PG). 3. Verify that the Host OS on the SUT is available. 4. Verify that windows booted from hibernate i.e. value should be 0x02. "run the following power shell command": Get-WinEvent -ProviderName Microsoft-Windows-Kernel-boot -MaxEvents 10 | Where-Object {$_.message -like "The boot type*"} 5. Verify that the second nibble of the FWSTS2 register on the SUT have a value of 0x6**0**xxxxxx. 6. 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.	
Configuration	If Deep S5 and/or G3 are supported on the SUT, confirm the following: • 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)
	Power States – **Final**	S0/MeOn (CM0,CM0-PG)
	Power States – **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	1. Briefly press the Power Button on the SUT. 2. Verify that the SUT is in S0/MeOn (CM0,CM0-PG). 3. Verify that the Host OS on the SUT is available. 4. Verify that 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*"} 5. Verify that the second nibble of the FWSTS2 register on the SUT have a value of 0x6**0**xxxxxx. 6. 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** | ☑ 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.

ID	**ME_PM_9.4**
Configuration	If Deep S5 and/or G3 are supported on the SUT, confirm the following: • 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
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. 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	1. Briefly press the Power Button on the SUT. 2. Verify that the SUT is in S0/MeOn (CM0,CM0-PG). 3. Verify that the Host OS on the SUT is available. 4. Verify that the second nibble of the FWSTS2 register on the SUT have a value of 0x6**0**xxxxxx. 5. 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: • 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



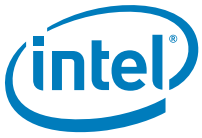
ID	ME_PM_9.5
Setup	1. Set the SUT power source to **AC+DC** where supported; otherwise **AC-only**. 2. Bring the SUT to the base state of S0/MeOn (CM0,CM0-PG), and confirm that the Host OS is available. 3. Ensure that the Host OS network device drivers are configured to **not wake** the SUT. This includes **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. Shutdown the SUT via the brief Power Button press. 6. Verify that the SUT is in S5,Deep S5,G3/MeOff (CM-Off).
Procedure	1. Briefly press the Power Button on the SUT. 2. Verify that the SUT is in S0/MeOn (CM0,CM0-PG). 3. Verify that the Host OS on the SUT is available. 4. Verify that the second nibble of the FWSTS2 register on the SUT have a value of 0x6**0**xxxxxx. 5. 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_9.7	
Title	G3/CM-Off to S0/CM0 via AC-attach (AC+DC,AC-only)	
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	If Deep S5 and/or G3 are supported on the SUT, confirm the following: • 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 BIOS is configured to boot SUT upon AC-attach after G3. 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	G3/MeOff (CM-Off)
	Power States – Final	S0/MeOn (CM0,CM0-PG)
	Power States – Trigger	AC-attach
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. Shutdown the SUT via the brief Power Button press. 6. Verify that the SUT is in S5,Deep S5,G3/MeOff (CM-Off). 7. 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. 8. Verify that the SUT is in G3/MeOff (CM-Off).	
Procedure	1. Set the SUT power source to AC+DC where supported; otherwise AC-only. For systems with DC-power support, consult the system design as it may be preferred to connect DC-power before AC-power. 2. Verify that the SUT is in S0/MeOn (CM0,CM0-PG). 3. Verify that the Host OS on the SUT is available. 4. Verify that the second nibble of the FWSTS2 register on the SUT have a value of 0x6**0**xxxxxx. 5. 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).	

10.8 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** ☑ System without a LAN-only network interface
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 S5 and/or G3 are supported on the SUT, confirm the following: • 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 LAN-only network interfaces are available on the SUT. Where network interfaces are available, LAN is the initial active network interface in the test.
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	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	1. Hibernate the SUT via the Host OS. 2. Verify that the SUT is in S4,S5,Deep S4,Deep S5,G3/MeOff (CM-Off). 3. Send three magic packets, at **2 second** intervals, by means of the active network interface. 4. Verify that the SUT is in S0/MeOn (CM0,CM0-PG). 5. Verify that the Host OS on the SUT is available. 6. Verify that windows booted from hibernate i.e. value should be 0x02. "run the following power shell command": Get-WinEvent -ProviderName Microsoft-Windows-Kernel-boot -MaxEvents 10 | Where-Object {$_.message -like "The boot type*"} 7. Verify that the second nibble of the FWSTS2 register on the SUT have a value of 0x6**0**xxxxxx. 8. Ensure that yellow bang is not seen on Drivers in Device Manager If LAN network interfaces are available, repeat this test procedure with the LAN interface set as the active network interface.
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** ☑ System without a LAN-only network interface
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	If Deep S5 and/or G3 are supported on the SUT, confirm the following: • 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 LAN-only network interfaces are available on the SUT. Where network interfaces are available, LAN is the initial active network interface in the test.

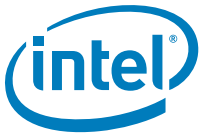


ID	ME_PM_10.5		
Parameters	System Power Source		AC+DC or AC-only
	Power States	Initial	S5, Deep S5, G3/MeOff (CM-Off)
		Final	S0/MeOn (CM0,CM0-PG)
		Trigger	Magic Packet receipt
Setup	1. Set the SUT power source to **AC+DC** where supported; otherwise **AC-only**. 2. Bring the SUT to the base state of 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		
Procedure	1. Shutdown the SUT via the Host OS. 2. Verify that the SUT is in S5,Deep S5,G3/MeOff (CM-Off). 3. Send three magic packets, at **2 second** intervals, by means of the active network interface. 4. Verify that the SUT is in S0/MeOn (CM0,CM0-PG). 5. Verify that the Host OS on the SUT is available. 6. Verify that the second nibble of the FWSTS2 register on the SUT have a value of 0x6**0**xxxxxx. 7. Ensure that yellow bang is not seen on Drivers in Device Manager If both LAN network interfaces are available, repeat this test procedure with the LAN interface set as the active network interface.		
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: • 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 LAN-only 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	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. Shutdown the SUT via the Host OS. 6. Verify that the SUT is in S5,Deep S5,G3/MeOff (CM-Off).		

ID	**ME_PM_10.6**
Procedure	1. Briefly press the Power Button on the SUT. 2. Verify that the SUT is in S0/MeOn (CM0,CM0-PG). 3. Verify that the Host OS on the SUT is available. 4. Verify that the second nibble of the FWSTS2 register on the SUT have a value of 0x6**0**xxxxxx. 5. 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**	☑ Non-Mobile (AC-only) systems ☑ System without a LAN-only network interface
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 S5 and/or G3 are supported on the SUT, confirm the following: • 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 LAN-only network interfaces are available on the SUT. Where both network interfaces are available, LAN is the initial active network interface in the test, and WLAN is the secondary network interface.		
Parameters	**System Power Source**: 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	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		
Procedure	1. Hibernate the SUT via the Host OS. 2. Verify that the SUT is in S4,S5,Deep S4,Deep S5,G3/MeOff (CM-Off). 3. Send three magic packets, at **2 second** intervals, by means of the active network interface. 4. Verify that the SUT is in S0/MeOn (CM0,CM0-PG). 5. Verify that the Host OS on the SUT is available. 6. Verify that windows booted from hibernate i.e. value should be 0x02. "run the following power shell command": Get-WinEvent -ProviderName Microsoft-Windows-Kernel-boot -MaxEvents 10 | Where-Object {$_.message -like "The boot type*"} 7. Verify that the second nibble of the FWSTS2 register on the SUT have a value of 0x6**0**xxxxxx. 8. Ensure that yellow bang is not seen on Drivers in Device Manager If LAN network interfaces are available, repeat this test procedure with the LAN interface set as the active network interface.		
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)		



ID	ME_PM_10.11		
Requirement	Mandatory	Exemptions	☑ Non-Mobile (AC-only) systems ☑ System without a LAN-only network interface
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	If Deep S5 and/or G3 are supported on the SUT, confirm the following: • 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 LAN-only network interfaces are available on the SUT. Where network interfaces are available, LAN is the initial active network interface in the test.		
Parameters	System Power Source: DC-only Power States – Initial: S5, Deep S5, G3/MeOff (CM-Off) Power States – Final: S0/MeOn (CM0,CM0-PG) Power States – 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 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		
Procedure	1. Shutdown the SUT via the Host OS. 2. Verify that the SUT is in S5,Deep S5,G3/MeOff (CM-Off). 3. Send three magic packets, at **2 second** intervals, by means of the active network interface. 4. Verify that the SUT is in S0/MeOn (CM0,CM0-PG). 5. Verify that the Host OS on the SUT is available. 6. Verify that the second nibble of the FWSTS2 register on the SUT have a value of 0x6**0**xxxxxx. 7. Ensure that yellow bang is not seen on Drivers in Device Manager If LAN network interfaces are available, repeat this test procedure with the LAN interface set as the active network interface.		
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).		

10.9 ME_PM_17: Cold Reset

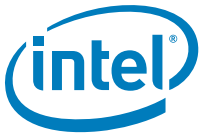
ID	ME_PM_17.6		
Title	S0/CM0 to S0/CM0 via CF9 Cold Reset (AC+DC,AC-only)		
Requirement	Mandatory	Exemptions	None
Method	Automated by Intel® PETS		
Objective	This test checks the SUT power flow from S0/CM0 to S0/CM0 via CF9 Cold Reset with the parameters outlined below.		
Configuration	This test assumes that either LAN-only, WLAN-only, or both LAN and WLAN network interfaces are available on the SUT.		

ID	**ME_PM_17.6**		
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	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	1. Ensure that CF9h Global Reset (CF9GR) is **cleared** to **0b**. 2. Perform a **cold reset** of the SUT by writing **Eh** to I/O register CF9h. 3. Verify that the SUT is in S0/MeOn (CM0,CM0-PG). 4. 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. 5. Ensure that yellow bang is not seen on Drivers in Device Manager		
Pass Criteria	The test passes if: • 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.		

10.10 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**	☑ Non-Mobile (AC-only) systems ☑ 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	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. 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 Manager 8. Write 1b to CF9GR to enable Global Reset		



ID	ME_PM_18.1
Procedure	1. Ensure that CF9h Global Reset (CF9GR) is **set** to **1b** to enable global reset. 2. Perform a **global reset** of the SUT by writing either **6h** or **Eh** to I/O register CF9h. 3. Verify that the SUT is in S0/MeOn (CM0,CM0-PG). 4. 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. 5. Ensure that yellow bang is not seen on Drivers in Device Manager
Pass Criteria	The test passes if: • 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.

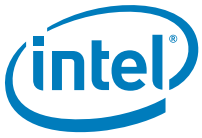
ID	ME_PM_18.2		
Title	S0/CM0 to S0/CM0 via CF9 Global Reset (AC+DC,AC-only)		
Requirement	Mandatory	Exemptions	☑ Systems not in Intel® ME manufacturing mode
Method	Automated by Intel® PETS		
Objective	This test checks the SUT power flow from S0/CM0 to S0/CM0 via CF9 Global Reset with the parameters outlined 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) Power States — Final: S0/MeOn (CM0,CM0-PG) Power States — Trigger: CF9 Global 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. 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	1. Ensure that CF9h Global Reset (CF9GR) is **set** to **1b** to enable global reset. 2. Perform a **global reset** of the SUT by writing either **6h** or **Eh** to I/O register CF9h. 3. Verify that the SUT is in S0/MeOn (CM0,CM0-PG). 4. 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. 5. Ensure that yellow bang is not seen on Drivers in Device Manager		
Pass Criteria	The test passes if: • 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.		

10.11 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	☑ Non-Mobile (AC-only) systems

ID	**ME_PM_19.1**
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: • The SUT and/or BIOS are properly configured to permit Deep S5 or G3 entry. • The correct Deep Sx policy is applied to the SUT profile in Intel® PETS. This test assumes that either LAN-only, WLAN-only, or both LAN and WLAN network interfaces are available on the SUT.
Parameters	**System Power Source**: DC-only **Power States** — **Initial**: S0/MeOn (CM0,CM0-PG) **Final**: S5, Deep S5, G3/MeOff (CM-Off) **Trigger**: Power 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.
Procedure	1. Shutdown the SUT via a Power Button press for more than **5 seconds**. 2. Verify that the SUT is in S5,Deep S5,G3/MeOff (CM-Off).
Pass Criteria	The test passes if the SUT moves to S5 (or Deep S5 or G3), and the Intel® 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
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: • 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	1. Shutdown the SUT via a Power Button press for more than **5 seconds**. 2. Verify that the SUT is in S5,Deep S5,G3/MeOff (CM-Off).
Pass Criteria	The test passes if the SUT moves to S5 (or Deep S5 or G3), and the Intel® ME moves to MeOff (CM-Off).



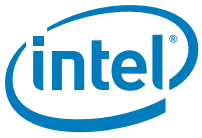
ID	**ME_PM_19.3**
Title	S3/CM-Off to S5/CM-Off via Power Button override (DC-only)
Requirement	Mandatory **Exemptions**: ☑ Non-Mobile (AC-only) systems; ☑ Modern Standby and InstantGo systems
Method	Automated by Intel® PETS
Objective	This test checks the SUT power flow from S3/CM-Off to S5/CM-Off via Power Button override with the parameters outlined below.
Configuration	If Deep S5, and/or G3 are supported on the SUT, confirm the following: • 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	1. Shutdown the SUT via a Power Button press for more than **5 seconds**. 2. Verify that the SUT is in S5,Deep S5,G3/MeOff (CM-Off).
Pass Criteria	The test passes if the SUT moves to S5 (or Deep S5 or G3), and the Intel® 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**: ☑ 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: • 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**: AC+DC or AC-only **Power States** — **Initial**: S3/MeOff (CM-Off); **Final**: S5, Deep S5, G3/MeOff (CM-Off); **Trigger**: Power Button override

ID	**ME_PM_19.4**
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. 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. 4. Suspend the SUT via the Host OS. 5. Verify that the SUT is in S3/MeOff (CM-Off).
Procedure	1. Shutdown the SUT via a Power Button press for more than **5 seconds**. 2. Verify that the SUT is in S5,Deep S5,G3/MeOff (CM-Off).
Pass Criteria	The test passes if the SUT moves to S5 (or Deep S5 or G3), and the Intel® 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_19.5**	
Title	S4/CM-Off to S5/CM-Off via Power Button override (DC-only)	
Requirement	Mandatory **Exemptions** ☑ 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	If Deep S5 and/or G3 are supported on the SUT, confirm the following: • 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)
	Power States – **Final**	S5, Deep S5, G3/MeOff (CM-Off)
	Power States – **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. 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	1. Shutdown the SUT via a Power Button press for more than **5 seconds**. 2. Verify that the SUT is in S5,Deep S5,G3/MeOff (CM-Off).	
Pass Criteria	The test passes if the SUT moves to, 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_19.6**
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.



ID	ME_PM_19.6
Configuration	If Deep S5 and/or G3 are supported on the SUT, confirm the following: • 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) Power States — Final: S5, Deep S5, G3/MeOff (CM-Off) Power States — 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	1. Shutdown the SUT via a Power Button press for more than **5 seconds**. 2. Verify that the SUT is in S5,Deep S5,G3/MeOff (CM-Off).
Pass Criteria	The test passes if the SUT moves to, 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).

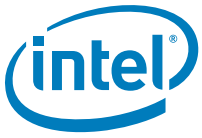
ID	ME_PM_19.7
Title	S5/CM-Off to S5/CM-Off via Power Button override (DC-only)
Requirement	Mandatory — Exemptions: ☑ Non-Mobile (AC-only) systems
Method	Automated by Intel® PETS
Objective	This test checks the SUT power flow from S5/CM-Off to S5/CM-Off via Power Button override with the parameters outlined below.
Configuration	If Deep S5 and/or G3 are supported on the SUT, please confirm the following: • 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) Power States — Final: S5, Deep S5, G3/MeOff (CM-Off) Power States — 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	1. Shutdown the SUT via a Power Button press for more than **5 seconds**. 2. Verify that the SUT is in S5,Deep S5,G3/MeOff (CM-Off).

ID	**ME_PM_19.7**
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).

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: • 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	1. Shutdown the SUT via a Power Button press for more than **5 seconds**. 2. Verify that the SUT is in S5,Deep S5,G3/MeOff (CM-Off).		
Pass Criteria	The test passes if the SUT 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).		

10.12 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**	☑ Non-Mobile (AC-only) systems ☑ System without a LAN-only network interface
Method	Automated by Intel® PETS		
Objective	This test checks the SUT power flow from S4/CM-Off to S0/CM0 via magic packet with the parameters outlined below.		

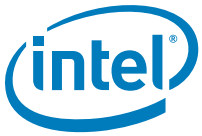


ID	ME_PM_25.1
Configuration	If Deep S5 and/or G3 are supported on the SUT, confirm the following: • The SUT and/or BIOS are properly configured to permit Deep S4/S5 or G3 entry. • The correct Deep Sx policy is applied to the SUT profile in Intel® PETS. This test assumes that LAN-only network interfaces are available on the SUT. Where both network interfaces are available, LAN is the initial active network interface in the test, and WLAN is the secondary network interface.
Parameters	**System Power Source**: 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	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
Procedure	1. Hibernate the SUT via the Host OS. 2. Verify that the SUT is in S4,S5,Deep S4,Deep S5,G3/MeOff (CM-Off). 3. 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. 4. Verify that the SUT is in S4,S5,Deep S4,Deep S5,G3/MeOff (CM-Off). 5. Send three magic packets, at **2 second** intervals, by means of the active network interface. 6. Verify that the SUT is in S0/MeOn (CM0,CM0-PG). 7. Verify that the Host OS on the SUT is available. 8. Verify that windows booted from hibernate i.e. value should be 0x02. "run the following power shell command": Get-WinEvent -ProviderName Microsoft-Windows-Kernel-boot -MaxEvents 10 | Where-Object {$_.message -like "The boot type*"} 9. Verify that the second nibble of the FWSTS2 register on the SUT have a value of 0x6**0**xxxxxx. 10. Ensure that yellow bang is not seen on Drivers in Device Manager If LAN network interfaces are available, repeat this test procedure with the LAN interface set as the active network interface.
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)
Requirement	Mandatory — **Exemptions**: ☑ Non-Mobile (AC-only) systems; ☑ System without a LAN-only network interface
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	If Deep S5 and/or G3 are supported on the SUT, confirm the following: • 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 LAN-only network interfaces are available on the SUT. Where network interfaces are available, LAN is the initial active network interface in the test.

ID	**ME_PM_25.2**		
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
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. Ensure that yellow bang is not seen on Drivers in Device Manager		
Procedure	1. Shutdown the SUT via the Host OS. 2. Verify that the SUT is in S5,Deep S5,G3/MeOff (CM-Off). 3. Set the SUT power source to AC+DC 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. 4. Verify that the SUT is in S5,Deep S5,G3/MeOff (CM-Off). 5. Send three magic packets, at **2 second** intervals, by means of the active network interface. 6. Verify that the SUT is in S0/MeOn (CM0,CM0-PG). 7. Verify that the Host OS on the SUT is available. 8. Verify that the second nibble of the FWSTS2 register on the SUT have a value of 0x6**0**xxxxxx. 9. Ensure that yellow bang is not seen on Drivers in Device Manager If LAN network interfaces are available, repeat this test procedure with the LAN interface set as the active network interface.		
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**	☑ Non-Mobile (AC-only) systems ☑ System without a LAN-only network interface
Method	Automated by Intel® PETS		
Objective	This test checks the SUT power flow from G3/CM-Off to S0/CM0 via magic packet with the parameters outlined below.		
Configuration	If Deep S5 and/or G3 are supported on the SUT, confirm the following: • 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 LAN-only network interfaces are available on the SUT. Where network interfaces are available, LAN is the initial active network interface in the test.		
Parameters	**System Power Source**		DC-only
	Power States	**Initial**	G3/MeOff (CM-Off)
		Final	S0/MeOn (CM0,CM0-PG)
		Trigger	Magic Packet receipt



ID	ME_PM_25.3
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. Ensure that yellow bang is not seen on Drivers in Device Manager
Procedure	1. Shutdown the SUT via the Host OS. 2. Verify that the SUT is in S5,Deep S5,G3/MeOff (CM-Off). 3. Remove power from the SUT via AC-detach, and if necessary also via DC-detach. Wait for **10 seconds** before continuing to allow full power drain from the SUT. 4. Verify that the SUT is in G3/MeOff (CM-Off). 5. Set the SUT power source to AC+DC where supported; otherwise AC-only. For systems with DC-power support, consult the system design as it may be preferred to connect DC-power before AC-power. 6. Verify that the SUT is in S5,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 the second nibble of the FWSTS2 register on the SUT have a value of 0x6**0**xxxxxx. 11. Ensure that yellow bang is not seen on Drivers in Device Manager If LAN network interfaces are available, repeat this test procedure with the LAN interface set as the active network interface.
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).

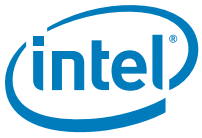
10.13 ME_PM_26: Warm Reset

ID	ME_PM_26.5	
Title	S0/CM0 to S0/CM0 via Reset Button press (or logic) (DC-only)	
Requirement	Mandatory **Exemptions** ☑ 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.	
Parameters	**System Power Source**	DC-only
	Power States – **Initial**	S0/MeOn (CM0,CM0-PG)
	Power States – **Final**	S0/MeOn (CM0,CM0-PG)
	Power States – **Trigger**	Reset Button press (or logic)
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 yellow bang is not seen on Drivers in Device Manager	

ID	**ME_PM_26.5**
Procedure	1. Perform a **warm reset** of the SUT by pressing the Reset Button. For designs without a Reset Button, access to the system reset logic should be prepared via blue wire. 2. Verify that the SUT is in S0/MeOn (CM0,CM0-PG). 3. Verify that the second nibble of the FWSTS2 register on the SUT have a value of 0x6**6**xxxxxx. 4. 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)
	Power States – **Final**	S0/MeOn (CM0,CM0-PG)
	Power States – **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), and confirm that the Host OS is available. 3. Ensure that yellow bang is not seen on Drivers in Device Manager	
Procedure	1. Perform a **warm reset** of the SUT by pressing the Reset Button. For designs without a Reset Button, access to the system reset logic should be prepared via blue wire. 2. Verify that the SUT is in S0/MeOn (CM0,CM0-PG). 3. Verify that the second nibble of the FWSTS2 register on the SUT have a value of 0x6**6**xxxxxx. 4. 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** | ☑ 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.	
Parameters	**System Power Source**	DC-only
	Power States – **Initial**	S0/MeOn (CM0,CM0-PG)
	Power States – **Final**	S0/MeOn (CM0,CM0-PG)
	Power States – **Trigger**	Host OS restart



ID	ME_PM_26.9
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 yellow bang is not seen on Drivers in Device Manager
Procedure	1. Perform a **warm reset** of the SUT via Host OS graceful restart. 2. Verify that the SUT is in S0/MeOn (CM0,CM0-PG). 3. Verify that the second nibble of the FWSTS2 register on the SUT have a value of 0Xx9xxxxxx. 4. 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)
	Power States – **Final**	S0/MeOn (CM0,CM0-PG)
	Power States – **Trigger**	Host OS restart
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 yellow bang is not seen on Drivers in Device Manager	
Procedure	1. Perform a **warm reset** of the SUT via Host OS graceful restart. 2. Verify that the SUT is in S0/MeOn (CM0,CM0-PG). 3. Verify that the second nibble of the FWSTS2 register on the SUT have a value of 0Xx9xxxxxx. 4. 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.

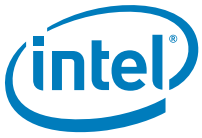
ID	**ME_PM_26.13**		
Parameters	**System Power Source**		AC+DC or AC-only
	Power States	**Initial**	S0/MeOn (CM0,CM0-PG)
		Final	S0/MeOn (CM0,CM0-PG)
		Trigger	CF9 Warm Reset
Setup	1. Set the SUT power source to **AC+DC** where supported; otherwise **AC-only**. 2. Bring the SUT to the base state of S0/MeOn (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	1. Ensure that CF9h Global Reset (CF9GR) is **cleared** to **0b**. 2. Perform a **warm reset** of the SUT by writing **6h** to I/O register CF9h. 3. Verify that the SUT is in S0/MeOn (CM0,CM0-PG). 4. 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. 5. Ensure that yellow bang is not seen on Drivers in Device Manager		
Pass Criteria	The test passes if: • 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.		

10.14 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	1. Remove power from the SUT via AC-detach, and if necessary also via DC-detach. Wait for **10 seconds** before continuing to allow full power drain from the SUT. 2. Verify that the SUT is in G3/MeOff (CM-Off).		
Pass Criteria	The test passes if the SUT moves from S0 to G3, and the Intel® ME moves to MeOff (CM-Off).		

10.15 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)

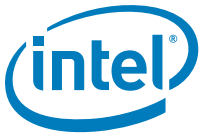


ID	ME_PM_44.3		
Requirement	Mandatory	Exemptions	☑ Non-Mobile (AC-only) systems ☑ Systems with a LAN-only network interface
Method	Automated by Intel® PETS with potential Test Operator interaction.		
Objective	This test checks the SUT power flow from S0/CM0-PG to S4/CM-Off via Host OS hibernate with the parameters outlined below.		
Configuration	If Deep S5 and/or G3 are supported on the SUT, confirm the following: • 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 that Intel® ME is in CM0-PG state for more than 50% within a time interval of **1 minute** 9. Verify that the SUT is in S0/MeOn (CM0-PG).		
Procedure	1. Hibernate the SUT via the Host OS. 2. Verify that the SUT is in S4,S5,Deep S4,Deep S5,G3/MeOff (CM-Off).		
Pass Criteria	The test passes if the SUT moves to S4, S5, Deep S4, Deep S5, or G3, and the Intel® 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	☑ 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 S5 and/or G3 are supported on the SUT, confirm the following: • 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	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 that Intel® ME is in CM0-PG state for more than 50% within a time interval of **1 minute** 7. Verify that the SUT is in S0/MeOn (CM0-PG).
Procedure	1. Hibernate the SUT via the Host OS. 2. Verify that the SUT is in S4,S5,Deep S4,Deep S5,G3/MeOff (CM-Off).
Pass Criteria	The test passes if the SUT moves to S4, S5, Deep S4, Deep S5, or G3, and the Intel® 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**	☑ Non-Mobile (AC-only) systems ☑ Systems with a LAN-only network interface
Method	Automated by Intel® PETS with potential Test Operator interaction.		
Objective	This test checks the SUT power flow from S0/CM0-PG to S5/CM-Off via Host OS shutdown with the parameters outlined below.		
Configuration	If Deep S5 and/or G3 are supported on the SUT, confirm the following: • 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	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 that Intel® ME is in CM0-PG state for more than 50% within a time interval of **1 minute** 9. Verify that the SUT is in S0/MeOn (CM0-PG).		
Procedure:	1. Shutdown the SUT via the Host OS. 2. Verify that the SUT is in S5,Deep S5,G3/MeOff (CM-Off).		
Pass Criteria:	The test passes if the SUT moves to S5 (or Deep S5 or G3), and the Intel® 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**	☑ Systems with a LAN-only network interface



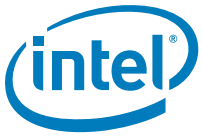
ID	**ME_PM_44.6**
Method	Automated by Intel® PETS with potential Test Operator interaction.
Objective	This test checks the SUT power flow from S0/CM0-PG to S5/CM-Off via Host OS shutdown with the parameters outlined below.
Configuration	If Deep S5 and/or G3 are supported on the SUT, confirm the following: • 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	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 that Intel® ME is in CM0-PG state for more than 50% within a time interval of **1 minute** 7. Verify that the SUT is in S0/MeOn (CM0-PG).
Procedure	1. Shutdown the SUT via the Host OS. 2. Verify that the SUT is in S5,Deep S5,G3/MeOff (CM-Off).
Pass Criteria	The test passes if the SUT moves to S5 (or Deep S5 or G3), and the Intel® ME moves to MeOff (CM-Off).

10.16 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**: ☑ Non-Mobile (AC-only) systems; ☑ 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 S5 and/or G3 are supported on the SUT, confirm the following: • 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	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	1. Briefly press the Power Button on the SUT. 2. Verify that the SUT is in S0. 3. Verify that the Host OS on the SUT is available. 4. Check that Intel® ME is in CM0-PG state for more than 50% within a time interval of **1 minute** 5. Verify that the SUT is in S0/MeOn (CM0-PG). 6. Verify that windows booted from hibernate i.e. value should be 0x02. "run the following power shell command": Get-WinEvent -ProviderName Microsoft-Windows-Kernel-boot -MaxEvents 10 | Where-Object {$_.message -like "The boot type*"} 7. 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).

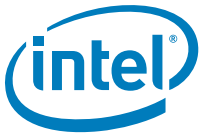
ID	ME_PM_45.4		
Title	S4/CM-Off to S0/CM0-PG via magic packet (AC+DC,AC-only)		
Requirement	Mandatory	Exemptions	☑ Systems without WoL and/or WoWLAN support ☑ Systems with a LAN-only network interface
Method	Automated by Intel® PETS with potential Test Operator interaction.		
Objective	This test checks the SUT power flow from S4/CM-Off to S0/CM0-PG via magic packet with the parameters outlined below.		
Configuration	If Deep S5 and/or G3 are supported on the SUT, confirm the following: • 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 is the initial active network interface in the test, and WLAN is the secondary network interface.		
Parameters	System Power Source		AC+DC or AC-only
	Power States	Initial	S4, S5, Deep S4, Deep S5, G3/MeOff (CM-Off)
		Final	S0/MeOn (CM0-PG)
		Trigger	Magic Packet receipt
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 is configured to **not** sleep on either AC (or DC, where available) power source configuration. 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. 5. Verify that the Host OS on the SUT is available. 6. Ensure that yellow bang is not seen on Drivers in Device Manager		



ID	ME_PM_45.4
Procedure	1. Hibernate the SUT via the Host OS. 2. Verify that the SUT is in S4,S5,Deep S4,Deep S5,G3/MeOff (CM-Off). 3. Send three magic packets, at **2 second** intervals, by means of the active network interface. 4. Verify that the SUT is in S0. 5. Verify that the Host OS on the SUT is available. 6. Check that Intel® ME is in CM0-PG state for more than 50% within a time interval of **1 minute** 7. Verify that the SUT is in S0/MeOn (CM0-PG). 8. Verify that windows booted from hibernate i.e. value should be 0x02. "run the following power shell command": Get-WinEvent -ProviderName Microsoft-Windows-Kernel-boot -MaxEvents 10 | Where-Object {$_.message -like "The boot type*"} 9. 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 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	☑ Non-Mobile (AC-only) systems ☑ 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: • 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	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	1. Briefly press the Power Button on the SUT. 2. Verify that the SUT is in S0. 3. Verify that the Host OS on the SUT is available. 4. Check that Intel® ME is in CM0-PG state for more than 50% within a time interval of **1 minute** 5. Verify that the SUT is in S0/MeOn (CM0-PG). 6. 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).		

<table>
<tr><td>ID</td><td colspan="3">ME_PM_45.7</td></tr>
<tr><td>Title</td><td colspan="3">G3/CM-Off to S0/CM0-PG via Power Button press (DC-only)</td></tr>
<tr><td>Requirement</td><td colspan="3">Mandatory Exemptions: ☑ Non-Mobile (AC-only) systems; ☑ Systems with a LAN-only network interface</td></tr>
<tr><td>Method</td><td colspan="3">Automated by Intel® PETS with potential Test Operator interaction.</td></tr>
<tr><td>Objective</td><td colspan="3">This test checks the SUT power flow from G3/CM-Off to S0/CM0-PG via Power Button press with the parameters outlined below.</td></tr>
<tr><td>Configuration</td><td colspan="3">If Deep S5 and/or G3 are supported on the SUT, confirm the following:
• 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.</td></tr>
<tr><td>Parameters</td><td colspan="3"><table><tr><td colspan="2">System Power Source</td><td>DC-only</td></tr><tr><td rowspan="3">Power States</td><td>Initial</td><td>G3/MeOff (CM-Off)</td></tr><tr><td>Final</td><td>S0/MeOn (CM0-PG)</td></tr><tr><td>Trigger</td><td>(DC-attach then) Power Button press</td></tr></table></td></tr>
<tr><td>Setup</td><td colspan="3">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).</td></tr>
<tr><td>Procedure</td><td colspan="3">1. Set the SUT power source to DC-only.
2. Briefly press the Power Button on the SUT.
3. Verify that the SUT is in S0.
4. Verify that the Host OS on the SUT is available.
5. Check that Intel® ME is in CM0-PG state for more than 50% within a time interval of 1 minute
6. Verify that the SUT is in S0/MeOn (CM0-PG).
7. Ensure that yellow bang is not seen on Drivers in Device Manager</td></tr>
<tr><td>Pass Criteria</td><td colspan="3">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).</td></tr>
</table>



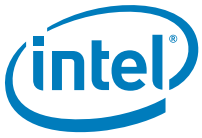
10.17 ME_PM_46: S0/CM0-PG, CM0 to S0/CM0-PG, CM0

ID	**ME_PM_46.1**
Title	S0/CM0-PG to S0/CM0-PG via Host OS restart (DC-only)
Requirement	Mandatory **Exemptions**: ☑ Non-Mobile (AC-only) systems; ☑ 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**: DC-only **Power States** — **Initial**: S0/MeOn (CM0-PG); **Final**: S0/MeOn (CM0-PG); **Trigger**: Host OS restart
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. Verify that the Host OS on the SUT is available. 7. Ensure that yellow bang is not seen on Drivers in Device Manager 8. Check that Intel® ME is in CM0-PG state for more than 50% within a time interval of **1 minute** 9. Verify that the SUT is in S0/MeOn (CM0-PG).
Procedure	1. Perform a **warm reset** of the SUT via Host OS graceful restart. 2. Verify that the SUT is in S0. 3. Verify that the Host OS on the SUT is available. 4. Check that Intel® ME is in CM0-PG state for more than 50% within a time interval of **1 minute** 5. Verify that the SUT is in S0/MeOn (CM0-PG). 6. 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_46.2**
Title	S0/CM0-PG to S0/CM0-PG via Host OS restart (AC+DC,AC-only)
Requirement	Mandatory **Exemptions**: ☑ 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	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 that Intel® ME is in CM0-PG state for more than 50% within a time interval of **1 minute** 7. Verify that the SUT is in S0/MeOn (CM0-PG).
Procedure	1. Perform a **warm reset** of the SUT via Host OS graceful restart. 2. Verify that the SUT is in S0. 3. Verify that the Host OS on the SUT is available. 4. Check that Intel® ME is in CM0-PG state for more than 50% within a time interval of **1 minute** 5. Verify that the SUT is in S0/MeOn (CM0-PG). 6. 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	☑ Non-Mobile (AC-only) systems ☑ 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		DC-only
	Power States	Initial	S0/MeOn (CM0-PG)
		Final	S0/MeOn (CM0-PG)
		Trigger	CF9 Cold Reset
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. Verify that the Host OS on the SUT is available. 7. Record the Host OS last boot time on the SUT (to verify reset execution). 8. Ensure that yellow bang is not seen on Drivers in Device Manager 9. Check that Intel® ME is in CM0-PG state for more than 50% within a time interval of **1 minute** 10. Verify that the SUT is in S0/MeOn (CM0-PG).		
Procedure	1. Ensure that CF9h Global Reset (CF9GR) is **cleared** to **0b**. 2. Perform a **cold reset** of the SUT by writing **Eh** to I/O register CF9h. 3. Verify that the SUT is in S0. 4. Verify that the Host OS on the SUT is available. 5. Verify the Host OS last boot time on the SUT **does not** match the boot time recorded before reset. 6. Check that Intel® ME is in CM0-PG state for more than 50% within a time interval of **1 minute** 7. Verify that the SUT is in S0/MeOn (CM0-PG). 8. Ensure that yellow bang is not seen on Drivers in Device Manager		



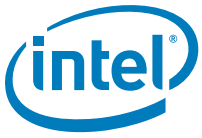
ID	ME_PM_46.3
Pass Criteria	The test passes if: • The SUT is reset to S0. • The Intel® ME is available in MeOn (CM0-PG). • The Host OS last boot time **does not** match.

ID	ME_PM_46.4		
Title	S0/CM0-PG to S0/CM0-PG via CF9 Cold Reset (AC+DC,AC-only)		
Requirement	Mandatory	Exemptions	☑ 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	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. Ensure that yellow bang is not seen on Drivers in Device Manager 7. Check that Intel® ME is in CM0-PG state for more than 50% within a time interval of **1 minute** 8. Verify that the SUT is in S0/MeOn (CM0-PG).		
Procedure	1. Ensure that CF9h Global Reset (CF9GR) is **cleared** to **0b**. 2. Perform a **cold reset** of the SUT by writing **Eh** to I/O register CF9h. 3. Verify that the SUT is in S0. 4. Verify that the Host OS on the SUT is available. 5. Verify the Host OS last boot time on the SUT **does not** match the boot time recorded before reset. 6. Check that Intel® ME is in CM0-PG state for more than 50% within a time interval of **1 minute** 7. Verify that the SUT is in S0/MeOn (CM0-PG). 8. Ensure that yellow bang is not seen on Drivers in Device Manager		
Pass Criteria	The test passes if: • 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	☑ Non-Mobile (AC-only) systems ☑ Systems with a LAN-only network interface ☑ 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	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. Verify that the Host OS on the SUT is available. 7. Record the Host OS last boot time on the SUT (to verify reset execution). 8. Verify that the Intel® ME is configured in manufacturing mode. 9. Ensure that yellow bang is not seen on Drivers in Device Manager 10. Check that Intel® ME is in CM0-PG state for more than 50% within a time interval of **1 minute** 11. Verify that the SUT is in S0/MeOn (CM0-PG). 12. Write 1b to CF9GR to enable Global Reset
Procedure	1. Ensure that CF9h Global Reset (CF9GR) is **set** to **1b** to enable global reset. 2. Perform a **global reset** of the SUT by writing either **6h** or **Eh** to I/O register CF9h. 3. Verify that the SUT is in S0. 4. Verify that the Host OS on the SUT is available. 5. Verify the Host OS last boot time on the SUT **does not** match the boot time recorded before reset. 6. Check that Intel® ME is in CM0-PG state for more than 50% within a time interval of **1 minute** 7. Verify that the SUT is in S0/MeOn (CM0-PG). 8. Ensure that yellow bang is not seen on Drivers in Device Manager
Pass Criteria	The test passes if: • 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_46.6**
Title	S0/CM0-PG to S0/CM0-PG via CF9 Global Reset (AC+DC,AC-only)
Requirement	Mandatory — **Exemptions**: ☑ Systems with a LAN-only network interface; ☑ 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	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 Manager 8. Check that Intel® ME is in CM0-PG state for more than 50% within a time interval of **1 minute** 9. Verify that the SUT is in S0/MeOn (CM0-PG). 10. Write 1b to CF9GR to enable Global Reset
Procedure	1. Ensure that CF9h Global Reset (CF9GR) is **set** to **1b** to enable global reset. 2. Perform a **global reset** of the SUT by writing either **6h** or **Eh** to I/O register CF9h. 3. Verify that the SUT is in S0. 4. Verify that the Host OS on the SUT is available. 5. Verify the Host OS last boot time on the SUT **does not** match the boot time recorded before reset. 6. Check that Intel® ME is in CM0-PG state for more than 50% within a time interval of **1 minute** 7. Verify that the SUT is in S0/MeOn (CM0-PG). 8. Ensure that yellow bang is not seen on Drivers in Device Manager
Pass Criteria	The test passes if: • The SUT is reset to S0. • The Intel® ME is available in MeOn (CM0-PG). • The Host OS last boot time **does not** match.

§ §

11 Intel® CSME 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).

11.1 System Power States

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

11.2 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.

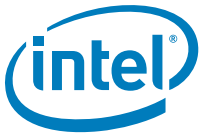
Other details about the configuration of the SUT are described on a per-test basis. Refer the test contents for details.

11.2.1 Test Parameters

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

Example 11-1.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 11-2.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.

11.2.2 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.

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

11.2.4 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 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 affects stress tests which boot the SUT to the Host OS.

11.2.5 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.

11.3 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. Refer to 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 would not support Modern Standby or Microsoft* Windows* InstantGo*. Refer the test Requirement section for Exemption details.

Network Configuration:
In general, all tests may be run on systems with any combination of LAN and/or WLAN network interface support. For tests that work with a subset of configurations, like LAN-only or LAN+WLAN, refer to 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*

11.4 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)

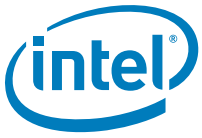
ID	**PM_ST_31**
Setup	1. Set the SUT power source to **AC+DC** where supported; otherwise **AC-only**. 2. Bring the SUT to the base state of S0/MeOn (CM0,CM0-PG).
Procedure	1. Wait **5 seconds** before proceeding to allow for power state stabilization. 2. Perform a **warm reset** of the SUT by pressing the Reset Button. For designs without a Reset Button, access to the system reset logic should be prepared via blue wire. 3. Verify that the SUT is in S0/MeOn (CM0,CM0-PG). Repeat this procedure for the remaining number of cycles desired in the stress test.
Pass Criteria	Test passes if all steps are completed successfully, for at least the recommended number of iterations as set by the OEM per the tolerance level of the system design. Suggested Iterations: Mobile: >=2000, Desktop/AIO >=750

11.5 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	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).		
Procedure	1. Shutdown the SUT via a Power Button press for more than **5 seconds**. 2. Verify that the SUT is in S5,Deep S5/MeOff (CM-Off). 3. Briefly press the Power Button on the SUT. 4. Verify that the SUT is in S0/MeOn (CM0,CM0-PG). Repeat this procedure for the remaining number of cycles desired in the stress test.		
Pass Criteria	Test passes if all steps are completed successfully, for at least the recommended number of iterations as set by the OEM per the tolerance level of the system design. Suggested Iterations: Mobile: >=2000, Desktop/AIO: >=750		

11.6 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)



ID	**PM_ST_33**
Requirement	Mandatory **Exemptions** ☑ Microsoft Windows* InstantGo* systems
Method	Automated by Intel® PETS
Objective	This test checks the SUT power flow from S0/CM0 to S3/CM-Off to S0/CM0 via Host OS suspend and Power Button press cycle with the parameters outlined below.
Configuration	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	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. 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. 4. Ensure that yellow bang is not seen on Drivers in Device Manager
Procedure	1. Suspend the SUT via the Host OS. 2. Verify that the SUT is in S3/MeOff (CM-Off). 3. Briefly press the Power Button on the SUT. 4. Verify that the SUT is in S0/MeOn (CM0,CM0-PG). 5. Verify that the Host OS on the SUT is available. 6. Verify the second nibble of the FWSTS2 register on the SUT have a value of 0x6**0**xxxxxx. 7. Ensure that yellow bang is not seen on Drivers in Device Manager 8. Check if there are any flash log. Success if there is no flash log.(Can test flash log by "MEInfo -FWSTS") Repeat this procedure for the remaining number of cycles desired in the stress test.
Pass Criteria	Test passes if all steps are completed successfully, for at least the recommended number of iterations as set by the OEM per the tolerance level of the system design. Suggested Iterations: Mobile: >=2000, Desktop/AIO: >=750

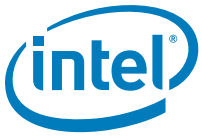
11.7 PM_ST_34: S0/CM0 to S4/CM-Off to S0/CM0 via Hibernate and WoL/WoWLAN

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** ☑ 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: • 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 is the initial active network interface in the test, and WLAN is the secondary network interface.

ID	**PM_ST_34**		
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
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, 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	1. Hibernate the SUT via the Host OS. 2. Verify that the SUT is in S4,S5,Deep S4,Deep S5/MeOff (CM-Off). 3. Send three magic packets, at **2 second** intervals, by means of the active network interface. 4. Verify that the SUT is in S0/MeOn (CM0,CM0-PG). 5. Verify that the Host OS on the SUT is available. 6. Verify the second nibble of the FWSTS2 register on the SUT have a value of 0x6**0**xxxxxx. 7. Verify that windows booted from hibernate i.e value should be 0x02. "Run the following power shell command "Get-WinEvent-ProviderName Microsoft-Windows-Kernel-boot-MaxEvents 10| where-Object{$_.message -like "The Boot Type*"} 8. If available, set the active network interface to **WLAN** (from LAN) to run the following: a. Hibernate the SUT via the Host OS. b. Verify that the SUT is in S4,S5,Deep S4,Deep S5/MeOff (CM-Off). c. Send three magic packets, at **2 second** intervals, by means of the **WLAN** network interface. d. Verify that the SUT is in S0/MeOn (CM0,CM0-PG). e. Verify that the Host OS on the SUT is available. f. Verify the second nibble of the FWSTS2 register on the SUT have a value of 0x6**0**xxxxxx. and Verify that windows booted from hibernate i.e value should be 0x02. "Run the following power shell command "Get-WinEvent-ProviderName Microsoft-Windows-Kernel-boot-MaxEvents 10| where-Object{$_.message -like "The Boot Type*"} 9. Ensure that yellow bang is not seen on Drivers in Device Manager 10. Check if there are any flash log. Success if there is no flash log.(Can test flash log by "MEInfo -FWSTS") Repeat this procedure for the remaining number of cycles desired in the stress test.		
Pass Criteria	Test passes if all steps are completed successfully, for at least the recommended number of iterations as set by the OEM per the tolerance level of the system design. Suggested Iterations: Mobile: >=2000, Desktop/AIO: >=750		

11.8 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.		



<table>
<tr><td>ID</td><td>PM_ST_35</td></tr>
<tr><td>Configuration</td><td>If Deep S5 is supported on the SUT, confirm the following:
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.
This test assumes that either LAN-only, WLAN-only, or both LAN and WLAN network interfaces are available on the SUT.</td></tr>
<tr><td>Parameters</td><td><table>
<tr><td colspan="2">System Power Source</td><td>AC+DC or AC-only</td></tr>
<tr><td rowspan="4">Power States</td><td>Initial</td><td>S0/MeOn (CM0,CM0-PG)</td></tr>
<tr><td>Middle</td><td>S5,Deep S5/MeOff (CM-Off)</td></tr>
<tr><td>Final</td><td>S0/MeOn (CM0,CM0-PG)</td></tr>
<tr><td>Trigger</td><td>Host OS shutdown ➲ Power Button press</td></tr>
</table></td></tr>
<tr><td>Setup</td><td>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</td></tr>
<tr><td>Procedure</td><td>Shutdown the SUT via the Host OS.
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).
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 0x6<u>0</u>xxxxxx.
Ensure that yellow bang is not seen on Drivers in Device Manager
Check if there are any flash log. Success if there is no flash log.(Can test flash log by “MEInfo -FWSTS”)
Repeat this procedure for the remaining number of cycles desired in the stress test.</td></tr>
<tr><td>Pass Criteria</td><td>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</td></tr>
</table>

§ §

12 Intel® Dynamic Application Loader (Intel® DAL)

Intel® Dynamic Application Loader (Intel® DAL) is an Intel® CSME infrastructure for applications such as Intel® Identity Protection Technology (Intel® IPT).

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.

Note: Intel® IPT testing is out of this compliance guide scope. Intel® IPT has a dedicated kit which includes compliance and collateral (available on VIP and in a separate Intel® PETS package).

12.1 Test Environment

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.

Note: DAL Applet needs to be signed with RSA 3K due to CSE signing method upgrade.

12.1.1 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.

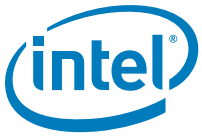
Package Compliance_DAL.xml should be loaded to Intel® PETS in order to compete the tests in this section.

12.1.2 Verifying if Required Software is Installed on 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).



12.2 Test Coverage Summary

Table 12-1. Compliancy Tests for Verifying that Intel® DAL 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 Kaby Lake SKUs
2. OS: Test runs on Microsoft* Windows* 7/8.x/10 only will.

Test ID	DAL_001
Test Case Title	Intel® DAL applications cleanup
Mandatory/Optional	Mandatory for those who implement Intel® IPT
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	Start test DAL_001 in the Intel® Platform Enablement Test Suite from management console. **Intel® Platform Enablement Test Suite performs the following steps:** 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 for those who implement Intel® IPT
Firmware SKU	Consumer and Corporate SKUs (Desktop, Mobile and Intel® Ultrabook™)
Description	Intel® DAL test application is installed and loaded, verifying basic functionality of Intel® DAL applications execution capability.

Test ID	DAL_002
Objective	To test that the Intel® Dynamic Application Loader basic functionality works properly.
Procedure	Start test DAL_002 in the Intel® Platform Enablement Test Suite from management console. Intel® Platform Enablement Test Suite performs the following steps: 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"

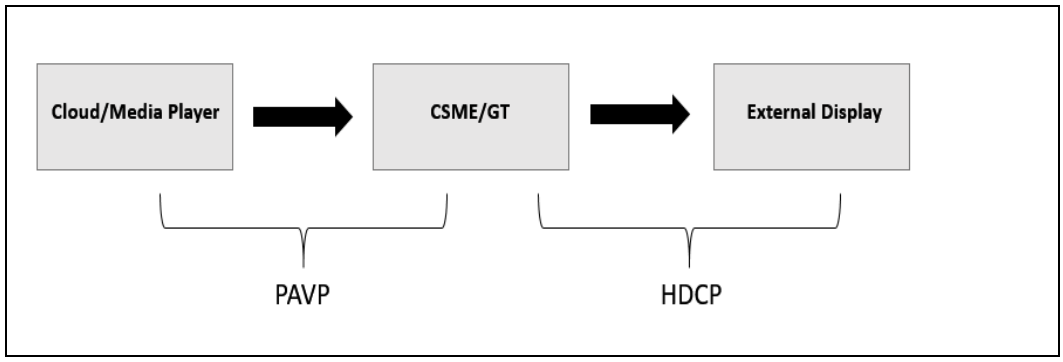
Test ID	DAL_003
Test Case Title	Intel® DAL communication channel exercise
Mandatory/Optional	Mandatory for those who implement Intel® IPT
Firmware SKU	Consumer and Corporate SKUs (Desktop, Mobile and Intel® Ultrabook™)
Description	Intel® DAL test application is installed and loaded, followed by a communication channel exercise between application and host side application.
Objective	To test that the Intel® Dynamic Application Loader application can communicate successfully with a host application.
Procedure	Start test DAL_003 in the Intel® Platform Enablement Test Suite from management console. Intel® Platform Enablement Test Suite performs the following steps: 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”

§ §

13 Protected Media Playback

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

- Intel® Protected Audio Video Path
- 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 support premium content video playback including Blu-ray discs and 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.

13.1 Scope

This chapter describes a validation strategy for protected content Protected Media Playback. This chapter is intended for validation purposes. 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.

13.2 Prerequisite

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® FP):** Is available in Windows* 32-bit (fptw.exe), Windows 64-bit (fptw64.exe) operating systems, EFI 32-bit and EFI 64-bit.

13.3 Test Environment Setup

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).

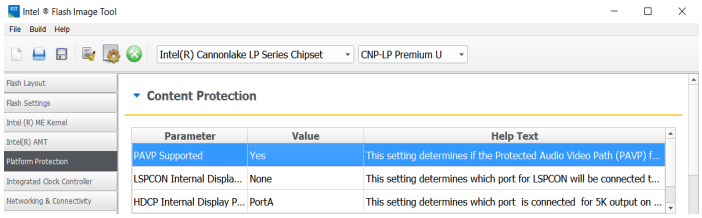
13.4 Media Playback Test Coverage Summary

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

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

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

Test ID	Test Case Title	PETS/Manual	OS Supported	Form Factor
Media_001	Verify default configuration settings for Protected Audio Video Path [PAVP] in Firmware Image Tool [FIT]	Manual	W WI	DT/MB/HE-DT
Media_004	Verify PAVP Enabled in BIOS (***Only if the SUT BIOS menu displays PAVP Mode***)	Manual	W WI	DT/MB/HE-DT

Test ID	Media_001
Test Case Title	Verify default configuration settings for Protected Audio Video Path [PAVP] in Firmware Image Tool [FIT]
Platform	TGL
Mandatory/Optional	Mandatory
Mobile Only	No
Firmware SKU	Consumer/Corporate
Description	Intel® CSME initiates PAVP secure session in firmware for key exchange and encryption for Content from Media player or cloud. PAVP can be enabled or disabled using FIT Tool. In this test we verify the PAVP is enabled in the SUT SPI image using FIT.
Objective	Verify if the PAVP control in Intel® FIT are set correctly
Procedure	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_004
Test Case Title	Verify PAVP Enabled in BIOS
Platform	TGL
Mandatory/Optional	Mandatory (Only if the SUT BIOS menu displays PAVP Mode)
Mobile Only	No
Firmware SKU	Consumer/Corporate
Description	PAVP can be configured in the BIOS. In this test we verifies what the PAVP mode is enabled in SUT BIOS.
Objective	Verify PAVP configuration in BIOS

Test ID	Media_004
Procedure	1. Boot system to BIOS menu. 2. Navigate in your BIOS menu where you have PAVP Option [example: in Intel BIOS goto - Intel Advance Menu->System Agent (SA) Configuration->Graphics Configuration-> PAVP Enable 3. Verify the PAVP mode setup. 
Test Pass/Fail Criteria	Test passes if we PAVP is enabled in SUT BIOS.

§ §

14 Intel® Integrated Clock Control Compliancy

This chapter covers details of ICC test cases supported by all TGL 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
TGL-LP SKUs	• Standard • Adaptive
TGL-H SKUs	• Standard • Adaptive • Overclocking

BCLK Overclocking recommendation for TGL-H SKUs:

- BCLK Overclocking > 100 MHz is achievable using ICC SDK ->
- This profile is added to support BCLK OC frequency >100 MHz when using warm reset flow.
- Overclocking Extended profile supports single 100–538.25 MHz BCLK frequency range. Customers are recommended to use this profile for overclocking.

ICC Profile and parameters configuration recommendation:

- Review the FW Bringup Guide to get familiar with supported frequency and SSC configurations for above features.
- OEMs are recommended to configure ICC Boot profile and parameters for the profile via Intel® FIT -> ICC tab. Make sure to choose appropriate profile and configure parameters to meet platform and HW requirements.

CCT Tool usage:

- for manual testing, ICC SDK is located under ../System_Tools/ICC Tools/.

ICC PETS test package details:

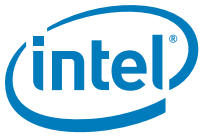
The test cases supported by platforms using Intel® Platform Enablement Test Suite (Intel® PETS) are defined as a part of Compliance_ICC_*.xml. Select respective ICC package since this version of PETS supports different PCHs.

- For TGL-LP SKUs, select xml file from:../TGL/../**Compliance_ICC_TGL-LP**
- For TGL-H SKUs, select xml file from:../TGL/../**Compliance_ICC_TGL_H**

Note: Pets automation will available in future releases.

14.1 TGL-LP and TGL-H Intel® Integrated Clock Control Test Coverage Summary

Test ID	Test Case Title	Mandatory	PETS/ Manual	Applicable to PCH SKU	Network Factor
ICC_TST_01	Test default settings for Standard configuration	Yes (Only mandatory when SUT's boot profile is selected based on standard profile under FIT or by means of BIOS)	PETS /Manual using ICC SDK embedded	• TGL- LP • TGL-H	LAN+WLAN; WLAN only
ICC_TST_02	Test default settings for Adaptive configuration	Yes (Only mandatory when SUT's boot profile is selected based on adaptive profile under FIT or by means of BIOS)	PETS/Manual using ICC SDK embedded	• TGL-LP • TGL-H	LAN+WLAN; WLAN only
ICC_TST_03	Test default settings for Overclocking configuration	Yes (Only mandatory when SUT's boot profile is selected based on overclocking Ext. profile under FIT or by means of BIOS)	PETS/Manual using ICC SDK embedded	• TGL-H	LAN+WLAN; WLAN only
ICC_TST_04	Test Get and Set of MPHY setting	Yes	PETS/Manual using ICC SDK embedded	• TGL-LP • TGL-H	LAN+WLAN; WLAN only



14.2 Test Cases

14.2.1 Standard Configuration Test Default Settings

Test ID	**ICC_TST_01**
Test Case Title	Test default settings for Standard configuration
Mandatory/Optional	Mandatory. ***Notes:*** 1. Only for SUTs with boot profile that to "standard" profile under FIT ->ICC -> Boot Profile or by means of BIOS 2. 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. 3. For BIOS, Check parameter using the request to HECI: ICC_GET_PROFILE_REQ if Boot profile selection is based on Standard profile, then this test is mandatory otherwise it can be skipped.
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	Get BCLK PLL Settings: • API: ICC_GET_CLOCK_SETTINGSEx • library method: *EXTERNAL_API UINT32IccLibGetCurrentClockSettingsWrapper(const ICC_HECI_CLOCK_ID clockId, ICC_GET_CLOCK_SETTINGSEx * const clockSettings);* An error should be returned in case the test has failed
Test Pass/Fail Criteria	Pass if the critical ICC registers values read are set correctly based on the standard configuration. Frequency= 400 MHz SSC = 0.5 ***Notes:*** 1. For FIT, Check parameter under Flash Image Tool| Integrated Clock Controller | Boot profile selection. If Boot profile is not based on standard profile then this test is expected to fail. 2. For BIOS, check parameter using the request to HECI : ICC_GET_PROFILE_REQ if Boot profile is not based on standard profile then this test is expected to fail.

14.2.2 Test Default Settings for Adaptive Configuration

Test ID	**ICC_TST_02**
Test Case Title	Test default settings for Adaptive configuration
Mandatory/Optional	Mandatory 1. Only for SUTs with boot profile that to "standard" profile under FIT ->ICC -> Boot Profile or by means of BIOS 2. 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. 3. For BIOS, Check parameter using the request to HECI: ICC_GET_PROFILE_REQ if Boot profile selection is based on Standard profile, then this test is mandatory otherwise it can be skipped.
Description	Verify if the current ICC registers setting in the SUT are set correctly based on Adaptive configuration

Test ID	**ICC_TST_02**
Objective	Ensure that critical ICC register values match defaults for Adaptive configuration
Procedure	Get BCLK PLL Settings: • API: _ICC_SET_CLOCK_SETTINGSEx • Library method: *EXTERNAL_API UINT32IccLibGetCurrentClockSettingsWrapper(const ICC_HECI_CLOCK_ID clockId, ICC_GET_CLOCK_SETTINGSEx * const clockSettings);* An error should be returned in case the test has failed Set the BCLK PLL settings: • API: _ICC_SET_CLOCK_SETTINGSEx • Library method: EXTERNAL_API UINT32 IccLibSetCurrentClockSettingsWrapper(const ICC_HECI_CLOCK_ID clockId, ICC_SET_CLOCK_SETTINGSEx * clockSettings); An error should be returned in case the test has failed
Test Pass/Fail Criteria	Pass if the critical ICC registers values read are set correctly based on the Adaptive configuration. ***Notes:*** 1. For FIT, Check parameter under Intel® Flash Image Tool| Integrated Clock Controller | Boot profile selection. If Boot profile is not based on Adaptive profile then this test is expected to fail. 2. For BIOS check parameter using the request to HECI : ICC_GET_PROFILE_REQ if Boot profile selection is based on Adaptive profile, then this test is mandatory otherwise it can be skipped. 3. Default frequency and SSC supported for Adaptive is 97.5MHz with 0.50%. Supported Min.-Max. frequency range is [97.5- 100 MHz]. This test checks default configuration for Adaptive clocking. Test may fail if customer change SSC or frequency from default value; however make sure to check if settings are within the expected range supported for Adaptive clocking.

14.2.3 Overclocking Configuration Test Default Settings

Test ID	**ICC_TST_03**
Test Case Title	Test default settings for Overclocking Ext. configuration
Mandatory/Optional	**Applicable to TGL-H consumer SKUs only**; Mandatory - Only for SUT's boot profile is selected based on overclocking Ext. profile under FIT or by means of BIOS. ***Notes:*** 1. For FIT Tool, Check parameter under FIT| Integrated Clock Controller | Boot profile selection. if boot profile selection is based on Overclocking Ext. profile, This test is mandatory else you can skip to execute it. Or, 2. BIOS check parameter using the request to HECI : ICC_GET_PROFILE_REQ if Boot profile selection is based on Adaptive profile, then this test is mandatory otherwise it can be skipped.
Description	Verify if the current ICC registers setting in the SUT are set correctly based on Overclocking Ext. configuration
Objective	Ensure that critical ICC register values match defaults for Overclocking Plus configuration
Procedure	Get BCLK PLL Settings: • API: _ICC_SET_CLOCK_SETTINGSEx • Library method: *EXTERNAL_API UINT32IccLibGetCurrentClockSettingsWrapper(const ICC_HECI_CLOCK_ID clockId, ICC_GET_CLOCK_SETTINGSEx * const clockSettings);* An error should be returned in case the test has failed Set the BCLK PLL settings: • API: _ICC_SET_CLOCK_SETTINGSEx • Library method: EXTERNAL_API UINT32 IccLibSetCurrentClockSettingsWrapper(const ICC_HECI_CLOCK_ID clockId, ICC_SET_CLOCK_SETTINGSEx * clockSettings); An error should be returned in case the test has failed
Test Pass/Fail Criteria	Pass if the critical ICC registers values read are set correctly based on the Overclocking Plus configuration. ***Notes:*** 1. For FIT, Check parameter under Flash Image Tool | Integrated Clock Controller | Boot profile selection. **If Boot profile is not based on Overclocking Ext. profile (for example, Standard, Adaptive, OverclockingEx), this test is expected to fail.** 2. Make sure to refer to BCLK Overclocking recommendation mentioned in this chapter. 3. Default frequency and SSC supported for Overclocking Ext. is 100 MHz with 0.5%. Supported Min-Max frequency range is [97.5 - 538.25 MHz]. This test checks default configuration for Overclocking Ext. clocking. Test may fail if customer change SSC or frequency from default; however make sure to check if settings are within the expected range supported for Overclocking Ext clocking.

14.2.4 GET and SET MPHY Settings

Test ID	**ICC_TST_04**
Test Case Title	Get and Set of MPHY setting
Mandatory/Optional	Mandatory, This is informative test.
Description	This test output high level detail like CRC count into a bin file , Version and product detail of chipset initialization settings. This test apply a new version of chipset User to manually verify data is correct or not.

Test ID	**ICC_TST_04**
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. Apply a new version of chipset initialization settings

Procedure	GET MPHY Version:
	API:_GET_MPHY_VERSION
	library method: EXTERNAL_API UINT32 IccLibGetMphyVersion(GET_MPHY_VERSION *survTable);
	
	GET MPHY table:
	library method: EXTERNAL_API UINT32 IccLibGetMphySettingsWrapper(UINT32 length, UINT32 offset, UINT8 *buffer,UINT32 *bytesRead);
	
	Set MPHY table:
	library method: EXTERNAL_API UINT32 IccLibSetMphySettingsWrapper(char *mphyFileName);
	Notes:
	1. 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.
	2. This test currently displays the command result only.

Test Pass/Fail Criteria	This is informative test and displays details like CRC count, Version and product detail. User to manually confirm if data looks correct or not.

§ §

15 Manufacturing Flow Simulation Test

15.1 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: [1]Form 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 is costly.

Test ID	MFG_001
Procedure	**Test Environment:** • System configuration should be as close as possible to what it is 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) **Test Preparation:** • Configure the desired secure boot setting (OEM public key hash, policy, and so forth) for Intel® Boot Guard and Intel® PTT Supported [FPF] for PTT and all the variables in MEManuf.xml under EOL VAR TEST session. • If this test is conducted on platform with **production configuration and ready to run EOM flow**, also configure the desired secure boot setting (OEM public key hash, policy, and so forth.) for **Intel® Boot Guard** and **Intel® PTT Supported [FPF]** for PTT in MEManuf.xml under **EOL CONFIG Test** session. **Test Procedure:** 1. Use the version of FPT and, MEManuf executable suitable for the chosen OS environment (located in the latest Intel® CSME kit) to simulate at least the Intel® CSME Manufacturing reference flow (Below steps). 2. If using pre-lock (the descriptor Master Access permission set to Intel recommended production value during image preparation), do only steps 5 and 8. 3. Reprogram the image currently on board (e.g. image.bin). Example: FPTW64.exe –f image.bin 4. Reset Intel® CSME and Host after program successfully Example: FPTW64.exe –greset 5. Verify Intel® CSME Example: MEManufWin64.exe Example (option): MEManufWin64.exe -f MEManuf.xml (use the MEManuf.xml configuration file configured during preparation) 6. Check Intel® Boot Guard, PTT, and all the variables match with setting configured in FIT Example: MEManufWin64.exe -EOL var -f MEManuf.xml (use the MEManuf configuration file configured during preparation) 7. 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 Example: FPTW64.exe –closemnf –y ***Note:*** PDR, EC BIOS or legacy addition could be used following FPTW64.exe –closemnf –y to allow various CPU/BIOS read/write access setting based on customer need. Check System Tool User Guide for more detail. 8. Perform end of line check on Intel recommended default test item and also Intel® Boot Guard, PTT, and all the configuration check a. Example: MEManufWin64.exe -EOL (It runs Intel recommended default test) or b. Example (option): MEManufWin64.exe -EOL config -f MEManuf.xml (use the MEManuf.xml configuration file configured during preparation with more sub tests enabled) ***Note:*** It is highly recommended user create the own script file to automatically run the above steps in order to better simulate the manufacturing flow.
Test Pass/Fail Criteria	Pass only when all the tools run above return pass result. ***Notes:*** When encounter failure, check below: 1. CRB test result in Compliance kit 2. Intel® CSME Firmware release note for known issues.

§ §

16 Intel® Device Protection Technology with Intel® Boot Guard

16.1 Overview

Intel® Boot Guard (BtG) formerly Anchor Cove (AnC) is an Intel platform boot integrity protection technology. Intel® Boot Guard can protect the platform boot integrity by preventing execution of unauthorized boot block. With Intel® Boot Guard, the OEM can create a platform boot policies, such that invocation of an unauthorized (or compromised) boot block triggers the platform protection per the OEM policies. Based in the hardware, Intel® Boot Guard also extend the trusted boundary of the platform boot process down to the hardware. A benefit of this protection is that Intel® Boot Guard can help OEM maintains platform integrity by preventing reuse of the OEM hardware to run unauthorized software stack.

Note: *The terms Intel® Boot Guard* and *Anchor Cove* may be used interchangeably in this section.

16.2 Scope

This chapter describes a validation strategy for Intel® Boot Guard. This chapter is intended for validation purposes. The objective is to provide validation professionals with additional insight into Intel® Boot Guard by highlighting validation considerations. This chapter is not a technology overview and does not replace the existing Intel® Boot Guard collateral. The reader is expected to be familiar with Intel® Boot Guard and to use this document as a validation supplement to develop his own validation plan.

16.3 Prerequisite

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

Table 16-1. Intel® Boot Guard Tools for Testing (Sheet 1 of 2)

Tool/Component	Revision	Comments
FIT	ME firmware kit with Intel® Boot Guard support	**FIT** is required to define the Intel® Boot Guard Boot Policies (persistent policies). Available on VIP
MEInfo	ME firmware kit with Intel® Boot Guard support	**MEInfo** is required to confirm Intel® Boot Guard Policies. Available on VIP ***Note:*** **Non-Windows* OS**: Use the EFI version of the CSME tools (MEinfo.efi) to confirm Intel® Boot Guard Policies

Table 16-1. Intel® Boot Guard Tools for Testing (Sheet 2 of 2)

Tool/Component	Revision	Comments
TXTBtgInfo.efi	0.7.10 or higher	TXTBtgInfo.efi can be used to confirm Intel® Boot Guard status in the test cases below. Training videos for TXTBtgInfo are available on PCDC under Ingredients->Technologies->Intel® Boot Guard->Latest Videos Intel® Boot Guard status can also be determined using various platform status registers: 1. Refer to BIOS Writers Guide for status registers (Example: ERRORCODE, BOOTSTATUS, ANC_SACM_INFO) usage 2. Refer to ME BIOS Writer's Guide for Intel® Boot Guard related FWSTS registers verification.

16.4 Intel® 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.

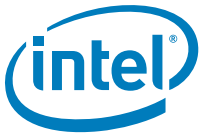
Note: Successful Intel® Boot Guard on S3 Resume has been removed as TXTBtgInfo.efi tool runs only from EFI shell.

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

Test ID	Test Case Title
BtG_001	Successful VM (Verified Measured) Boot to OS[1]
BtG_002	Unsecure Boot to OS[1]
BtG_003	Failed VM (Verified Measured) Boot fail to Fallback
BtG_004	Platform Public Signing Key Provisioned
BtG_005	Successful VM (Verified Measured) Boot to OS[1] using FPF
BtG_006	BIOS Update Procedure includes Signature Verification
BtG_007	Service Center's Recovery process for Intel® Boot Guard failed platform
BtG_008	BIOS Continues the Chain of Trust

[1] Refer to Section 1.1 for supported Operating Systems (OS).

Test ID	BtG_001
Test Case Title	Successful Verified-Measured (VM) Boot to OS
Mandatory/Optional	Mandatory
Firmware SKU	Consumer / Corporate
Description	In this test case, Intel® Boot Guard performs a successful verification and measuring of the SUT Initial Boot Block (IBB.) Upon successful verification Intel® Boot Guard passes 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 Intel® Boot Guard for IBB verification and measurement

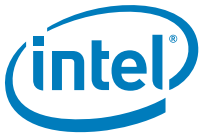


Test ID	BtG_001
Procedure	**Prepare the SUT Persistent Policy (FPF)** 1. Provision the SUT Persistent Policies (NVAR, if this is development system) to either the VM or FVE or FVME profile. Per the testing objective: — **The *FVME* profile usage is not advised for the development or testing environment.** In this strictest protection mode, test failure requires BIOS flashing to restore the system. — Refer the ME Firmware Bring Up Guide for information on the Intel® Boot Guard related FIT options and settings 2. Install the Intel® ME firmware and BIOS image that are Intel® 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 SUT. 4. 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. **Verify the Boot** 5. Power-off the SUT. 6. Power-on the SUT. 7. Boot to EFI shell and execute TXTBtgInfo.efi 8. Verify the TXTBtgInfo.efi output to confirm that Intel® Boot Guard has booted as configured to verify and measure the IBB. 9. Boot to OS. 10. Execute PETS package for Intel® Boot Guard from Remote Console 11. Verify PETS results should Pass
Test Pass/Fail Criteria	Test passes, if the SUT: • 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 Intel® Boot Guard was successful.

Test ID	BtG_002
Test Case Title	Unsecure Boot to OS
Mandatory/Optional	Mandatory
Firmware SKU	Consumer / Corporate
Description	In this test case, Intel® Boot Guard performs a successful un secure boot of SUT Initial Boot Block (IBB.) Upon successful completion Intel® Boot Guard 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** Intel® Boot Guard verification and measuring of the IBB.

Test ID	**BtG_002**
Procedure	**Prepare the SUT Persistent Policy (FPF)** 1. Verify *Persistent Policies* on the SUT set to default (that is, all '0') or set the *No_FVME* profile. — Refer the ME Firmware Bring Up Guide for information on the Intel® Boot Guard related FIT options and setting. 2. Install the Intel® CSME firmware and BIOS image that are Intel® 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. **Verify the Boot** 5. Power-off the SUT. 6. Power-on the SUT. 7. Boot to EFI shell and execute TXTBtgInfo.efi. 8. Verify the TXTBtgInfo.efi output to confirm that Intel® Boot Guard has booted as configured to verify and measure the IBB. 9. Boot to the targeted OS. 10. Execute PETS package for Intel® Boot Guard from Remote Console. 11. Verify PETS results should Pass.
Test Pass/Fail Criteria	Test passes, if the SUT: • Boots fully functional to OS. • PETS tests BootGuard_001 and BootGuard_002 should Pass. • TXTBtgInfo.efi reports that Intel® 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, Intel® Boot Guard performs an unsuccessful verification and measuring of the SUT Initial Boot Block (IBB.) Upon verification failure Intel® Boot Guard performs the fallback behavior per the persistent policy.
Objective	This test verifies that the SUT has all the required components: hardware, firmware, ACM, and BIOS. Additionally, the SUT has been correctly provisioned in manufacturing for the platform to handle failure condition per the SUT targeted security objective

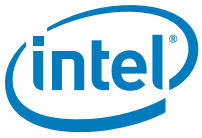


Test ID	BtG_003
Procedure	**Prepare the SUT Persistent Policy (FPF)** 1. Provision the SUT *Persistent Policies* (NVAR if this is development system) to either the *VM or FVE* or *FVME* profile. Per your testing objective. — **The *FVME* profile usage is not advised for the development or testing environment.** In this strictest protection mode, test failure requires BIOS flashing to restore the system. — Refer the ME Firmware Bring Up Guide for information on the Intel® Boot Guard related FIT options and settings. 2. Install the Intel® ME firmware and BIOS image that are Intel® 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 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. **Prepare the SUT BIOS** 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. **Verify the Boot** 6. Power-off the SUT. 7. Power-on the SUT. 8. Execute PETS package for Intel® Boot Guard from Remote Console. 9. Verify PETS results should Fail. 10. Verify that the platform has failed per the persistent policy. — Refer to the Intel® Boot Guard for HSW-ULT to details on expected failure handling behavior for the SUT.
Test Pass/Fail Criteria	Test passes, if the SUT exhibit the failure condition as expected per the configured profile: • ***FVE*** - The platform halts upon verification failure. • ***FVME*** - The platform halts upon verification failure. • ***VM*** - The platform would not halt upon verification failure.

Test ID	BtG_004
Test Case Title	Platform Public Signing Key Provisioned
Mandatory/Optional	Mandatory
Firmware SKU	Consumer / Corporate
Description	In this test case, the platform public signing key is verified to be provisioned for the platform.
Objective	This is intended to be a check of the OEM signing capability and persistent policy provisioning process.
Procedure	**Prepare the SUT Persistent Policy** 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 — **The *FVE* profile usage is not advised for the development or testing environment.** In this strictest protection mode, test failure requires BIOS flashing to restore the system. **Verify the signing key in the Persistent Policy** 2. Boot the SUT to OS. 3. Run MEInfo.exe. 4. Evaluate the Intel® Boot Guard related fields: a. "FPF" for committed Persistent policies b. "ME" for NVAR stored Persistent policies
Test Pass/Fail Criteria	Test passes, if the SUT: • 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	Intel® Boot Guard feature testing using Field programmable Fuse (FPF) values
Mandatory/Optional	Mandatory
Firmware SKU	Consumer / Corporate
Description	In this test case, Intel® Boot Guard performs Intel® Boot Guard feature testing using the values from the FPFs that is, accessing the Intel® Boot Guard profile values from the FPFs instead of the Flash variables that is, NVARs). ***Note:*** This test can be skipped if test BtG_001 or BtG_004 were completed using FPF Persistent Policies.
Objective	This test performs and validates all the components used in the Intel® Boot Guard feature that is, hardware, firmware, ACM and BIOS. It also tests that the platform is properly provisioned for Intel® Boot Guard IBB verification and measurement from the Field Programmable Fuses (FPFs).
Procedure	**Pre-requisite**: Perform this test ONLY, when all the tests (BtG_001 to BtG_006) have passed by testing Intel® Boot Guard using the profile values from the NVARs (flash variables). **Important**: The profile selected to be committed into FPFs becomes the final profile, which cannot be altered later. It is not possible to return the system to a pre-test configuration state, once FPF has been committed. As such, care must be taken to ensure that the proper test pre-requisites have been completed before proceeding. 1. Perform the step to commit the Intel® Boot Guard profile values to the FPFs. This is done automatically after CSME Manufacturing mode is disabled (during the global reset from FPT -closemnf or first boot for Pre-Lock image), if firmware and MCP combination is Production. Or Done by means of a specific FPF MEI command (if combination of firmware and MCP is Pre-production). Below commands can be used for FPF commit on pre-production platforms. (Also refer the CSME Tools guide for the tools usage). - "FPT -FPFs" - To retrieve the FPF names. - "FPT -COMMITFPFS <FPFname>" - To commit values to FPFs one at a time. - "FPT -COMMITFPF All" - To commit values to FPFs all at once. 2. Run MEinfo tool to view the values set in the FPFs and the NVAR-FPF mismatch field. If there is a mismatch, tool indicates it with a FPF mismatch message. 3. Execute the tests (Test ID BtG_001 or BtG_004) based on the profile that has been committed on the FPFs.
Test Pass/Fail Criteria	Test passes, if the SUT: • The FPF commit command is successfully executed and • MEinfo tool O/P shows the correct Intel® Boot Guard profile settings and values under the "FPF" column for each Intel® Boot Guard variable. • Further Fail/Pass criteria is the same as criteria mentioned for each of the tests above (test id #BtG_001 or BtG_004).

Test ID	**BtG_006**
Test Case Title	BIOS Update Procedure includes Signature Verification
Mandatory/Optional	Optional
Firmware SKU	Consumer / Corporate
Description	This is a manual assessment of the platform BIOS update process to ensure that signature verification is applied to maintain BIOS integrity.
Objective	Confirm the signature authorization structure defined by the Persistent Policy (FPF)->KM->BPM->IBB are maintained in your BIOS update process.
Procedure	Confirm with the BIOS Development team that BIOS update process is using proper authorization process to maintain the Intel® Boot Guard authorization structure from FPF->KM->BPM->IBB.



Test ID	BtG_006
Test Pass/Fail Criteria	Test passes, if the SUT: • If the BIOS update process contains the proper checks to maintain the Intel® Boot Guard signature authorization structure.

Test ID	BtG_007
Test Case Title	Service Center's Recovery process for Intel® Boot Guard failed platform
Mandatory/Optional	Optional
Firmware SKU	Consumer / Corporate
Description	This is a manual assessment of the platform service process to ensure that platforms that has failed Intel® Boot Guard verification can be recovered to fully functional state
Objective	Confirm that a service process is established to handle Intel® Boot Guard failure per your configured persistent policy
Procedure	Evaluate the platform service process for the failed Intel® Boot Guard scenario. Does the service process meet the platform business objective?
Test Pass/Fail Criteria	Test passes, if the SUT: • If the platform recovery process meets the business objective.

Test ID	BtG_008
Test Case Title	BIOS Continues the Chain of Trust
Mandatory/Optional	Optional
Firmware SKU	Consumer / Corporate
Description	This is a manual test to confirm that the BIOS has taken the required steps to protect and continue the chain of trust from Intel® Boot Guard.
Objective	Ensure that the SUT maintains the secure boot value proposition from when Intel® Boot Guard completes to when the UEFI Secure Boot protection are implemented in the BIOS.
Procedure	Confirm with the BIOS Development team that IBB and the next boot phase is protecting the integrity of the secure boot on the platform, as recommended in the Intel® Boot Guard BIOS Writer's Guide, when it receives platform controls from the Intel® 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

§ §

17 Intel® Platform Trust Technology (Intel® PTT) Compliancy

Intel® Platform Trust Technology (Intel® PTT) is the Intel implementation of TCG TPM 2.0 standard in firmware. For more information about Intel® PTT integration with BIOS refer BIOS Writers Guide and Intel® PTT Overview documentation.

The purpose of this section is to describe the tests required to verify PTT is functional, main PTT end to end use cases are working and platform meets Windows* 10 requirements for TPM 2.0 support.

The scope of this section is end to end testing and is not intended to provide TPM command level testing.

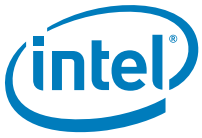
Note: Intel® Boot Guard testing with Intel® PTT is out of scope of this chapter and should be done as part of Intel® Boot Guard testing.

Test Environment for PTT Compliancy Section:

- Tiger 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 Compliancy kit release. Refer to the Intel® Platform Enablement Test Suite (Intel® PETS) user guide available in the Intel Compliancy kit for exact instructions on how to load and setup the Intel® Platform Enablement Test Suite (Intel® PETS) software.
- Windows* 10 HLK Testing Environment
- manage-bde.exe (Windows* command line tool for BitLocker Driver Configuration)
- bdehdcfg.exe (Windows* command line tool for BitLocker Drive Encryption)
- makecert.exe (command line tool, part of Windows* 10 SDK)
- pvk2pfx.exe (command line tool, part Windows* 10 SDK)
- CertUtil.exe (Windows* 10 Command line tool)

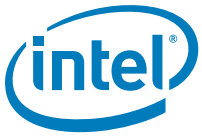


17.1 Test Coverage Summary

Test ID	Test Case Title	PETS/Manual
PTT_001	CRB Interface Communication Test	PETS
PTT_002	Intel® PTT Windows* 10 Basic Functionality	PETS
PTT_003	TPM Clear and Physical Presence	PETS
PTT_004	Windows* 10 BitLocker Integration	PETS
PTT_005	Windows* 10 BitLocker TPM Protection	PETS
PTT_006	Windows* 10 Virtual Smart Card (VSC) Tests	PETS
PTT_007	Microsoft* Windows* HLK TPM Tests	Manual ***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.
PTT_008	Intel® PTT Enable/Disable from BIOS	Manual
PTT_009	Power Transition Testing with Intel® PTT Enabled	PETS
PTT_010	Dictionary Attack Lockout After Coin Battery Removal with EOM Commit	Manual

17.2 Verifying BIOS and Intel® PTT Communication Over CRB Interface

Test ID	**PTT_001**
Test Case Title	CRB Interface Communication Test
Mandatory/Optional	Mandatory ***Note:*** This test uses CRB access and therefore needs to run with disabled driver to ensure elimination of false failures.
Description	The test confirms that BIOS correctly implements the CRB protocol for communication with Intel® PTT
Objective	Verify BIOS is able to successfully send commands to Intel® PTT
Procedure	1. Confirm Intel® PTT is enabled in the SPI image. 2. Disable the Microsoft* TPM driver: From an Elevated Command Window issue the following command: reg add HKLM\SYSTEM\CurrentControlSet\Services\TPM /f /v ImagePath /t REG_EXPAND_SZ /d \SystemRoot\system32\drivers\tpm.sy_ Reboot the system 3. Relinquish locality 0: Write 1 to TPM_LOC_CTRL_0.Relinquish (0xfed40008, bit 1). 4. Request locality 0: Write 1 to TPM_LOC_CTRL_0.RequestAccess (0xfed40008, bit 0). 5. 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. 6. Write 1 to TPM_CRB_CTRL_REQ_0.cmdReady (0xfed40040, bit 0) 7. Poll TPM_CRB_CTRL_REQ_0.cmdReady every 5 ms for 500 ms until it is 0 8. Verify TPM_CRB_CTRL_STS_0.tpmIdle (0xfed40044, bit 1) is 0 9. Write a TPM command such as TPM2_SelfTest to TPM_CRB_DATA_BUFFER register (0xfed4_0080) 10. Write "1" to the TPM_CRB_CTRL_START register (0xFED4_004C). 11. Poll the TPM_CRB_CTRL_START register (0Xfed4_004C) until its value becomes "0". 12. Write 1 to TPM_CRB_CTRL_REQ_0.goIdle (0xfed40040, bit 1). 13. Poll TPM_CRB_CTRL_REQ_0.goIdle for 500ms until it is 0. 14. Relinquish locality 0: Write 1 to TPM_LOC_CTRL_0.Relinquish (0xfed40008, bit 1). 15. 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. 16. Request locality 0: Write 1 to TPM_LOC_CTRL_0.RequestAccess (0xfed40008, bit 0). 17. Re-enable the Microsoft* TPM driver: From an Elevated Command Window issue the following command: reg add HKLM\SYSTEM\CurrentControlSet\Services\TPM /f /v ImagePath /t REG_EXPAND_SZ /d \SystemRoot\system32\drivers\tpm.sys Reboot the system ***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.

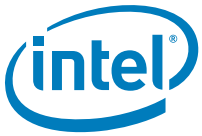


17.3 Intel® PTT Basic Functionality Under Windows* 10

Test ID	**PTT_002**
Test Case Title	Intel® PTT Basic Functionality Under Windows* 10
Mandatory/Optional	Mandatory
Description	Verify Intel® PTT has been enabled on the platform and Intel® PTT is functional on Windows* 10
Objective	Windows* can successfully communicate with Intel® PTT
Procedure	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 Manufacturer Name = **INTC**, TPM Specification Version = **2.0** 5. Verify Status is "The TPM is ready for use." 6. Open an elevated command prompt with admin privileges and enter powershell (type powershell at prompt) 7. Prepare the WMI object for querying Intel® PTT information by typing: *$ptt = get-wmiobject -namespace "root/cimv2/security/microsofttpm" win32_tpm* 8. Check different Intel® PTT parameters by typing the following at the PS prompt: d. $ptt.IsEnabled() e. $ptt.IsActivated() f. $ptt.IsAutoProvisioningEnabled() g. $ptt.IsOwned() h. $ptt.IsReadyInformation()
Test Pass/Fail Criteria	No "yellow bang" in device manager, Intel® PTT is the TPM device and all TPM queries return "true". ***Note:*** Manufacturer version matches the firmware version.

17.4 Trusted Platform Module (TPM) Clear and Physical Presence

Test ID	**PTT_003**
Test Case Title	TPM Clear and Physical Presence
Mandatory/Optional	Mandatory
Description	TPM Clear command erases user data on the TPM. TPM Clear requires BIOS to check for physical presence to authorize the TPM Clear operation. We saves 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	1. Save the current SrkPublicKey by performing the following actions: a. Open elevated command prompt and enter PowerShell by typing “powershell” at the prompt and type: b. $ptt = get-wmiobject -namespace "root/cimv2/security/microsofttpm" win32_tpm c. $ret = $ptt.GetSrkPublicKeyModulus() d. $ret.SrkPublicKeyModulus > SrkPubModOld.txt 2. Run “tpm.msc” to open TPM Management Console 3. 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 authorizes, ESC rejects the operation. 6. Upon booting to Windows*, pop-up window shows up indicating OS is taking ownership of the TPM 7. After ownership operation completes, press OK. 8. Save the new SrkPublicKey by performing the following actions: a. Open elevated command prompt and enter PowerShell by typing “powershell” at the prompt and type: b. $ptt = get-wmiobject -namespace "root/cimv2/security/microsofttpm" win32_tpm c. $ret = $ptt.GetSrkPublicKeyModulus() d. $ret.SrkPublicKeyModulus > SrkPubModNew.txt 9. Compare the old and new keys
Test Pass/Fail Criteria	OS takes ownership of TPM, new/old keys differ

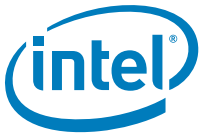


17.5 Windows* 10 BitLocker Integration

Test ID	**PTT_004**
Test Case Title	Windows* 10 BitLocker Integration
Mandatory/Optional	Mandatory
Description	BitLocker uses Intel® PTT to store and retrieve keys securely, in addition Windows* BitLocker confirms system components did not change by checking system load measurements saved to TPM. The test verify BitLocker can be activated, BitLocker can encrypt, decrypt, and restart encryption after reboot.
Objective	Test BitLocker integration with Intel® PTT
Procedure	1. In elevated permissions command line run: "bdehdcfg.exe –driveinfo" and check system drive is configured to support BitLocker 2. Set BitLocker to use TPM for measuring boot devices in Windows* Group Policy by: a. Run "gpedit.msc" to open Group Policy Editor b. Open "Local Computer Policy" > "Computer Configuration" > "Administrative Templates" > "Windows Components" > BitLocker Drive Encryption" > "Operating System Drives" c. On the right pane double click "Configure TPM platform profile for native UEFI firmware configuration" d. Check the enabled radio button. Verify PCR 0, PCR2, PCR4 and PCR11 are checked in the "Options" pane. e. Click apply and OK. f. Commit the group policy change by typing "gpupdate /force" in an elevated command prompt ***Note:*** This action is required once per OS installation. 3. Set up tpm as a BitLocker protector with recovery password and turn-on BitLocker by typing the following at the command prompt a. manage-bde -protectors -add c: -tpm b. manage-bde -protectors -add c: -rp 000000-000000-000000-000000-000000-000000-000000-000000 c. manage-bde -on c: d. shutdown –r –t 0 4. 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 5. After encryption reaches 10%, restart system, and verify encryption continues without error message after reboot completes. 6. Turn off BitLocker by typing "manage-bde –off c:" at the command line, decryption process should start 7. After decryption process ends, reboot and verify system boots into OS without error message. BitLocker should be off
Test Pass/Fail Criteria	All system boots complete successfully and OS loads.

17.6 BitLocker TPM Protection

Test ID	**PTT_005**
Test Case Title	BitLocker TPM Protection
Mandatory/Optional	Optional
Description	When BitLocker is set to use TPM protection, BitLocker enters recovery mode if any protected component changed during boot. By disabling Intel® PTT, user checks BitLocker is indeed using TPM as key protector.
Objective	Verify BitLocker is using Intel® PTT as a key protector
Procedure	1. Encrypt the OS drive using BitLocker with TPM protection (follow instructions in PTT_004 steps 1 through 5, and wait till drive encryption reaches 10%) 2. Run manage-bde –status and verify drive is "protected" 3. Create a measured boot failure in order to trigger BitLocker Recovery a. In BIOS, choose disable Intel® PTT or send a TPM_Clear command. ***Note:*** Clearing TPM by means of the OS disables BitLocker and would not prompt the user for his recovery password. The TPM must be cleared by the BIOS. b. System should boot into BitLocker recovery screen. Provide the recovery password to continue boot. c. Verify boot completes successfully 4. Disable BitLocker by typing "manage-bde –off c:" at the command line, decryption process should start 5. After decryption process ends, reboot and verify system boots into OS without error message. BitLocker should be off
Test Pass/Fail Criteria	BitLocker completes drive encryption successfully and reboots. System displays BitLocker recovery screen after choosing Disable Intel® PTT or Clear TPM in BIOS setup.



17.7 Virtual Smart Card Tests

Test ID	**PTT_006**
Test Case Title	Virtual Smart Card (VSC) Tests
Mandatory/Optional	Optional
Description	Virtual Smart Card is a new Microsoft* use case for TPMs. More information on VSC can be found on Microsoft* web site. This test verifies a VSC can be created and certificate installed so VSC is accessible
Objective	Intel® PTT can be used to support VSC use case
Procedure	1. Create a VSC running the following command on an elevated command line: tpmvscmgr.exe create /name TPM2VSC /adminkey random /PUK default /pin default /generate 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 banged in device manager 4. Create and import a self-signed certificate into the VSC a. Ensure the following registry keys exist under [HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Cryptography\Defaults\Provider\Microsoft Base Smart Card Crypto Provider]: • "AllowPrivateSignatureKeyImport"=DWord:00000001 • "AllowPrivateExchangeKeyImport"=DWord:00000001 b. Open an elevated command prompt c. Type: MakeCert.exe -sky exchange -r -n "CN=TPM2VSCCert" -pe -a sha1 -len 2048 -ss My -m 36 -sv "TPM2VSCCert.pvk" "TPM2VSCCert.cer" 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: pvk2pfx.exe -pvk "TPM2VSCCert.pvk" -pi 123 -spc "TPM2VSCCert.cer" -pfx "TPM2VSCCert.pfx" –f f. Import the certificate into the smart card using the following command: CertUtil.exe -p 123 -csp "Microsoft* Base Smart Card Crypto Provider" -pin 12345678 -importpfx TPM2VSCCert.pfx AT_KEYEXCHANGE 5. Verify import was successful by examining the certificate in the VSC using the following command: CertUtil.exe -scinfo –pin "12345678". Window allowing to view the certificate pops 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 a. Retrieve the name of the container to use by typing: CertUtil.exe -key -csp "Microsoft* Base Smart Card Crypto Provider" -pin "12345678" -v -privatekey –user b. Use the container name returned in the previous command prefixed to the "[Default Container]" and replace the text in bold: CertUtil.exe -delkey -csp "Microsoft* Base Smart Card Crypto Provider" -pin "12345678" -v -privatekey **"TPM2VSCCert-0d6e6c94-9bd6-4640-aa-63900"** 8. Destroy the VSC by running: `TpmVscMgr.exe destroy /instance ROOT\SMARTCARDREADER\0000`, making sure to use the correct index of the smartcard created
Test Pass/Fail Criteria	VSC created successfully, certificate can be loaded and is persistent across reboot. VSC can be removed after key is deleted.

17.8 Microsoft* Windows* Hardware Lab Kit (HLK) TPM Testing

Test ID	**PTT_007**
Test Case Title	Microsoft* Windows* Hardware Lab Kit (HLK) TPM Testing
Mandatory/Optional	Optional
Description	Windows* 10 Logo requires TPM device to pass all TPM related tests in the HLK.
Objective	Ensure Intel® PTT passes all required platform HLK test for TPM device. ***Note:*** This test is not required for Intel® CSME compliance but may be required for Microsoft* logo certification. For any questions or support issues when running this test, refer 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

17.9 Intel® PTT Disable/Enable from BIOS

Test ID	**PTT_008**
Test Case Title	Intel® PTT Disable/Enable from BIOS
Mandatory/Optional	Optional
Description	BIOS may implement option to disable/enable Intel® PTT, or switch between Intel® PTT and a discrete TPM 1.2.
Objective	Ensure BIOS can enable and disable Intel® PTT successfully and that BIOS clears the TPM during disable.
Procedure	Can be run on Windows* 10 or Windows* 8.1. 1. Boot to Windows*, verify PTT_002 passing. 2. Reboot, enter BIOS and disable Intel® PTT through BIOS. 3. 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® PTT. 4. Reboot, enter BIOS and enable Intel® PTT through BIOS. 5. 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).

17.10 Intel® PTT and Power Flows

Test ID	**PTT_009**
Test Case Title	Power Flow Testing
Mandatory/Optional	Mandatory
Description	System with Intel® PTT enabled must pass all platform power flow testing. Intel® PTT must also be able to support all power flows when BitLocker is enabled and using Intel® PTT as a protector
Objective	Verify Intel® PTT does not interfere with system power operations
Procedure	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%: 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.

17.11 Dictionary Attack Lockout After Coin Battery Removal with EOM Commit

Test ID	**PTT_010**
Test Case Title	Dictionary Attack Lockout Mechanism with coin battery removal
Mandatory/Optional	Optional for systems that do not have RPMC enabled in the image. ***Note:*** This test is not relevant to platforms that do not include a coin battery.
Description	Intel® PTT keeps monotonic counters for Dictionary Attack (DA) under RTC power well. When RTC power is lost, Intel® PTT enters lockout period to avoid Dictionary Attack for 2 hours. This is only after the coin battery has been removed 10 times and after EOM. Before that, Intel® PTT would not enter the lockout period of 2 hours. ***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. ***Note:*** This test can be run only once on a specific part. After this test is run, all FPF bits related to the feature is blown. With such parts, test consistently enters dictionary attack scenario after every RTC clear operation.

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	1. System must be after the EOM procedure, as DA lockout would not occur during manufacturing mode 2. Set up a VSC with certificate (Instructions can be found in test PTT_006 steps 1 through 6) 3. Shutdown system, and perform RTC clear operation by removing all power and RTC battery from the board and close the RTC jumper. Repeat this procedure 11 times. 4. Return RTC battery and power, boot system to Windows* 10 5. Try to view the certificate in VSC by running: CertUtil.exe -scinfo -pin "12345678". 6. The command should fail due to Dictionary Attack lockout 7. Wait 2 hours for lockout to pass, and try again, it should be possible to access the certificate 8. Remove the certificate and VSC (Instruction can be found in test PTT_006 steps 8 and 9) ***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. **WARNING: This flow is irreversible, the part is permanently fused causing every RTC clear to cause a 2 hour TPM lockout.**
Test Pass/Fail Criteria	Intel® PTT would not allow access to user data (VSC) during lockout period post coin battery removal ***Note:*** In this test Field Programmable Fuses (FPF) is blown on every battery removal and there is no recovery for it. Select few processors to be used for this test and track them.

§ §

18 Platform Controller Hub (PCH) Soft Strap Configuration

The Intel® PCH Soft Straps 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 Soft Straps such as the Flexible I/O, SMLINK, GbE, and Intel® ME. The PCH Soft Straps are configure using the FIT tool. Refer to the SPI Programming Guide for the details description on all the available PCH Soft Straps.

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.

18.1 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® Compliancy kit for exact instructions on how to load and setup the Intel® PETS software.

Intel® Flash Image Tool (FIT.exe)

Intel® Flash Programming Tool: Available in DOS (fpt.exe), EFI (fpt.efi), Windows* 32-bit (fptw.exe), and Windows* 64-bit operating systems.

18.2 Test Environment

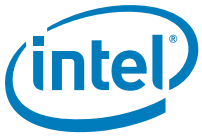
The System Under Test (SUT) is to be configured in manual configuration mode a with wired LAN dynamic IP address. The DHCP server connecting the SUT and Management Console (MC) must be configured to ensure that the wired LAN and wireless LAN addresses reside on separate subnets. The MC could be a laptop 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).

18.3 Test Coverage Summary

Test ID	Test Case Title	PETS/Manual	Network Factor
PSS_001	Intel Integrated Wired LAN Test	PETS	LAN+WLAN; WLAN only
PSS_002	Wake On Wireless LAN (WoWLAN) Test	PETS	LAN+WLAN; WLAN only
PSS_003	Flexible I/O Test	PETS	LAN+WLAN; WLAN only
PSS_004	BIOS Boot-Block Size Test	PETS	LAN+WLAN; WLAN only
PSS_007	Power State Deep Sx Test	PETS	LAN+WLAN; WLAN only
PSS_008	TPM on SPI Test	PETS	LAN+WLAN; WLAN only

18.4 Intel Integrated Wired LAN Test

Test ID	**PSS_001**
Test Case Title	Intel Integrated Wired LAN Test
Mandatory/Optional	Mandatory
Description	The PCH Soft Straps 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 Soft Straps must be configured correctly as well.
Objective	To verify correct configuration of PCH Soft Straps related to Intel Integrated Wired LAN.



<table>
<tr><th>Test ID</th><td>PSS_001</td></tr>
<tr><th>Procedure</th><td>
Boot to targeted OS. Verify correct configuration of the PCH Soft Straps below:

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 0x195 [0] LP A0
Offset 0x199 [0] LP A1 & B0
Offset 0x1B1 [0] H</td><td>1h</td></tr>
<tr><td>GbE PHY SMBus Address</td><td>Offset 0x1C8 [6:0] LP A0
Offset 0x1CC [6:0] LP A1 &B0
Offset 0x220 [6:0] H</td><td>64h</td></tr>
<tr><td>GbE MAC SMBus Address</td><td>Offset 0x1C0 [6:0] LP A0
Offset 0x1C4 [6:0] LP A1 & B0
Offset 0x218 [6:0] H</td><td>70h</td></tr>
<tr><td>Gbe MAC SMBus Address Enable</td><td>Offset 0x1C3 [0] LP A0
Offset 0x1C7 [0] LP A1 & B0
Offset 0x21B [0] H</td><td>1h</td></tr>
<tr><td>PHY Connection</td><td>Offset 0x20A [2:0] LP A0
Offset 0x20E [2:0] LP A1 & B0
Offset 0x28A [2:0] H</td><td>2h</td></tr>
<tr><td>Intel® Integrated wired LAN Enable</td><td>Offset 0xC18 [0] LP A0/A1/B0 & H</td><td>0h</td></tr>
</table>
a. What PCIe* port is the Intel® PHY attached?
<table>
<tr><th>Name</th><th>Location</th><th>Value</th></tr>
<tr><td>GBE PCIe* Port Select</td><td>Offset 0x1F3 [7:4] LP A0
Offset 0x1F4 [3:0]
Offset 0x1F4 [7:4]

Offset 0x1F7 [7:4] LP A1 & B0
Offset 0x1F8 [3:0]
Offset 0x1F8 [7:4]

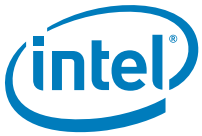
Offset 0x265 [7:4] H
Offset 0x26B [7:4]
Offset 0x26D [3:0]
Offset 0x26D [7:4]</td><td>Port 7 = 8h
Port 8 = 8h
Port 9 = 8h

Port 7 = 8h
Port 8 = 8h
Port 9 = 8h

Port 5 = 8h
Port 9 = 8h
Port 12 = 8h
Port 13 = 8h</td></tr>
</table>

</td></tr>
</table>

<table>
<tr><td>Test ID</td><td>PSS_001</td></tr>
<tr><td></td><td>
b. Is GPD11 from PCH routed to LAN_DISABLE_N on the Intel wired LAN PHY? (Requires Schematic Review)
— If YES:
<table>
<tr><th>Name</th><th>Location</th><th>Value</th></tr>
<tr><td>LAN PHY Power Control GPD11 Signal Configuration</td><td>Offset 0x118 [4] LP A0/A1/B0
Offset 0x110 [4] H</td><td>0h</td></tr>
</table>
— If NO:
<table>
<tr><th>Name</th><th>Location</th><th>Value</th></tr>
<tr><td>LAN PHY Power Control GPD11 Signal Configuration</td><td>Offset 0x118 [4] LP A0/A1/B0
Offset 0x110 [4] H</td><td>1h</td></tr>
</table>
</td></tr>
<tr><td></td><td>
2. If not using Intel Integrated Wired LAN solution:
<table>
<tr><th>Name</th><th>Location</th><th>Value</th></tr>
<tr><td>LAN PHY Power Control GPD11 Signal Configuration</td><td>Offset 0x118 [4] LP A0/A1/B0
Offset 0x110 [4] H</td><td>1h</td></tr>
<tr><td>Gbe MAC SMBus Address Enable</td><td>Offset 0x1C3 [6:0] LP A0
Offset 0x1C7 [6:0] LP A1 & B0
Offset 0x218 [6:0] H</td><td>0h</td></tr>
<tr><td>PHY Connection</td><td>Offset 0x20A [2:0] LP A0
Offset 0x20E [2:0] LP A1 & B0
Offset 0x28A [2:0] H</td><td>0h</td></tr>
<tr><td>Intel® Integrated wired LAN Enable</td><td>Offset 0xC18 [0] LP A0/A1/B0/H</td><td>1h</td></tr>
</table>
</td></tr>
<tr><td>Test Pass/Fail Criteria</td><td>Test passes if Soft Straps / register setting in this step matches to the configuration in the target system.</td></tr>
</table>



18.5 Wake On Wireless LAN (WoWLAN) Test

<table>
<tr><td>Test ID</td><td>PSS_002</td></tr>
<tr><td>Test Case Title</td><td>Wake On Wireless LAN (WoWLAN) Test</td></tr>
<tr><td>Mandatory/Optional</td><td>Mandatory</td></tr>
<tr><td>Description</td><td>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.</td></tr>
<tr><td>Objective</td><td>To verify correct configuration of the SLP_WLAN# SoftStrap setting.</td></tr>
<tr><td>Procedure</td><td>Boot to targeted OS. Verify correct configuration of the PCH Soft Straps below:

1. Is Wake On Wireless LAN (WoWLAN) required?
— If YES:

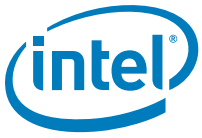
<table>
<tr><th>Name</th><th>Location</th><th>Value</th></tr>
<tr><td>SLP_WLAN# / GPD9 Signal Configuration</td><td>Offset 0x118 [3] LP A0/A1/B0
Offset 0x110 [3] H</td><td>0h</td></tr>
</table>

— If NO:

<table>
<tr><th>Name</th><th>Location</th><th>Value</th></tr>
<tr><td>SLP_WLAN# / GPD9 Signal Configuration</td><td>Offset 0x118 [3] LP A0/A1/B0
Offset 0x110 [3] H</td><td>1h</td></tr>
</table>
</td></tr>
<tr><td>Test Pass/Fail Criteria</td><td>Test passes if Soft Straps/register setting in this step matches to the configuration in the target system.</td></tr>
</table>

18.6 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 Soft Straps, 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 Soft Straps.



<table>
<tr><th>Test ID</th><td>PSS_003</td></tr>
<tr><th>Procedure</th><td>

Boot to targeted OS. Verify correct configuration of the PCH Soft Straps 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 0x161 [4:3] **LP A0/A1/B0 H**	3h

iii. Are the lanes reversed?

— If Reversed:

Name	Location	Value
PCIe* Controller 1 Lane Reversal	Offset 0x161 [2] **LP A0/A1/B0 H**	1h

— If NOT Reversed:

Name	Location	Value
PCIe* Controller 1 Lane Reversal	Offset 0x161 [2] **LP A0/A1/B0 H**	0h

b. 2x2 – two 2 lane PCIe* Port

Name	Location	Value
PCIe* Controller 1 (Port 1-4)	Offset 0x161 [4:3] **LP A0/A1/B0 H**	2h

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

Name	Location	Value
PCIe* Controller 1 (Port 1-4)	Offset 0x161 [4:3] **LP A0/A1/B0 H**	1h

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

Name	Location	Value
PCIe* Controller 1 (Port 1-4)	Offset 0x161 [4:3] **LP A0/A1/B0 H**	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 0x169 [4:3] **LP A0/A1/B0 H**	3h

</td></tr>
</table>

<table>
<tr><th>Test ID</th><th>PSS_003</th></tr>
<tr><td></td><td>
i. Are the lanes reversed?
— If reversed:
<table>
<tr><th>Name</th><th>Location</th><th>Value</th></tr>
<tr><td>PCIe* Controller 2 Lane Reversal</td><td>Offset 0x169 [2] LP A0/A1/B0 H</td><td>1h</td></tr>
</table>
— If NOT reversed:
<table>
<tr><th>Name</th><th>Location</th><th>Value</th></tr>
<tr><td>PCIe* Controller 2 Lane Reversal</td><td>Offset 0x169 [2] LP A0/A1/B0 H</td><td>0h</td></tr>
</table>
b. 2x2 – two 2 lanes PCIe* Port.
<table>
<tr><th>Name</th><th>Location</th><th>Value</th></tr>
<tr><td>PCIe* Controller 2 (Port 5-8)</td><td>Offset 0x169 [4:3] LP A0/A1/B0 H</td><td>2h</td></tr>
</table>
c. 1x2, 2x1 – One 2 lanes PCIe* Port, Two 1 lane PCIe* Port.
<table>
<tr><th>Name</th><th>Location</th><th>Value</th></tr>
<tr><td>PCIe* Controller 2 (Port 5-8)</td><td>Offset 0x169 [4:3] LP A0/A1/B0 H</td><td>1h</td></tr>
</table>
d. 4x1- One 1 lane PCIe* Port.
<table>
<tr><th>Name</th><th>Location</th><th>Value</th></tr>
<tr><td>PCIe* Controller 2 (Port 5-8)</td><td>Offset 0x169 [4:3] LP A0/A1/B0 H</td><td>0h</td></tr>
</table>
2. How do you have PCIe* Controller 3 (Port 9-12) configured?
a. 1x4 – One 4 lanes PCIe* Port.
<table>
<tr><th>Name</th><th>Location</th><th>Value</th></tr>
<tr><td>PCIe* Controller 3 (Port 9-12)</td><td>Offset 0x171 [4:3] LP A0/A1/B0 H</td><td>3h</td></tr>
</table>
i. Are the lanes reversed?
— If reversed:
<table>
<tr><th>Name</th><th>Location</th><th>Value</th></tr>
<tr><td>PCIe* Controller 3 Lane Reversal</td><td>Offset 0x171 [2] LP A0/A1/B0 H</td><td>1h</td></tr>
</table>
— If NOT reversed:
<table>
<tr><th>Name</th><th>Location</th><th>Value</th></tr>
<tr><td>PCIe* Controller 3 Lane Reversal</td><td>Offset 0x171 [2] LP A0/A1/B0 H</td><td>0h</td></tr>
</table>
b. 2x2 – two 2 lanes PCIe* Port.
<table>
<tr><th>Name</th><th>Location</th><th>Value</th></tr>
<tr><td>PCIe* Controller 3 (Port 9-12)</td><td>Offset 0x171 [4:3] LP A0/A1/B0 H</td><td>2h</td></tr>
</table>
c. 1x2, 2x1 – One 2 lanes PCIe* Port, Two 1 lane PCIe* Port.
<table>
<tr><th>Name</th><th>Location</th><th>Value</th></tr>
<tr><td>PCIe* Controller 3 (Port 9-12)</td><td>Offset 0x171 [4:3] LP A0/A1/B0 H</td><td>1h</td></tr>
</table>
</td></tr>
</table>

<table>
<tr><td>Test ID</td><td>PSS_003</td></tr>
<tr><td>Procedure</td><td>

Tiger Lake / Rocket Lake-H

a. 4x1- One 1 lane PCIe* Port.

Name	Location	Value
PCIe* Controller 3 (Port 9-12)	Offset 0x169 [4:3] **LP A0/A1/B0 H**	0h

1. How do you have PCIe* Controller 4 (Port 13-16) configured?

a. 1x4 – one 4 lane PCIe* Port

Name	Location	Value
PCIe* Controller 4 (Port 13-16)	Offset 0x179 [4:3] **H**	3h

i. Are the lanes reversed?

— If Reversed:

Name	Location	Value
PCIe* Controller 4 Lane Reversal	Offset 0x179 [2] **H**	1h

— If NOT Reversed:

Name	Location	Value
PCIe* Controller 4 Lane Reversal	Offset 0x179 [2] **H**	0h

b. 2x2 – two 2 lane PCIe* Port

Name	Location	Value
PCIe* Controller 4 (Port 13-16)	Offset 0x179 [4:3] **H**	3h

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

Name	Location	Value
PCIe* Controller 4 (Port 13-16)	Offset 0x179 [4:3] **H**	1h

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

Name	Location	Value
PCIe* Controller 4 (Port 13-16)	Offset 0x179 [4:3] **H**	1h

2. How do you have PCIe* Controller 5 (Port 17-20) configured?

a. 1x4 – One 4 lanes PCIe* Port.

Name	Location	Value
PCIe* Controller 5 (Port 17-20)	Offset 0x181 [4:3] **H**	3h

i. Are the lanes reversed?

— If Reversed:

Name	Location	Value
PCIe* Controller 5 Lane Reversal	Offset 0x181 [2] **H**	1h

— If NOT Reversed:

Name	Location	Value
PCIe* Controller 5 Lane Reversal	Offset 0x181 [2] **H**	0h

</td></tr>
</table>

<table>
<tr><td>Test ID:</td><td>PSS_003</td></tr>
<tr><td>Procedure</td><td>
Tiger Lake / Rocket Lake-H
a. 2x2 – two 2 lane PCIe* Port
<table>
<tr><th>Name</th><th>Location</th><th>Value</th></tr>
<tr><td>PCIe* Controller 5 (Port 17-20)</td><td>Offset 0x181 [4:3] H</td><td>3h</td></tr>
</table>
b. 1x2, 2x1- One 2 lane PCIe* Port, Two 1 lane PCIe* Port
<table>
<tr><th>Name</th><th>Location</th><th>Value</th></tr>
<tr><td>PCIe* Controller 4 (Port 13-16)</td><td>Offset 0x181 [4:3] H</td><td>1h</td></tr>
</table>
c. 4x1: Ports (1-4) (x1)
<table>
<tr><th>Name</th><th>Location</th><th>Value</th></tr>
<tr><td>PCIe* Controller 4 (Port 13-16)</td><td>Offset 0x181 [4:3] H</td><td>1h</td></tr>
</table>
1. How do you have PCIe* Controller 6 (Port 21-24) configured?
a. 1x4 – One 4 lanes PCIe* Port.
<table>
<tr><th>Name</th><th>Location</th><th>Value</th></tr>
<tr><td>PCIe* Controller 6 (Port 21-24)</td><td>Offset 0x189 [4:3] H</td><td>3h</td></tr>
</table>
i. Are the lanes reversed?
— If Reversed:
<table>
<tr><th>Name</th><th>Location</th><th>Value</th></tr>
<tr><td>PCIe* Controller 6 Lane Reversal</td><td>Offset 0x181 [2] H</td><td>1h</td></tr>
</table>
— If NOT Reversed:
<table>
<tr><th>Name</th><th>Location</th><th>Value</th></tr>
<tr><td>PCIe* Controller 6 Lane Reversal</td><td>Offset 0x181 [2] H</td><td>0h</td></tr>
</table>
b. 2x2 – two 2 lane PCIe* Port
<table>
<tr><th>Name</th><th>Location</th><th>Value</th></tr>
<tr><td>PCIe* Controller 6 (Port 21-24)</td><td>Offset 0x181 [4:3] H</td><td>3h</td></tr>
</table>
c. 1x2, 2x1- One 2 lane PCIe* Port, Two 1 lane PCIe* Port
<table>
<tr><th>Name</th><th>Location</th><th>Value</th></tr>
<tr><td>PCIe* Controller 6 (Port 21-24)</td><td>Offset 0x181 [4:3] H</td><td>1h</td></tr>
</table>
d. 4x1: Ports (1-4) (x1)
<table>
<tr><th>Name</th><th>Location</th><th>Value</th></tr>
<tr><td>PCIe* Controller 6 (Port 21-24)</td><td>Offset 0x181 [4:3] H</td><td>1h</td></tr>
</table>
</td></tr>
</table>

<table>
<tr><th>Test ID</th><th>PSS_003</th></tr>
<tr><td></td><td>

1. Does this platform use PCH PCIe* port 1 as USB3 Port 1 (LP) or PCH Port 1 as USB3 Port 7 (H)?

— If yes, PCH PCIe* Port 1 or 7 configured as USB3

<table>
<tr><th>Name</th><th>Location</th><th>Value</th></tr>
<tr><td>USB3 / PCIe* Combo Port 0</td><td>Offset 0x1F0 [5:2] LP A0
Offset 0x1F4 [5:2] LP A1 & B0
Offset 0x263 [7:4] H</td><td>1h</td></tr>
</table>

— If no is, PCH PCIe* Port 1 or 7 configured as PCIe

<table>
<tr><th>Name</th><th>Location</th><th>Value</th></tr>
<tr><td>USB3 / PCIe* Combo Port 0</td><td>Offset 0x1F0 [5:2] LP A0
Offset 0x1F4 [5:2] LP A1 & B0
Offset 0x263 [7:4] H</td><td>5h</td></tr>
</table>

— If no is, PCH PCIe* 1 or 7 Statically disabled

<table>
<tr><th>Name</th><th>Location</th><th>Value</th></tr>
<tr><td>USB3 / PCIe* Combo Port 0</td><td>Offset 0x1F0 [5:2] LP A0
Offset 0x1F4 [5:2] LP A1 & B0
Offset 0x263 [7:4] H</td><td>0h</td></tr>
</table>

2. Does this platform use PCH PCIe* Port 2 as USB3 Port 2 (LP) or PCH Port 2 USB3 Port 8 (H)?

— If yes, PCH PCIe* Port 2 or 8 configured as USB3

<table>
<tr><th>Name</th><th>Location</th><th>Value</th></tr>
<tr><td>USB3 / PCIe* Combo Port 1</td><td>Offset 0x1F1 [3:0] LP A0
Offset 0x1F5 [3:0] LP A1 & B0
Offset 0x264 [3:0] H</td><td>1h</td></tr>
</table>

— If no is, PCH PCIe* Port 2 or 8 configured as PCIe

<table>
<tr><th>Name</th><th>Location</th><th>Value</th></tr>
<tr><td>USB3 / PCIe* Combo Port 1</td><td>Offset 0x1F1 [3:0] LP A0
Offset 0x1F5 [3:0] LP A1 & B0
Offset 0x264 [3:0] H</td><td>5h</td></tr>
</table>

— If no is, PCH PCIe* 2 or 8 Statically disabled

<table>
<tr><th>Name</th><th>Location</th><th>Value</th></tr>
<tr><td>USB3 / PCIe* Combo Port 1</td><td>Offset 0x1F1 [3:0] LP A0
Offset 0x1F5 [3:0] LP A1 & B0
Offset 0x264 [3:0] H</td><td>0h</td></tr>
</table>

</td></tr>
</table>

<table>
<tr><th>Test ID</th><th>PSS_003</th></tr>
<tr><td></td><td>

3. Does this platform use PCH PCIe* Port 3 as USB3 Port 3 (LP) or PCH Port 3 USB3 Port 9 (H)?

— If yes, PCH PCIe* Port 3 or 9 configured as USB3

<table>
<tr><th>Name</th><th>Location</th><th>Value</th></tr>
<tr><td>USB3 / PCIe* Combo Port 2</td><td>Offset 0x1F1 [7:4] LP A0
Offset 0x1F5 [7:4] LP A1 & B0
Offset 0x265 [7:4] H</td><td>1h</td></tr>
</table>

— If no is, PCH PCIe* Port 3 or 9 configured as PCIe

<table>
<tr><th>Name</th><th>Location</th><th>Value</th></tr>
<tr><td>USB3 / PCIe* Combo Port 2</td><td>Offset 0x1F1 [7:4] LP A0
Offset 0x1F5 [7:4] LP A1 & B0
Offset 0x265 [7:4] H</td><td>5h</td></tr>
</table>

— If no is, PCH PCIe* 3 or 9 Statically disabled

<table>
<tr><th>Name</th><th>Location</th><th>Value</th></tr>
<tr><td>USB3 / PCIe* Combo Port 2</td><td>Offset 0x1F1 [7:4] LP A0
Offset 0x1F5 [7:4] LP A1 & B0
Offset 0x265 [7:4] H</td><td>0h</td></tr>
</table>

3. Does this platform use PCH PCIe* Port 4 as USB3 Port 4 (LP) or PCH Port 4 USB3 Port 10 (H)?

— If yes, PCH PCIe* Port 4 configured as USB3

<table>
<tr><th>Name</th><th>Location</th><th>Value</th></tr>
<tr><td>USB3 / PCIe* Combo Port 3</td><td>Offset 0x1F2 [3:0] LP A0
Offset 0x1F6 [3:0] LP A1 & B0
Offset 0x265 [3:0] H</td><td>1h</td></tr>
</table>

— If no is, PCH PCIe* Port 4 configured as PCIe

<table>
<tr><th>Name</th><th>Location</th><th>Value</th></tr>
<tr><td>USB3 / PCIe* Combo Port 3</td><td>Offset 0x1F2 [3:0] LP A0
Offset 0x1F6 [3:0] LP A1 & B0
Offset 0x265 [3:0] H</td><td>5h</td></tr>
</table>

— If no is, PCH PCIe* 4 Statically disabled

<table>
<tr><th>Name</th><th>Location</th><th>Value</th></tr>
<tr><td>USB3 / PCIe* Combo Port 3</td><td>Offset 0x1F2 [3:0] LP A0
Offset 0x1F6 [3:0] LP A1 & B0
Offset 0x265 [3:0] H</td><td>0h</td></tr>
</table>

</td></tr>
</table>

<table>
<tr><th>Test ID</th><th>PSS_003</th></tr>
<tr><td></td><td>

Tiger Lake-LP

1. How is SATA / PCIe* Combo Port 0 Strap configured on the platform?

i. Statically assigned to SATA Port 0.

Name	Location	Value
SATA / PCIe* Combo Port 0 Strap	Offset 0x1F5 [7:4] **LP A0** Offset 0x1F9 [7:4] **LP A1 & B0**	7h

ii. Statically assigned to PCIe* Port 11.

Name	Location	Value
SATA / PCIe* Combo Port 0 Strap	Offset 0x1F5 [7:4] **LP A0** Offset 0x1F9 [7:4] **LP A1 & B0**	5h

iii. Assigned PCIe* based on the native mode of GPP_E0 pin.

Name	Location	Value
SATA / PCIe* Combo Port 0 Strap	Offset 0x1F5 [7:4] **LP A0** Offset 0x1F9 [7:4] **LP A1 & B0**	Ch

iv. Assigned SATA based on the native mode of GPP_E0 pin.

Name	Location	Value
SATA / PCIe* Combo Port 0 Strap	Offset 0x1F5 [7:4] **LP A0** Offset 0x1F9 [7:4] **LP A1 & B0**	Dh

v. PCIe* Port 11 Statically disabled.

Name	Location	Value
SATA / PCIe* Combo Port 0 Strap	Offset 0x1F5 [7:4] **LP A0** Offset 0x1F9 [7:4] **LP A1 & B0**	0h

2. How is SATA / PCIe* Combo Port 1 Strap configured on the platform?

i. Statically assigned to SATA Port 1.

Name	Location	Value
SATA / PCIe* Combo Port 1 Strap	Offset 0x1F6 [3:0] **LP A0** Offset 0x1FA [3:0] **LP A1 & B0**	7h

ii. Statically assigned to PCIe* Port 12.

Name	Location	Value
SATA / PCIe* Combo Port 1 Strap	Offset 0x1F6 [3:0] **LP A0** Offset 0x1FA [3:0] **LP A1 & B0**	5h

iii. Assigned PCIe* based on the native mode of GPP_E1 pin.

Name	Location	Value
SATA / PCIe* Combo Port 1 Strap	Offset 0x1F6 [3:0] **LP A0** Offset 0x1FA [3:0] **LP A1 & B0**	Ch

iv. Assigned SATA based on the native mode of GPP_E1 pin.

Name	Location	Value
SATA / PCIe* Combo Port 1 Strap	Offset 0x1F6 [3:0] **LP A0** Offset 0x1FA [3:0] **LP A1 & B0**	Dh

v. PCI Port 12 Statically disabled.

Name	Location	Value
SATA / PCIe* Combo Port 1 Strap	Offset 0x1F6 [3:0] **LP A0** Offset 0x1FA [3:0] **LP A1 & B0**	0h

</td></tr>
</table>

<table>
<tr><th>Test ID</th><th>PSS_003</th></tr>
<tr><td></td><td>

Tiger Lake / Rocket Lake-H

1. How is SATA / PCIe* Combo Port 0 Strap configured on the platform?

i. Statically assigned to SATA Port 0a.

Name	Location	Value
SATA / PCIe* Combo Port 0 Strap	Offset 0x26C [7:4] **H**	7h

ii. Statically assigned to PCIe* Port 11.

Name	Location	Value
SATA / PCIe* Combo Port 0 Strap	Offset 0x26C [7:4] **H**	5h

iii. Assigned PCIe* based on the native mode of GPP_E0 pin.

Name	Location	Value
SATA / PCIe* Combo Port 0 Strap	Offset 0x26C [7:4] **H**	Ch

iv. Assigned SATA based on the native mode of GPP_E0 pin.

Name	Location	Value
SATA / PCIe* Combo Port 0 Strap	Offset 0x26C [7:4] **H**	Dh

v. PCIe* Port 11 Statically disabled.

Name	Location	Value
SATA / PCIe* Combo Port 0 Strap	Offset 0x26C [7:4] **H**	0h

2. How is SATA / PCIe* Combo Port 1 Strap configured on the platform?

i. Statically assigned to SATA Port 1a.

Name	Location	Value
SATA / PCIe* Combo Port 1 Strap	Offset 0x26D [3:0] **H**	7h

ii. Statically assigned to PCIe* Port 12.

Name	Location	Value
SATA / PCIe* Combo Port 1 Strap	Offset 0x26D [3:0] **H**	5h

iii. Assigned PCIe* based on the native mode of GPP_E1 pin.

Name	Location	Value
SATA / PCIe* Combo Port 1 Strap	Offset 0x26D [3:0] **H**	Ch

iv. Assigned SATA based on the native mode of GPP_E1 pin.

Name	Location	Value
SATA / PCIe* Combo Port 1 Strap	Offset 0x26D [3:0] **H**	Dh

v. PCI Port 12 Statically disabled.

Name	Location	Value
SATA / PCIe* Combo Port 1 Strap	Offset 0x26D [3:0] **H**	0h

</td></tr>
</table>

<table>
<tr><th>Test ID</th><th>PSS_003</th></tr>
<tr><td></td><td>

Tiger Lake / Rocket Lake-H

1. How is SATA / PCIe* Combo Port 2 Strap configured on the platform?

i. Statically assigned to SATA Port 0b.

Name	Location	Value
SATA / PCIe* Combo Port 2 Strap	Offset 0x26D [7:4] **H**	7h

ii. Statically assigned to PCIe* Port 13.

Name	Location	Value
SATA / PCIe* Combo Port 2 Strap	Offset 0x26D [7:4] **H**	5h

iii. Assigned PCIe* based on the native mode of GPP_E0 pin.

Name	Location	Value
SATA / PCIe* Combo Port 2 Strap	Offset 0x26D [7:4] **H**	Ch

iv. Assigned SATA based on the native mode of GPP_E0 pin.

Name	Location	Value
SATA / PCIe* Combo Port 2 Strap	Offset 0x26D [7:4] **H**	Dh

v. PCIe* Port 13 Statically disabled.

Name	Location	Value
SATA / PCIe* Combo Port 0 Strap	Offset 0x26C [7:4] **H**	0h

2. How is SATA / PCIe* Combo Port 3 Strap configured on the platform?

i. Statically assigned to SATA Port 1b.

Name	Location	Value
SATA / PCIe* Combo Port 3 Strap	Offset 0x26E [3:0] **H**	7h

ii. Statically assigned to PCIe* Port 14.

Name	Location	Value
SATA / PCIe* Combo Port 3 Strap	Offset 0x26E [3:0] **H**	5h

iii. Assigned PCIe* based on the native mode of GPP_E1 pin.

Name	Location	Value
SATA / PCIe* Combo Port 3 Strap	Offset 0x26E [3:0] **H**	Ch

iv. Assigned SATA based on the native mode of GPP_E1 pin.

Name	Location	Value
SATA / PCIe* Combo Port 3 Strap	Offset 0x26E [3:0] **H**	Dh

v. PCI Port 14 Statically disabled.

Name	Location	Value
SATA / PCIe* Combo Port 3 Strap	Offset 0x26E [3:0] **H**	0h

</td></tr>
</table>

<table>
<tr><th>Test ID</th><th>PSS_003</th></tr>
<tr><td></td><td>

Tiger Lake / Rocket Lake-H

1. How is SATA / PCIe* Combo Port 4 Strap configured on the platform?

i. Statically assigned to SATA Port 2.

Name	Location	Value
SATA / PCIe* Combo Port 4 Strap	Offset 0x26E [7:4] **H**	7h

ii. Statically assigned to PCIe* Port 15.

Name	Location	Value
SATA / PCIe* Combo Port 4 Strap	Offset 0x26E [7:4] **H**	5h

iii. Assigned PCIe* based on the native mode of GPP_E0 pin.

Name	Location	Value
SATA / PCIe* Combo Port 4 Strap	Offset 0x26E [7:4] **H**	Ch

iv. Assigned SATA based on the native mode of GPP_E0 pin.

Name	Location	Value
SATA / PCIe* Combo Port 4 Strap	Offset 0x26E [7:4] **H**	Dh

v. PCIe* Port 15 Statically disabled.

Name	Location	Value
SATA / PCIe* Combo Port 4 Strap	Offset 0x26E [7:4] **H**	0h

2. How is SATA / PCIe* Combo Port 5 Strap configured on the platform?

i. Statically assigned to SATA Port 3.

Name	Location	Value
SATA / PCIe* Combo Port 5 Strap	Offset 0x26F [3:0] **H**	7h

ii. Statically assigned to PCIe* Port 16.

Name	Location	Value
SATA / PCIe* Combo Port 5 Strap	Offset 0x26F [3:0] **H**	5h

iii. Assigned PCIe* based on the native mode of GPP_E1 pin.

Name	Location	Value
SATA / PCIe* Combo Port 5 Strap	Offset 0x26F [3:0] **H**	Ch

iv. Assigned SATA based on the native mode of GPP_E1 pin.

Name	Location	Value
SATA / PCIe* Combo Port 5 Strap	Offset 0x26F [3:0] **H**	Dh

v. PCI Port 16 Statically disabled.

Name	Location	Value
SATA / PCIe* Combo Port 5 Strap	Offset 0x26E [3:0] **H**	0h

</td></tr>
</table>

<table>
<tr><th>Test ID</th><th>PSS_003</th></tr>
<tr><td></td><td>

Tiger Lake / Rocket Lake-H

1. How is SATA / PCIe* Combo Port 6 Strap configured on the platform?

i. Statically assigned to SATA Port 4.

Name	Location	Value
SATA / PCIe* Combo Port 6 Strap	Offset 0x26F [7:4] **H**	7h

ii. Statically assigned to PCIe* Port 17.

Name	Location	Value
SATA / PCIe* Combo Port 6 Strap	Offset 0x26F [7:4] **H**	5h

iii. Assigned PCIe* based on the native mode of GPP_E0 pin.

Name	Location	Value
SATA / PCIe* Combo Port 6 Strap	Offset 0x26F [7:4] **H**	Ch

iv. Assigned SATA based on the native mode of GPP_E0 pin.

Name	Location	Value
SATA / PCIe* Combo Port 6 Strap	Offset 0x26F [7:4] **H**	Dh

v. PCIe* Port 17 Statically disabled.

Name	Location	Value
SATA / PCIe* Combo Port 6 Strap	Offset 0x26F [7:4] **H**	0h

2. How is SATA / PCIe* Combo Port 7 Strap configured on the platform?

i. Statically assigned to SATA Port 5.

Name	Location	Value
SATA / PCIe* Combo Port 7 Strap	Offset 0x270 [3:0] **H**	7h

ii. Statically assigned to PCIe* Port 18.

Name	Location	Value
SATA / PCIe* Combo Port 7 Strap	Offset 0x270 [3:0] **H**	5h

iii. Assigned PCIe* based on the native mode of GPP_E1 pin.

Name	Location	Value
SATA / PCIe* Combo Port 7 Strap	Offset 0x270 [3:0] **H**	Ch

iv. Assigned SATA based on the native mode of GPP_E1 pin.

Name	Location	Value
SATA / PCIe* Combo Port 7 Strap	Offset 0x270 [3:0] **H**	Dh

v. PCI Port 18 Statically disabled.

Name	Location	Value
SATA / PCIe* Combo Port 7 Strap	Offset 0x270 [3:0] **H**	0h

</td></tr>
</table>

<table>
<tr><th>Test ID</th><th>PSS_003</th></tr>
<tr><td></td><td>

Tiger Lake / Rocket Lake-H

1. How is SATA / PCIe* Combo Port 8 Strap configured on the platform?

i. Statically assigned to SATA Port 6.

Name	Location	Value
SATA / PCIe* Combo Port 8 Strap	Offset 0x270 [7:4] **H**	7h

ii. Statically assigned to PCIe* Port 19.

Name	Location	Value
SATA / PCIe* Combo Port 8 Strap	Offset 0x270 [7:4] **H**	5h

iii. Assigned PCIe* based on the native mode of GPP_E0 pin.

Name	Location	Value
SATA / PCIe* Combo Port 8 Strap	Offset 0x270 [7:4] **H**	Ch

iv. Assigned SATA based on the native mode of GPP_E0 pin.

Name	Location	Value
SATA / PCIe* Combo Port 8 Strap	Offset 0x270 [7:4] **H**	Dh

v. PCIe* Port 19 Statically disabled.

Name	Location	Value
SATA / PCIe* Combo Port 8 Strap	Offset 0x270 [7:4] **H**	0h

2. How is SATA / PCIe* Combo Port 9 Strap configured on the platform?

i. Statically assigned to SATA Port 7.

Name	Location	Value
SATA / PCIe* Combo Port 9 Strap	Offset 0x271 [3:0] **H**	7h

ii. Statically assigned to PCIe* Port 20.

Name	Location	Value
SATA / PCIe* Combo Port 9 Strap	Offset 0x271 [3:0] **H**	5h

iii. Assigned PCIe* based on the native mode of GPP_E1 pin.

Name	Location	Value
SATA / PCIe* Combo Port 9 Strap	Offset 0x271 [3:0] **H**	Ch

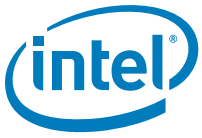
iv. Assigned SATA based on the native mode of GPP_E1 pin.

Name	Location	Value
SATA / PCIe* Combo Port 9 Strap	Offset 0x271 [3:0] **H**	Dh

v. PCI Port 20 Statically disabled.

Name	Location	Value
SATA / PCIe* Combo Port 9 Strap	Offset 0x271 [3:0] **H**	0h

</td></tr>
</table>

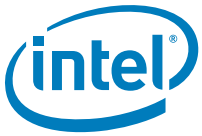


18.7 BIOS Boot-Block Size Test

Test ID	**PSS_004**
Test Case Title	BIOS Boot-Block size Test
Mandatory/Optional	Mandatory
Description	BIOS Boot-Block size deals with a BIOS recovery mechanism. If this is not set correctly, then BIOS boot-block recovery mechanism would not work.
Objective	To verify BIOS boot-block size of correctly setup.

<table>
<tr><td>Test ID</td><td>PSS_004</td></tr>
<tr><td>Procedure</td><td>
Boot to targeted OS. Verify correct configuration of the PCH Soft Straps below:

1. What size is your SPI flash BIOS boot block?
a. If 64KB
<table>
<tr><th>Name</th><th>Location</th><th>Value</th></tr>
<tr><td>Top Swap Block size</td><td>Offset 0x14C [6:4] LP A0/A1/B0
Offset 0x144 [6:4] H</td><td>0h</td></tr>
</table>
a. 128KB
<table>
<tr><th>Name</th><th>Location</th><th>Value</th></tr>
<tr><td>Top Swap Block size</td><td>Offset 0x14C [6:4] LP A0/A1/B0
Offset 0x144 [6:4] H</td><td>1h</td></tr>
</table>
b. 256KB
<table>
<tr><th>Name</th><th>Location</th><th>Value</th></tr>
<tr><td>Top Swap Block size</td><td>Offset 0x14C [6:4] LP A0/A1/B0
Offset 0x144 [6:4] H</td><td>2h</td></tr>
</table>
c. 512KB
<table>
<tr><th>Name</th><th>Location</th><th>Value</th></tr>
<tr><td>Top Swap Block size</td><td>Offset 0x14C [6:4] LP A0/A1/B0
Offset 0x144 [6:4] H</td><td>3h</td></tr>
</table>
d. 1MB
<table>
<tr><th>Name</th><th>Location</th><th>Value</th></tr>
<tr><td>Top Swap Block size</td><td>Offset 0x14C [6:4] LP A0/A1/B0
Offset 0x144 [6:4] H</td><td>4h</td></tr>
</table>
e. 2MB
<table>
<tr><th>Name</th><th>Location</th><th>Value</th></tr>
<tr><td>Top Swap Block size</td><td>Offset 0x14C [6:4] LP A0/A1/B0
Offset 0x144 [6:4] H</td><td>5h</td></tr>
</table>
f. 4MB
<table>
<tr><th>Name</th><th>Location</th><th>Value</th></tr>
<tr><td>Top Swap Block size</td><td>Offset 0x14C [6:4] LP A0/A1/B0
Offset 0x144 [6:4] H</td><td>6h</td></tr>
</table>
g. 8MB
<table>
<tr><th>Name</th><th>Location</th><th>Value</th></tr>
<tr><td>Top Swap Block size</td><td>Offset 0x14C [6:4] LP A0/A1/B0
Offset 0x144 [6:4] H</td><td>7h</td></tr>
</table>
</td></tr>
<tr><td>Test Pass/Fail Criteria</td><td>Test passes if Soft Straps/register setting in this step matches to the configuration in the target system.</td></tr>
</table>



18.8 Power State Deep Sx Test

<table>
<tr><td>Test ID</td><td>PSS_007</td></tr>
<tr><td>Test Case Title</td><td>Power State Deep Sx Test</td></tr>
<tr><td>Mandatory/Optional</td><td>Mandatory</td></tr>
<tr><td>Description</td><td>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.</td></tr>
<tr><td>Objective</td><td>To verify correct configuration of Power State Deep Sx.</td></tr>
<tr><td>Procedure</td><td>Boot to targeted OS. Verify correct configuration of the PCH Soft Straps 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 0x17C [20] LP A0/A1/B0
Offset 0x194 [20] H
Offset 0xC14 [20] All</td><td>1h
1h
1h</td></tr>
</table>

— If NO,

<table>
<tr><th>Name</th><th>Location</th><th>Value</th></tr>
<tr><td>Deep Sx Enable</td><td>Offset 0x17C [20] LP A0/A1/B0
Offset 0x194 [20] H
Offset 0xC14 [20] All</td><td>0h
0h
0h</td></tr>
</table>

Note: This is not the same as Intel® CSME power state M3.</td></tr>
<tr><td>Test Pass/Fail Criteria</td><td>Test passes if Soft Straps/register setting in this step matches to the configuration in the target system.</td></tr>
</table>

18.9 Trusted Platform Module (TPM) on SPI Test

<table>
<tr><td>Test ID</td><td>PSS_008</td></tr>
<tr><td>Test Case Title</td><td>Trusted Platform Module on SPI Test</td></tr>
<tr><td>Mandatory/Optional</td><td>Mandatory</td></tr>
<tr><td>Description</td><td>TPM can be configured through PCH Soft Straps to operate over LPC or SPI, but no more than 1 TPM is allowed in the target system.</td></tr>
<tr><td>Objective</td><td>To verify TPM on SPI is correctly configured.</td></tr>
<tr><td>Procedure</td><td>
Boot to targeted OS. Verify correct configuration of the PCH Soft Straps 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 0x1EC [0] LP A0
Offset 0x1F0 [0] LP A1/B0
Offset 0x25C [0] H</td><td>1h</td></tr>
</table>
— 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 0x1EC [0] LP A0
Offset 0x1F0 [0] LP A1/B0
Offset 0x25C [0] H</td><td>0h</td></tr>
</table>
Boot to targeted OS. Verify correct configuration of the PCH Soft Straps below:

1. What Clock Frequency is being used for TPM on SPI?
a. If 48 MHz
<table>
<tr><th>Name</th><th>Location</th><th>Value</th></tr>
<tr><td>SPI TPM Clock Frequency</td><td>Offset 0x151 [2:0] LP A0/A1/B0
Offset 0x149 [2:0] H</td><td>2h</td></tr>
</table>
b. 30 MHz
<table>
<tr><th>Name</th><th>Location</th><th>Value</th></tr>
<tr><td>SPI TPM Clock Frequency</td><td>Offset 0x151 [2:0] LP A0/A1/B0
Offset 0x149 [2:0] H</td><td>4h</td></tr>
</table>
c. 14 MHz
<table>
<tr><th>Name</th><th>Location</th><th>Value</th></tr>
<tr><td>SPI TPM Clock Frequency</td><td>Offset 0x151 [2:0] LP A0/A1/B0
Offset 0x149 [2:0] H</td><td>6h</td></tr>
</table>
</td></tr>
<tr><td>Test Pass/Fail Criteria</td><td>Test passes if Soft Straps/register setting in this step matches to the configuration in the target system.</td></tr>
</table>

§ §

19 Intel® Virtualization Technology (Intel® VT)

Throughout this chapter, 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.

19.1 Introduction

19.1.1 Purpose and Scope

The purpose of this chapter 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 is not a technology overview and does not supplant the existing Intel® VT collateral (refer Section 1.6: "Reference Documents"). The readers are expected to be familiar with Intel® VT-x and Intel® VT-d and to use this document as a validation supplement to develop their own Intel® VT validation plan.

19.1.2 Platforms Applicable

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

Table 19-1. Applicable Platforms

Platform Name
8th Generation Intel® Core™ and Intel® Core™ M Processors Platforms
Tiger Lake Platforms

19.1.3 Terminology

Table 19-2. Terminology (Sheet 1 of 2)

Term	Description
DMA	Direct Memory Access

Table 19-2. Terminology (Sheet 2 of 2)

Term	Description
GPA	Guest Physical Address
HPA	Host Physical Address
HVM	Hardware Virtual Machine (Virtual Machine using Intel® VT)
MMIO	Memory Mapped I/O Address Space
OS	Operating System
Intel® TXT	Intel® Trusted Execution Technology
VM	Virtual Machine
VMM	Virtual Machine Monitor

19.1.4 Testing Prerequisites

Table 19-3. Virtualization Testing Prerequisites

Prerequisite Checklist	Location
Client VT Info Tool	# 551893
Fedora Live USB Creator (Optional)	Open Source
OpenSUSE	Open Source

19.2 Test Plan and Details

Table 19-4. 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
Xen*/Linux* Environment Tests				
VT_TC03A	Xen* Hypervisor Boots (Xen* Environment)	Manual	Optional	Pass
VT_TC03B	Intel® VT-x and VT-d Enabled (Xen* Environment)	Manual	Optional	Pass

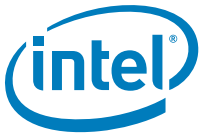


Table 19-4. Test Overview

ID	Test Case Description	Tool/ Manual	Mandatory/ Optional	Result
VT_TC03C	Intel® VT-d Functionality—Virtual Machine (VM) Boots (Xen* Environment)	Manual	Optional	Pass
VT_TC03D	Intel® VT-d Functionality—Pass Through with No VT-d Error (Xen* Environment)	Manual	Optional	Pass
VT_TC04	Intel® VT-d Functionality—IOMMU Exercise (Xen* Environment)	Manual	Optional	Pass

19.3 Tests in EFI Shell

19.3.0.1 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 Setting.

Note: Disabling Intel® TXT is just for test purposes:

Tools for Testing:

- **Client VT Info Tool:** Get the latest version of the tool from PC Design Center VT Technology page or using document #551893.

19.3.0.2 Verifying if 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	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 CDI/IBL #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.) Refer example outputs below in section Section 19.3.0.2.1: "Sample Output for Client VT Info Tool Results—Passing All Tests", Section 19.3.0.2.2: "Sample Output for Client VT Info Tool Results—Failing Some Tests", and Section 19.3.0.2.3: "Sample Output for Client VT Info Tool Results—Obtaining Test Result Details". ***Note:*** For additional information on VT Status, use **vtinfo -h** to display other command line options.
Test Pass/Fail Criteria	Test passes when: 1. Tool returns **VT Test Status: PASS** 2. **No Errors** are reported in test results

19.3.0.2.1 Sample Output for Client VT Info Tool Results—Passing All Tests

This example was generated using the -t option with Client VT Info Tool:

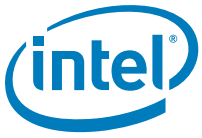
```
**********************************************
VtInfo vXX.XX.XX
Built: XXX X 2014 XX:XX:XX
Intel Corporation
Copyright (c) 2014
**********************************************
--------------------
VT Test Status: PASS
--------------------
--------------------
Pass  | 52
Fail  | 00
Warn  | 00
NA    | 05
Total | 57
--------------------
```

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

19.3.0.2.2 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 Adress(0xAFFFFFFF) is not marked as reserved in system memory map.

62) VTd Support for Large Pages (2MB and 1GB) on DEFAULT and GFX VTd Unit.
-- Remapping Engine 0xFED91000 Capability Register BIT56 must be set.

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

19.3.0.2.3 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    0x0000000000000FF07
 [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 Adress(0xAFFFFFFF) is not marked as reserved in system memory map.

62) VTd Support for Large Pages (2MB and 1GB) on DEFAULT and GFX VTd Unit.
-- Remapping Engine 0xFED91000 Capability Register BIT56 must be set.

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

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

19.3.1.1 Test Environment

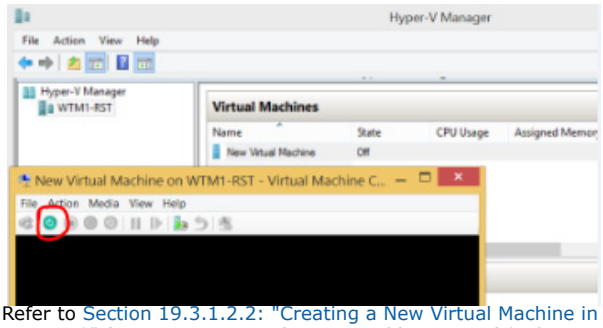
A system under test is needed which has an Intel® VT-x and Intel® VT-d capable Processor and stable BIOS with support for VT-x and VT-d technologies. Prior to tests **enable Virtualization (or VT-x)** and **Intel® VT-d** in BIOS and make sure **TXT is Disabled.**

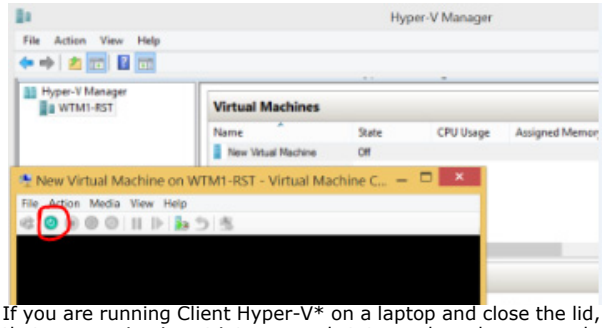
Note: Disabling TXT is just for test purposes.

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	1. Enable Intel® Virtualization Technology (VT-x) in BIOS. 2. Boot to Windows* 10 and open Client Hyper-V* Manager. ***Note:*** Refer to Section 19.3.1.2: "Microsoft* Client Hyper-V* and Virtual Machine Enabling and Installation Instructions" for instructions on how to enable Client Hyper-V*.
Test Pass/Fail Criteria	Test passes when: Microsoft* Client Hyper-V* Manager Boots.

Test ID	**VT_TC02B**
Test Case Title	Verify Virtual Machine Boots in Microsoft* Client Hyper-V* Manager
Mandatory/Optional	Mandatory
Description	Microsoft* Client Hyper-V* uses Intel® VT to launch a virtual guest OS in Windows* 10 host OS.
Objective	Verify Intel® VT-x implementation at platform level
Procedure	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.  ***Note:*** Refer to Section 19.3.1.2.2: "Creating a New Virtual Machine in Client Hyper-V*" for instructions on how to enable Microsoft* Client Hyper-V*.
Test Pass/Fail Criteria	Test passes when: Virtual Machine Guest boots within Client Hyper-V* (when Intel® VT is enabled in BIOS).

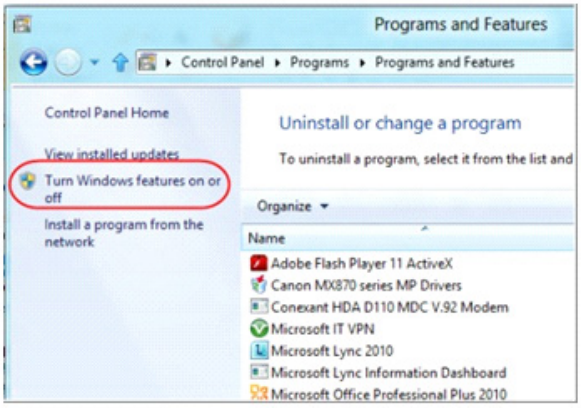
Test ID	**VT_TC02C**
Test Case Title	Verify Virtual Machine Correctly Resumes during Sleep and Hibernate Cycles on Host OS.
Mandatory/Optional	Mandatory
Description	While performing Sleep and Hibernate cycles on the Host Machine, the Virtual Machine should correctly resume and remain stable.
Objective	Verify Intel® VT-x implementation at platform level.
Procedure	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, user can click on the start button.  ***Note:*** If you are running Client Hyper-V* on a laptop and close the lid, the VMs that are running is put into a saved state, and can be resumed when the machine wakes, **as long as lid close action is set to sleep or hibernate**. 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: • Virtual machine is alive and working *after system Sleep cycle.* • Virtual machine is alive and working *after Hibernate cycle.*

19.3.1.2 Microsoft* Client Hyper-V* and Virtual Machine Enabling and Installation Instructions

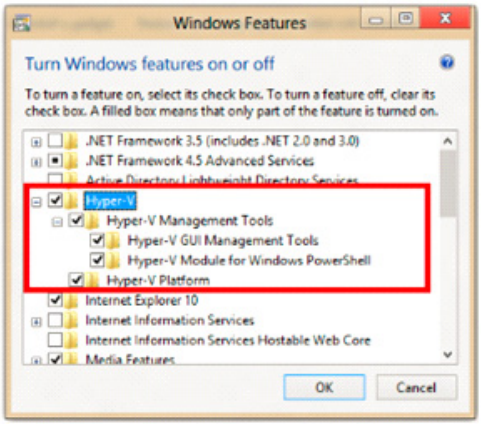
19.3.1.2.1 Enabling Microsoft* Client Hyper-V*

1. In the Windows* 10 Control Panel, tap or click Programs, and then tap or click **Programs and Features**.

2. 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*

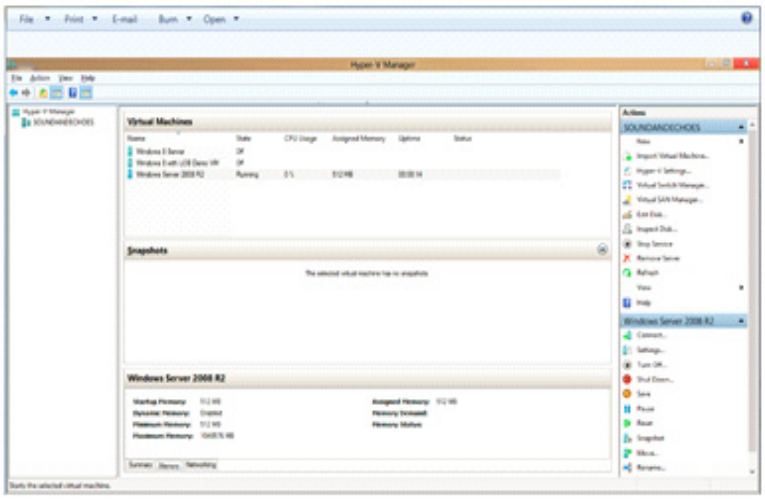
Note: Enabling Client Hyper-V* installs Hyper-V* Manager. User use Hyper-V* Manager to create and manage your virtual machines.

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

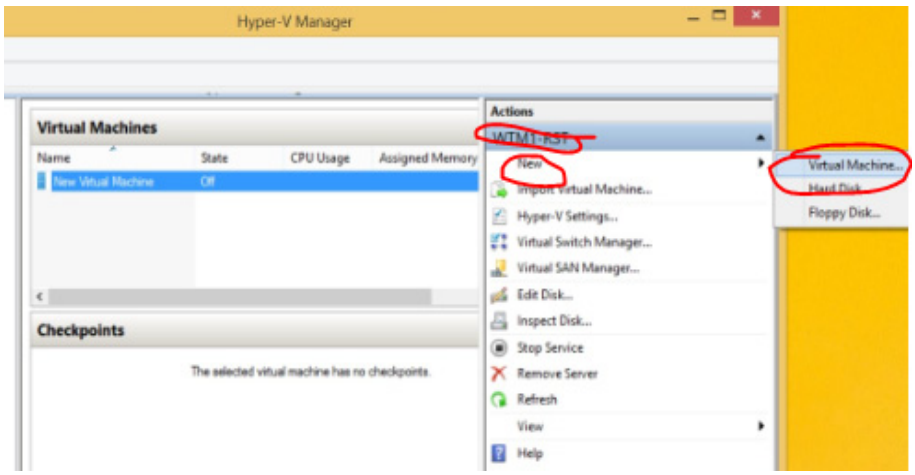
19.3.1.2.2 Creating a New Virtual Machine in Client Hyper-V*

Skip this page if user already have a Virtual Machine in Client Hyper-V* Manager.

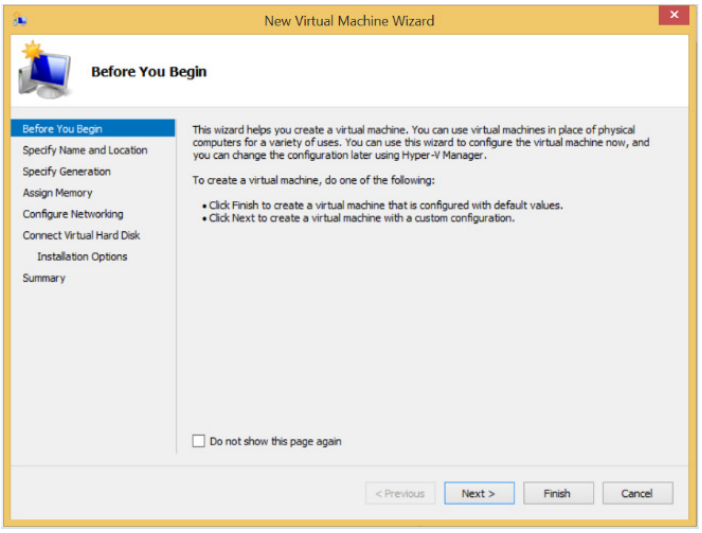
1. Open Hyper-V* Manager from Windows* Start screen (In Windows* 10 you may need to go to Start screen -> Click arrow at bottom left -> Hyper-V Management tools -> Hyper-V Manager.)



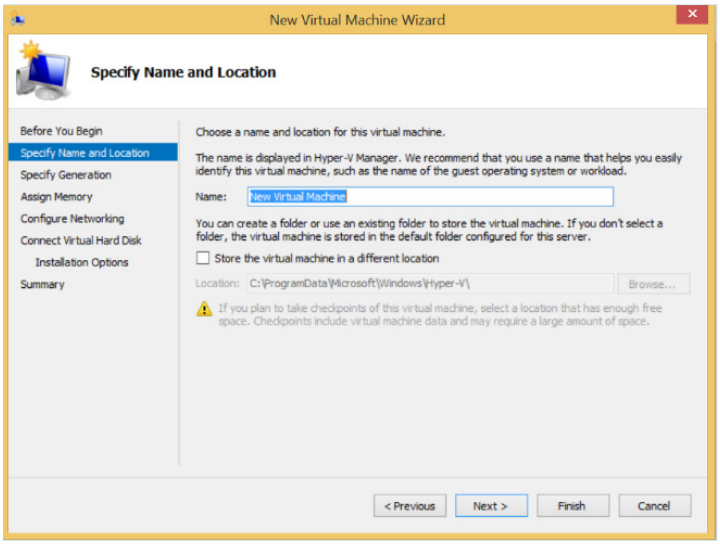
2. From the navigation pane of Hyper-V* Manager, select the computer name.
3. From the **Action** pane on the right side, click **New**, and then click **Virtual Machine**.The New Virtual



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

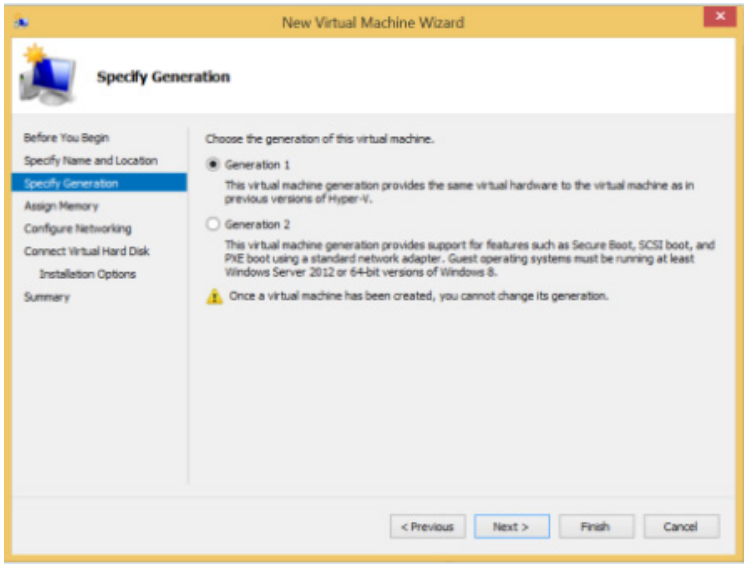


5. On the **Specify Name and Location** page, type any name.

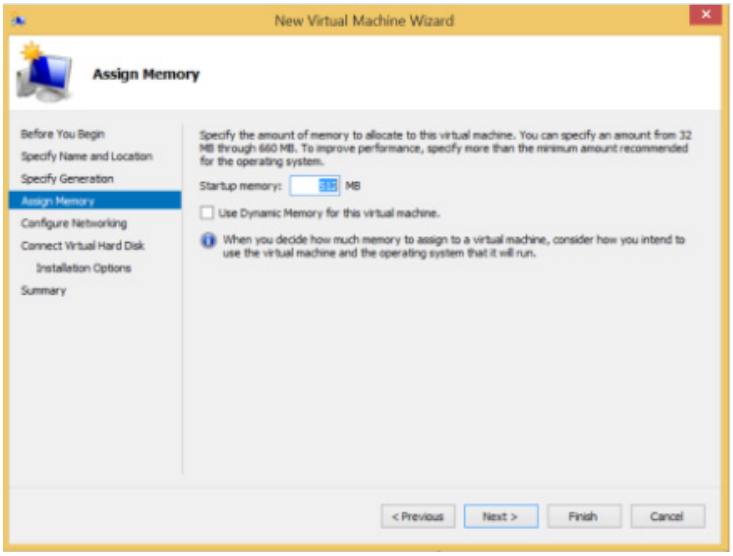


6. On the **Specify Generation** page, leave the default, Generation 1.

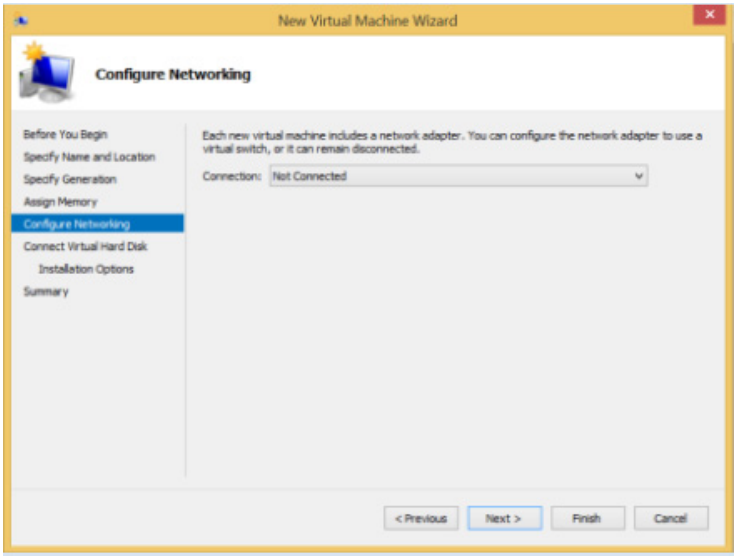
Note: Earlier versions of Client Hyper-V* may not have this step.



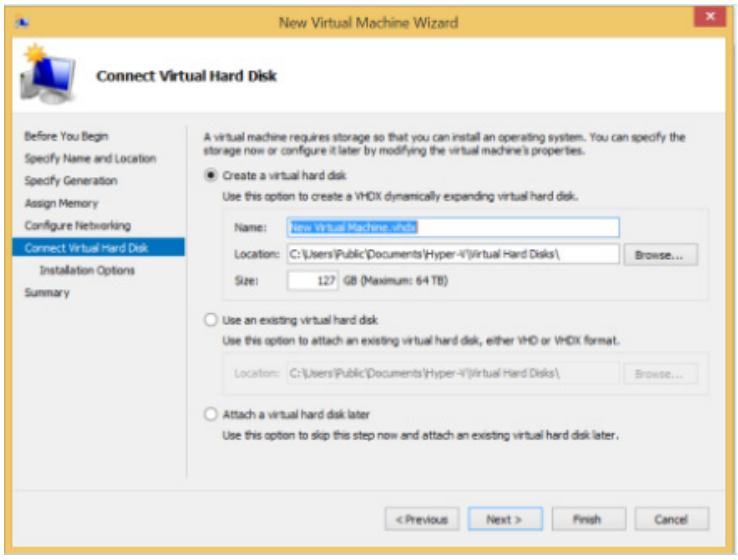
7. On the **Assign Memory** page, specify enough memory to start the guest operating system.

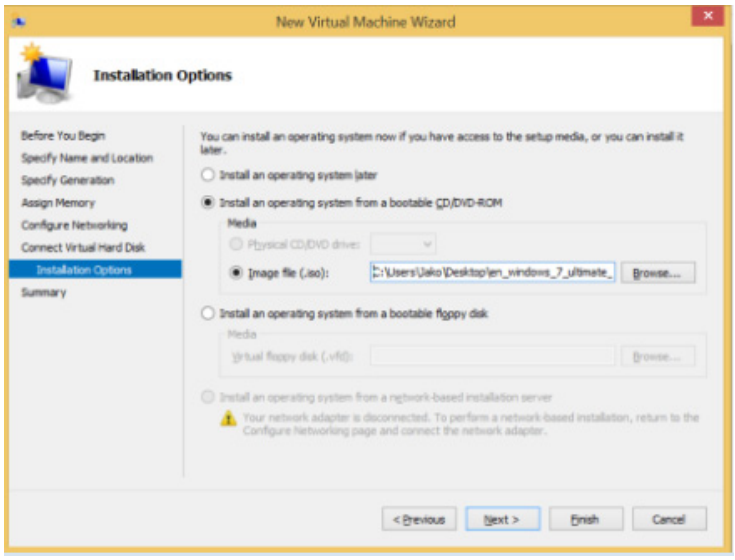


8. On the **Configure Networking** page, leave the default settings.



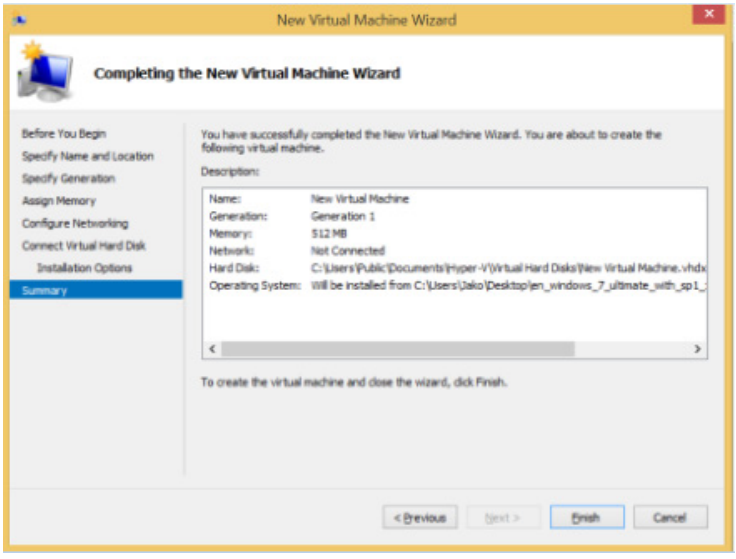
On the **Connect Virtual Hard Disk** and **Installation Options** pages, choose the option that is appropriate for how you plan to install the guest operating system:
If user installs the guest operating system from a DVD or an image file (an.ISO file), choose **Create a virtual hard disk**. Click **Next**, and then click the option that describes the type of media user use. For example, to use an .iso file, click **Install an operating system from a boot CD/DVD** and then specify the path to the .iso file**. (This is recommended)**



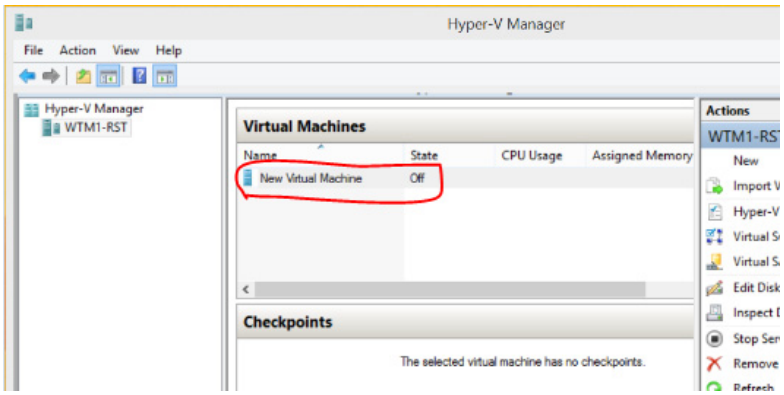


g. If the guest operating system is already installed in a virtual hard disk, choose **Use an existing virtual hard disk** and click Next. (Refer figure at top of page). Then, choose **Install an operating system later.**

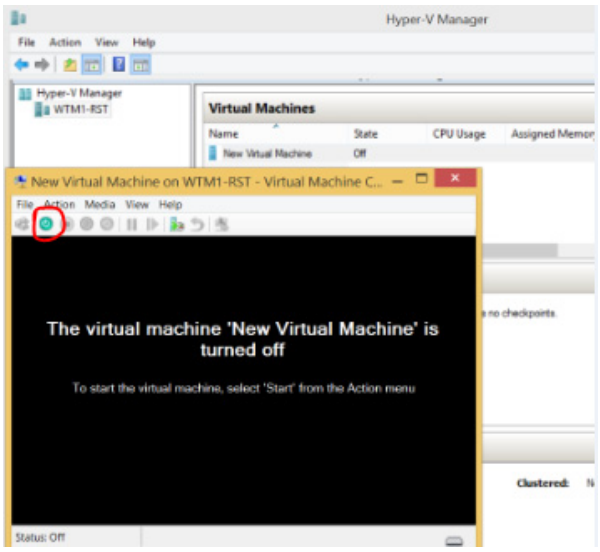
9. On the **Summary page,** verify your selections and then click **Finish**.



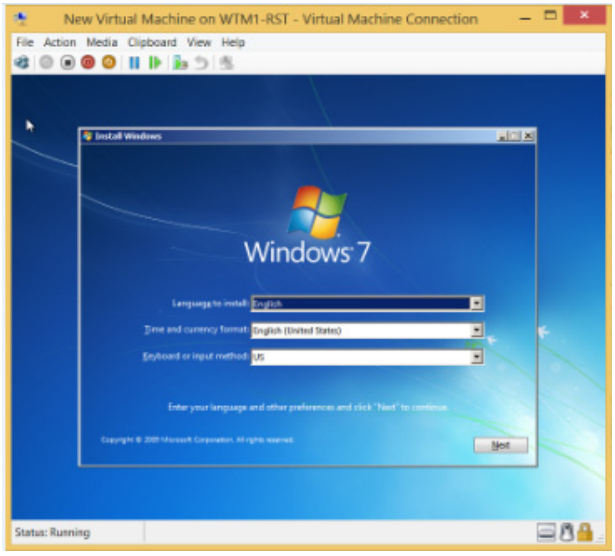
10. Double Click to **Virtual Machine** to Open it.



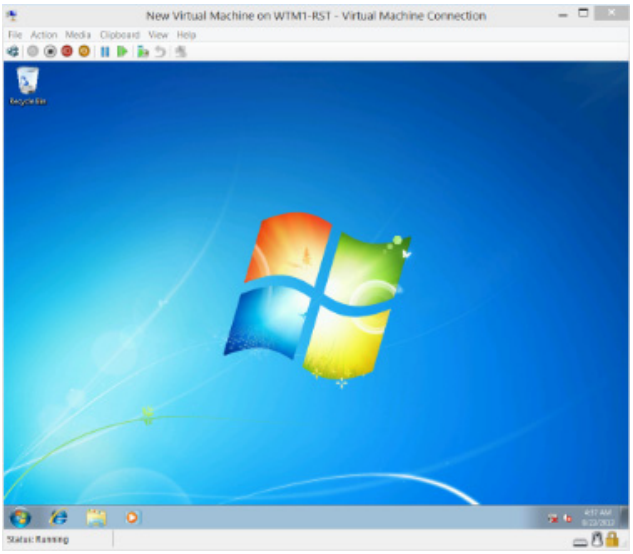
11. Click on the green **Start** button to run Virtual Machine .

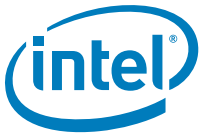


12. **Follow** normal OS Installation Instructions, this depends on OS you have chosen.



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





19.3.2 Intel® VT Tests in Xen*/Linux* Environment

Test Environment:

A system under test is needed which has an Intel® VT-x and Intel® VT-d capable Processor, a stable BIOS with support for VT-x and VT-d technologies. Prior to tests **enable Virtualization (or VT-x)** and **VT-d** in BIOS and make sure **TXT is Disabled.**

Tools for Testing:

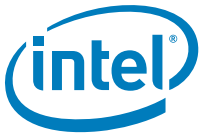
- Open source openSUSE* 42.1 or Open source Fedora* 17
- Xen* open source VMM

19.3.2.1 Verifying System Under Test (SUT) Boots Xen* Mode/VMM

Test ID	**VT_TC03A**
Test Case Title	Xen* Hypervisor Boots (Xen* Environment)
Mandatory/Optional	Optional
Description	Ensures that Test cases VT_TC13, VT_TC14 and VT_TC15 can be executed.
Objective	Verify platform can boot to Xen* Hypervisor/VMM
Preparation	1. Install Xen* OS (for example openSUSE* 42.1 or Fedora* 17 or equivalent). 2. Enable Intel® Virtualization Technology (VT-x) and VT-d in BIOS. 3. Build/Install Xen* VMM. **Installation steps are explained in Section 19.4.**
Procedure	1. Boot to Xen* drive 2. Choose Xen* Hypervisor option 3. When system boots, login as root. 4. To login as root: Change user to root and use password: linux123 5. Enter "xl info" into terminal. Result should give Xen version number and no error message.
Test Pass/Fail Criteria	Test passes when the following occurs: System successfully boots to Xen* Hypervisor with no error messages.

19.3.2.2 Verifying Intel® VT-x and VT-d Enabled (Xen* Mode)

Test ID	**VT_TC03B**
Test Case Title	Intel® VT-x and VT-d Enabled (Xen* Environment)
Mandatory/Optional	Optional
Description	Ensures that VT-d is enabled and supported. This test is in Xen* Hypervisor.
Objective	Verify Intel® VT Functionality is enabled on the SUT.
Preparation	Install Xen* OS (for example openSUSE* 42.1 of Fedora* 17) Download and build/Install Xen*. **Installation steps are explained in** Section 19.4**.**
Procedure	1. Boot to Xen* Mode 2. Open terminal 3. Enter **xl dmesg | grep -i Virt** *This should yield:* *(XEN) I/O virtualisation enabled* 4. Enter **xl dmesg | grep -i VT** *This should yield:* *(XEN) Intel VT-d iommu 0 supported page sizes: 4kB, 2MB, 1GB.* *(XEN) Intel VT-d iommu 1 supported page sizes: 4kB, 2MB, 1GB.* *(XEN) Intel VT-d Snoop Control not enabled.* *(XEN) Intel VT-d Dom0 DMA Passthrough not enabled.* *(XEN) Intel VT-d Queued Invalidation enabled.* *(XEN) Intel VT-d Interrupt Remapping enabled.* *(XEN) Intel VT-d Shared EPT tables enabled.* ***Note:*** "dmesg" is Xen* command, run from a terminal. Depending on the version of Xen kernel, "xl" might be replaced with "xl -f" or "xm"
Test Pass/Fail Criteria	Test passes when all the following occur: 1. "xl dmesg | grep -i virtual" results in: (XEN) I/O virtualisation 2. "xl dmesg | grep -i VT" results in: (XEN) Intel VT-d iommu 0 supported page sizes: 4kB, 2MB, 1GB. (XEN) Intel VT-d iommu 1 supported page sizes: 4kB, 2MB, 1GB. (XEN) Intel VT-d Snoop Control not enabled. (XEN) Intel VT-d Dom0 DMA Passthrough not enabled. (XEN) Intel VT-d Queued Invalidation enabled. (XEN) Intel VT-d Interrupt Remapping enabled. (XEN) Intel VT-d Shared EPT tables enabled. ***Note:*** There may be additional results too; if above results are shown on test system, this test is passing.

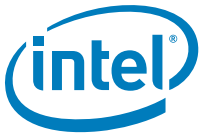


19.3.2.3 Verifying Intel® VT-d Functionality VM Boots (Xen* Mode)

Test ID	**VT_TC03C**
Test Case Title	Intel® VT-d Functionality - Virtual Machine (VM) Boots (Xen* Environment)
Mandatory/Optional	Optional
Description	Verifies VT_TC14 can be executed.
Objective	Verify Intel® VT implementation at platform level.
Preparation	Enable Intel® Virtualization Technology (VT-x) and VT-d in BIOS 1. Install Xen* OS (for example openSUSE* 42.1 or Fedora* 17). 2. Install/Build Xen* VMM onto Xen* OS. **Instructions are explained in** Section 19.4**.**
Procedure	1. Boot to Xen* Hypervisor Mode. 2. Open Virtual Machine Manager. 3. Create a Virtual Machine. Instructions are explained in Section 19.4.2.3: "Creating a Virtual Machine on openSUSE* 42.1". 4. Launch Hardware Virtual Machine (HVM) for example Windows* XP, Windows* 7 or other OS as a Virtual Machine. 5. Verify that no VT faults are reported using **dmesg | grep -i VT**
Test Pass/Fail Criteria	Test passes when all the following occur: 1. A Virtual Machine (VM) is open and working. 2. Verify that no VT faults are reported in serial log messages and "dmesg" log. ***Note:*** "dmesg" is Xen* command, run from a terminal. User may need to use xm dmesg (prior to Xen* 4.1.0) or xl dmesg (if user is using Xen* 4.1.0 and later.)

19.3.2.4 Verifying Intel® VT-d Functionality Pass Through (Xen* Mode)

Test ID	**VT_TC03D**
Test Case Title	Intel® VT-d Functionality—Pass through with No VT-d Error (Xen* Environment)
Mandatory/Optional	Optional
Description	Verifies Intel® VT-d Functionality by Assigning Devices to Guest OS and checking for errors by output log messages. • Validates Intel® VT BIOS implementation by using Intel® VT hardware as exposed by BIOS through ACPI table. • Creates Address translation tables as per Intel® VT Specification • Exercises Intel® VT-d functionality by assigning devices to guest OS – outputs log messages • Outputs debug messages on serial port. (Intel® VT messages have a keyword "Intel VT" or "Intel VT-d" on the lines)
Objective	Verify Intel® VT implementation at platform level.
Preparation	Required to test VT_TC13.
Procedure	If you already have an open Virtual Machine, you can skip to step 3. 1. Boot to Xen* Hypervisor (with Intel® VT and Intel® VT-d enabled in BIOS setup options). 2. Launch Hardware Virtual Machine (HVM) for example Windows* XP or Windows* 7. 3. Directly assign one or more I/O devices to guest HVM, for example Ethernet Controller, Integrated Network device, Audio, Firewire, USB controller and so forth. Refer Section 19.4.2.4: "Testing Intel® VT Using Xen* VMM in OpenSUSE* 42.1" for instructions. 4. Verify that no VT faults are reported in serial log messages. 5. Verify that no VT faults are reported using **dmesg | grep -i VT**
Test Pass/Fail Criteria	Test passes when all the following occur: 1. Directly assign one or more I/O devices to guest HVM, for example Integrated Network device, Audio, Firewire, USB controller and so forth. 2. Verify that directly assigned I/O device is visible only in HVM 3. Verify that no VT faults are reported in serial log messages and "dmesg" log. ***Note:*** "dmesg" is Xen* command, run from a terminal. You may need to use xm dmesg (prior to Xen* 4.1.0) or xl dmesg (if you are using Xen* 4.1.0 and later.)



19.3.2.5 Verifying Intel® VT-d Functionality Through IOMMU Exercise

Test ID	**VT_TC04**
Test Case Title	Intel® VT-d Functionality - IOMMU Exercise (Xen* Environment)
Mandatory/Optional	Optional
Description	Runs in Xen* Environment. Enable Intel® Virtualization Technology (VT-x) and VT-d in BIOS Dynamically creates Intel® VT-d address translation tables by running concurrent workloads on integrated I/O devices like graphics, network device, HD audio, Firewire or USB device. Since Xen* IOMMU does page invalidation on each I/O transaction, it stresses the Intel® VT-d at system level in a unique way.
Objective	Verify Intel® VT-d functionality through the IOMMU driver.
Preparation	Install openSUSE* 42.1. The latest stable Xen* includes Intel® VT-d IOMMU driver Xen* installation steps are explained in Section 19.4.
Procedure	1. Boot openSUSE* Xen* with Intel® Virtualization Technology (VT-x) and VT-d enabled in BIOS. 2. Run concurrent workloads like TTCP or disk copy, **while** playing audio to stress these I/O devices, and/or playing video clips from Internet (for example YouTube* and so forth) at same time. 3. Check for error messages. IOMMU driver forwards faults in the DMESG log or the RS232 port.
Test Pass/Fail Criteria	Test passes when IOMMU messages appear in DMESG log or on RS232 port, and no VT-d faults are reported in DMESG log or serial port log. ***Note:*** "dmesg" is Xen* command, run from a terminal. You may need to use xm dmesg (prior to Xen* 4.1.0) or xl dmesg (if you are using Xen* 4.1.0 and later.)

19.4 User Guide—Installing and Using Linux* (openSUSE* 42.1, Fedora* 17) and Xen* VMM for Intel® VT Testing

19.4.1 Platform Setup Requirements

The system/platform on which the Linux*/Xen* is to be installed is System Under Test (SUT). The following are the SUT setup requirements:

System needs to be stable and booting to DOS*/Windows* OS

- Add Intel® PRO100 Network PCI card. This is needed as Linux*/Xen* installation requires a working network connection. If the system is based on Intel® 5 Series Express Chipsets or previous generation chipsets, the onboard wired network is sufficient.
- Add DVD ROM drive for booting Linux* from CD or DVD.
- BIOS setup options:
  - — **Optional: Disable** "Intel Virtualization Technology" and "Intel® VT-d" in BIOS setup options (prior to OS installation, then **Enable after installation** is complete).
  - — Set SATA disk drive mode to **AHCI mode.**

19.4.2 Using openSUSE* 42.1 (64-Bit)

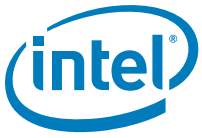
For a video on openSUSE* 11.3 Xen Hypervisor Installation, refer the Videos Section on Broadwell Platform PCDC VT page.

Note: openSUSE* 11.3 installation is very similar to openSUSE* 42.1 installation.

19.4.2.1 Standard Linux* Installation for openSUSE* 42.1

View instructions below or Refer openSUSE* Installation Instructions. Be sure to also follow **step 8** below.

1. Download openSUSE* 42.1 (64-bit) and burn it on a DVD. Examples and references used in this procedure are based on installing openSUSE* 42.1 on an Intel CRB.
2. After booting the openSUSE* DVD, choose Installation.
3. Select Language and Keyboard Layout. Click **Next.**
4. Choose New Installation. Click **Next**.
5. Choose region and Time Zone. Click **Next**.
6. Select preferred desktop environment. Click **Next**.
7. Choose Partition based or LVM based. Click **Next**.
8. Enter Username and Password. Click Next. **(Un-check the option to automatically sign in, during installation).**



9. Review settings, modify any if necessary, and Click **Install**.
10. After Installation the configuration ill automatically be created.

19.4.2.2 Xen* Hypervisor Installation on openSUSE* 42.1

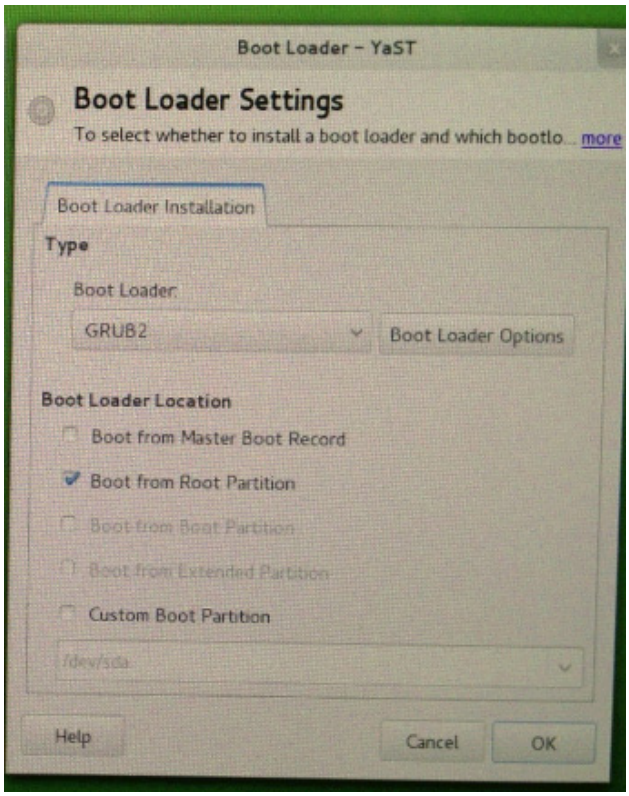
1. Choose the default option on boot options menu, and log in using root as the username.
2. Ensure your openSUSE* 42.1 installation disk is loaded.
3. In the Applications Menu go to System > Install Hypervisor and Tools (Or search for YaST2).
4. Choose Xen* and Accept.
5. When asked to configure a default network bridge, choose Yes.
6. Reboot Machine.
7. To verify if Xen* Hypervisor is installed:
   a. Boot up machine.
   b. Choose Xen* – openSUSE* 42.1.
   c. Log in as root user.
   d. Open terminal and type **uname –r**
   e. "xen" should be seen along with the kernel* version number.

19.4.2.2.1 Tip: When Xen Hypervisor Option Does Not Show Up

After Xen Installation, if Xen Hypervisor doesn't show up in the boot loader menu, you may need to change its boot loader configuration file after Xen Installation:

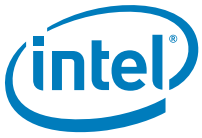
1. Reboot your system after installation.
2. Use Desktop boot option (the first option).
3. Find the Yast Boot Loader Settings: **Computer > Yast > System > Boot Loader** or **Administrator Settings > Boot Loader**
4. Enter Boot loader type: **GRUB2.** Choose **Boot from Root Partition.** Click **OK**.
5. After a reboot, user would see the hypervisor in the boot loader menu.

Figure 19-1. Boot Loader Settings



19.4.2.3 Creating a Virtual Machine on openSUSE* 42.1

1. Choose Xen* Hypervisor boot option and log in using root as username.
2. In Applications Menu go to **System** -> **Virtualization** -> **Create Virtual Machines**.
3. Click **Forward**.
4. Insert Guest OS Installation disk.
5. Choose I need to install an operating system. Click **Forward**.
6. Choose Guest OS you would like to use and click **Forward**.
7. Review Summary of Virtual Machine.
   a. You may want to change the Name of Virtual Machine. Click **Apply**.
   b. Also in Hardware section, ensure that you have at least 1024MB of Initial Memory and Maximum Memory. Click **Apply**.
   c. In Disks option, add CD-ROM by clicking on CD-ROM and Move CD-ROM to the top option using the arrows. Click **Apply**.
   d. In Network Adapters delete any default adapters. Click **Apply**.
   e. Click **OK**.



f. Follow the on screen instructions for installing the Guest OS in the Virtual Machine.

19.4.2.4 Testing Intel® VT Using Xen* VMM in OpenSUSE* 42.1

The Intel® VT can be tested by assigning PCIe* I/O device(s) to the guest OS. When Intel® VT-d is used to directly assign an I/O device to a guest, the guest OS has direct access to I/O device hardware and guest VM owns the physical driver for that I/O device.

The test is considered to be passing when all of the following occur:

1. An I/O device can be successfully assigned to guest VM (Section 19.4.2.4.1).
2. Xen* VMM does not report any VT faults. Xen* VMM reports no VT faults in "dmesg" log. User need to search for VT faults by executing the following and search for VT messages:

```
dmesg | grep -i fault
--OR--
xm dmesg | grep -i fault (if using Xen earlier than 4.1)
--OR--
xl dmesg | grep -i fault (if using Xen 4.1.0 or later)
```

3. Guest VM detects the presence of new hardware. (In a Windows* OS, this can be determined through the VM device manager.)
4. If the physical driver for the newly assigned I/O device is present in the guest OS, check that the device is functional.

19.4.2.4.1 Assigning an I/O Device Using PCISTUB Method

1. First obtain the Bus, Device, Function (BFD) ID of the device using:

```
lspci --OR-- lspci | grep -i Ethernet
Example result:
...
00:19.0 Ethernet controller: Intel Corporation 82566DM Giga-
bit Net...
...
BDF = "00:19.0"
```

2. Enter the following, in order to unbind and attach the device:
   a. echo -n 0000:00:19.0 > /sys/bus/pci/devices/0000:00:19.0/driver/unbind
   b. echo 0000:00:19.0 > /sys/bus/pci/devices/0000:00:19.0/driver/unbind
   c. echo 0000:00:19.0 > /sys/bus/pci/drivers/pciback/new_slot
   d. echo 0000:00:19.0 > /sys/bus/pci/drivers/pciback/bind
   e. **ls -l /sys/bus/pci/devices/0000:00:19.0/driver**
      this verifies the binding
   f. xl pci-attach *Guest* 0:0:19.0
      where *Guest* is the name of virtual machine

Note: In Xen* 4.1 or earlier, use "xm" instead of "xl"

To find version of Xen* you are using, use **xl info** or **xm info** command.

19.4.2.5 Special Instructions to Obtain Serial Log on openSUSE* 42.1

User need to modify the serial device parameters in the grub file, in order to receive kernel information on a serial port.

1. Open /boot/grub/menu.lst
2. Add the changes highlighted in red below:

Original

```
title Desktop -- openSUSE 42.1 - 2.6.37.1-1.2.Original
        root (hd0,0)
        kernel /vmlinuz-2.6.37.1-1.2-desktop root=/dev/system/root
        resume=/dev/system/swap splash=silent showopts vga=0x31a
        initrd /initrd-2.6.37.1-1.2-desktop
```

New

```
title Desktop -- openSUSE 42.1 - 2.6.37.1-1.2
        root (hd0,0)
        kernel /vmlinuz-2.6.37.1-1.2-desktop com6=115200,8n1 con-
        sole=com6L root=/dev/system/root resume=/dev/system/swap
        splash=silent console=tty0 console=ttyS0,115200 showopts
        vga=0x31a
        initrd /initrd-2.6.37.1-1.2-desktop
```

Note: In this example, com6/com6L is used, however COMM ports may vary.

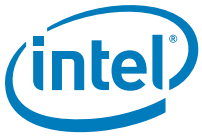
19.4.3 Using Fedora*17 (64-Bit)

For a video on Installing Fedora* and Xen*, refer VT Training Series Videos on PC Design Center.

19.4.3.1 Standard Linux* Installation for Fedora* 17 (64-Bit)

Prior to OS Installation, refer Section 19.4.1 “Platform Setup Requirements”. Download Fedora* 17 (64-bit) and burn it on a DVD. Examples and references used in this procedure are based on installing Fedora* 17 on this platform (using Intel CRB). After booting the Fedora* DVD, follow the installation instructions below, (also, Refer to Fedora* installation guide on web).

1. Select Language and Keyboard Layout. Click **Next** after each page is complete.
2. Choose “Basic Storage Devices” in Installation Options. Click **Next**.
3. Choose system name, desired time zone, and password. Click **Next** after each.
4. Choose what type of Installation to use (It is recommended to Use All Space.”), also check Use LVM. Click **Next** and Write Changes to Disk.
5. When prompted, choose “Software Development” and “Customize Now” option (at bottom of page) to install additional packages. Click **Next**. The recommended packages to install are:
   a. Applications: Office and Productivity
   b. Development: Development Tools
   c. Development: Development Libraries
   d. Base System: System Tools



e. Base System: Virtualization Client

f. Base System: Virtualization Hypervisor

g. Servers: Network Server

6. Click **Next** and continue the installation.
7. The system prompts for reboot after installing Fedora* so that the changes can be made.
8. After the reboot, follow the instructions to create an account when prompted. Click Forward.
9. Alter login settings from user account:
   a. Log on with the personal account you created.
   b. Move to root permissions (using Linux* command "su").
   c. When prompted for a password, make sure to use the root password.
   d. Edit files for root login:
      i. Change to root directory using **cd /**
      ii. Edit "gdm-password" file in: /etc/pam.d/gdm-password
      iii. Comment out the following line:
      Auth required pam_succeed_if.so user !=root quiet
      iv. Save the file and log out of system
10. Log back in as root user.
11. **Optional:** If you need to enable Ethernet access on boot:
    a. Edit the following file: "/etc/sysconfig/network-scripts/ifcfg-eth0"
    b. change **ONBOOT=no** to **ONBOOT=yes**
    c. Reboot system.
    d. Log in as root after system reboot.

19.4.3.1.1 Installing Additional Packages for use with Fedora* 17

1. Open a web browser or terminal window and check again that you have a good internet connection (using "ifconfig", look for an assigned IP address in terminal)
2. Optional: If your environment uses a proxy to connect to the internet, open a terminal window and type the command (as an example)

   export http_proxy=http://proxy.yourcompany.com:port#
3. Install the following packages using yum:
   a. yum -y update yum
   b. yum -y install bridge-utils
   c. yum -y install mkinitrd
   d. yum -y install iasl
   e. yum -y install dev86
   f. yum -y install unifdef
   g. yum -y install mercurial
   h. yum -y install xfig
   i. yum -y install tigervnc-server

j. yum -y install git

k. yum -y install mesa-demos (this is for glxgears)

Note: If you receive the following error: **"Error: Cannot retrieve metalink for repository: Fedora. Verify its path and try again"** Do the following to fix it:

1. CD to /etc/yum.repos.d
2. open fedora.repo in a text editor
3. Mask each instance of "#mirrorlist=" and unmask each instance of "baseurl="
4. Save file and do the same (steps 2 and 3) for fedora-updates.repo

Note: If you have difficulty installing from CD-ROM, try using an ISO file. Be sure to first copy the ISO file over to the local system (Using right click > Copy To > Home) and then use the local file.

19.4.3.2 Xen* Hypervisor Installation on Fedora* 17

First log into system as root user and ensure that your system is connected to the internet. To install and configure Xen* Hypervisor:

1. Enter **yum install xen* and/or yum install xen* kernel-xen,** or Download from **http://xen.org/products/xen_source** (This downloads latest Xen* Hypervisor available on the xen.org website).

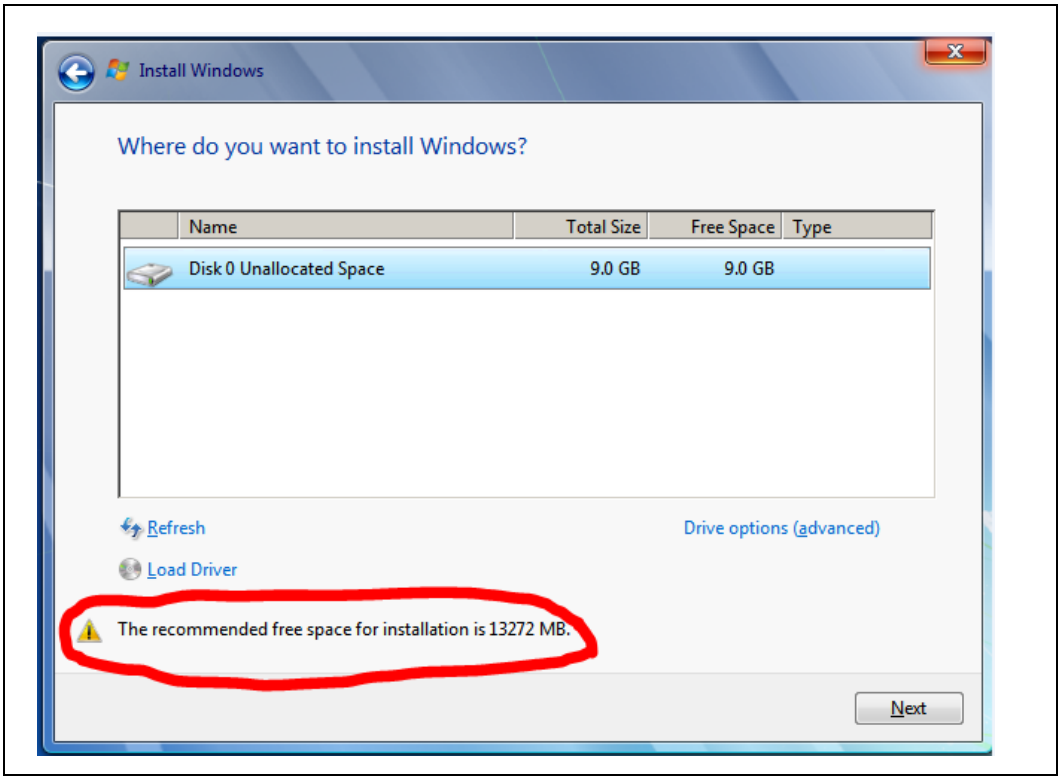
19.4.3.3 Creating a Virtual Machine on Fedora* 17

For a video on Creating a virtual machine on Fedora* 14, refer the Videos Section on Broadwell Platform PCDC VT page.

Note: This process in Fedora* 14 is very similar to Fedora* 17.

1. Go to Applications -> System Tools -> Virtual Machine Manager. (if you are not logged in as root user, user need to provide root password to continue.)
2. Go to File -> Add Connection -> Choose Xen and Click **Connect**.
3. Click on localhost (xen*).
4. Click on Create a new virtual machine icon and enter Name. Choose Xen* as connection type. Select Local installation media (ISO image or CD-ROM).
5. Select the Installation Source (If using an ISO file, it is best to copy the file directly to the system), Choose OS type and version. Click Forward.
6. Choose 2048MB RAM or more, and 1 Processor. Click Forward.
7. Choose Enable storage for this virtual machine, allocate at least 14GB (This number may vary. If you do not have enough space allocated, you may get an error that tells user how much to allocate. Refer to Figure 19-2), and check allocate entire disk now.
8. Optional: In Final step, open Advanced options, use default Virtual network, change Virtual Type to xen*, set architecture as x86_64 and Click Finish.
9. Follow the installation instructions for the OS.

Figure 19-2. Example Warning—Allocating Space for Windows* 7/Virtual Machine



19.4.3.4 Testing Intel® VT Using Xen* VMM in Fedora* 17

The Intel® VT can be tested by assigning PCIe* I/O device(s) to the guest OS. When Intel® VT is used to directly assign an I/O device to a guest, the guest OS has direct access to I/O device hardware and guest VM owns the physical driver for that I/O device.

The test is considered to be passing when all of the following occur:

1. An I/O device can be successfully assigned to guest VM (Section 19.4.3.4.1).
2. Xen* VMM does not report any VT faults. Xen* VMM reports no VT faults in "dmesg" log. User need to search for VT faults by executing the following and search for VT messages:

```
dmesg | grep -i fault
--OR--
xm dmesg | grep -i fault (if using Xen earlier than 4.1)
--OR--
xl dmesg | grep -i fault (if using Xen 4.1.0 or later)
```

3. Guest VM detects the presence of new hardware. (In a Windows* OS, this can be determined through the VM device manager.)

4. If the physical driver for the newly assigned I/O device is present in the guest OS, check that the device is functional

19.4.3.4.1 Assigning an I/O Device Using PCISTUB Method

1. First obtain the Bus, Device, Function (BFD) ID of the device using:

```
lspci --OR-- lspci | grep -i "Ethernet"
Example result:
...
00:19.0 Ethernet controller: Intel Corporation 82566DM Giga-
bit Net...
...
BDF = “00:19.0”
```

2. Now obtain device ID

```
lspci -n
Example Result:
...
00:19.0 0200: 8086:153a (rev 01)
00:16.0 0200: 8086:8c3a (rev 01)
...
Use the BDF to find Device ID
Device ID = “8086 153a”
```

3. Enter the following, in order to unbind and attach the device

```
echo -n 0000:00:19.0 > /sys/bus/pci/devices/0000:00:19.0/
driver/unbind
echo "8086 153a" > /sys/bus/pci/drivers/pci-stub/new_id
echo -n 0000:00:19.0 > /sys/bus/pci/drivers/pci-stub/bind

ls -l /sys/bus/pci/devices/0000:00:19.0/driver
this verifies the binding

xm pci-attach Guest 0:0:19.0
```

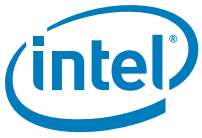
where *Guest* is the name of virtual machine

xl pci-assignable-add/remove

19.4.3.5 Special Instructions to Obtain Serial Log on Fedora* 17

To be added in a future revision.

§ §



20 ISH Firmware (FW) Compliancy

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 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 compliancy 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.

20.1 Test Coverage Summary

Test ID	Test Case Title	Target OS	Automated/ Manual	Mandatory/ Optional
ISS_TST_01	Sensor communication test	Windows*	PETS	Mandatory
ISS_TST_02	Sensor data check	Windows*	Manual	Mandatory
ISS_TST_03	ISH FW loading and execution	Windows*	Manual	Mandatory
ISS_TST_04	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

20.2 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	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 passes if each of the tests were completed successfully without any errors.

20.3 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	Verify the sensors information in the PDT Editor: 1. Open the full SPI image in the FITC tool. (Decompose it) 2. In the FITC tool folder, a folder is created with the name of the image that was decomposed using FITC. 3. Using the PDT Editor open the PDT table from that image, it is located under: FITC\"image_name"\Decomp\PdtBinary.bin. 4. In the PDT Editor, verify that each of the sensors configured with the rights settings.
Test Pass/Fail Criteria	Test passes if the sensors information were configured correctly in the PDT Editor.

20.4 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.

Test ID	ISS_TST_03
Objective	Verify that ISH is responsive and that ISH FW can be read.
Windows* Procedure	1. Boot the platform to AOS/WOS shell. 2. From elevated command line run the ISSUtil Tool: ISSUtil.exe -INFO 3. In the tool output check that: 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 passes if ISH status is "responding" and ISH FW can be read.

20.5 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	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 passes if in the sensor viewer, all of the sensors state is "Ready" and the data is received for each of the sensors

20.6 Test System Sensors

20.6.1 Sensor Noise and Error Levels

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

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 deg
3D Compass	2 deg	2 deg	0.75 deg
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.

20.6.2 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	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. 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. 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.
Objective	Gather statistical data on both sensor data input (RAW sensor data) and data output of sensor algorithms.
Procedure	Automated (PETS) Initial state of the SUT should be S0. 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). **Intel® Platform Enablement Test Suite (Intel® PETS) performs the following steps:** 1. Gather RAW and virtual sensor data over a designated period (i.e. 10s). Data is gathered from all present physical sensors on platform and all available sensor SW drivers. 2. If the System is a 2-in-1 device, convert it into a tablet form-factor (screen on top of keyboard or detached from it_ and repeat step #1
Test Pass/Fail Criteria	Test passes if all sequences show: 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. For #1 and #2 - the tool refers to the pass/fail levels placed in the section "Sensor Noise and Error Levels". In the case that the test results are above the pass/fail limits - the tests raises a "warning" to the user.

20.6.3 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	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. 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.
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	Semi-Automated (PETS) Initial state of the SUT should be S0. The audio sub-system should be fully functional. 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). **Intel® Platform Enablement Test Suite (Intel® PETS) performs the following steps:** 1. The system exercises known interference sources to see if they have influences on the system. Data should be gathered at each step for at least 10 seconds. The interference sources include: — 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 For each sample data sample - the system gathers RAW and virtual sensor data. The noise levels and any movement should be recorded and compared to pass/fail levels. 2. The system exercises known interference sources to see if they have influences on the system. Data Should be gathered at each step. 3. If the system is a 2-in-1 device, convert it into a tablet form-factor (detached/screen on to of keyboard) and repeat steps #1 and #2
Test Pass/Fail Criteria	Test passes if all sequences show: 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. ***Note:*** For #1 and #2 - the tool refers to the pass/fail levels placed in the section "Sensor Noise and Error Levels". ***Note:*** In the case that the test results are above the pass/fail limits - the tests raises a "warning" to the user**.**

20.7 Test System Performance and Effective Calibration under 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	Semi-Automated (PETS) Initial state of the SUT should be S0. The system should have run through the ISS sensor calibration procedure with the calibration data stored and used on the system. The system should be configured in a tablet context. If the device is a 2- in-1, suggest repeating in the PC form-factor with the system placed in a box that can be moved in the pattern shown below. The user is asked to run through the following movements to test the gyroscope: **Test Sub-Section A: Gyroscope Z-Axis:** 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. **Test Sub-Section B: Gyroscope X-Axis:** 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. **Test Sub-Section C: Gyroscope Y-Axis:** 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. **Test Sub-Section D: Accelerometer:** Place the system in the following positions: 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	Test passes if all sequences show: **For the gyroscope:** The correct direction was recorded from the gyroscope when moving the system. For the accelerometer: The accelerometer reading was correct within a 5 degree error.

20.8 Barometer (Pressure) Sensor Sanity Test

Test ID	**ISS_TST_08**
Test Case Title	Barometer (pressure) sensor sanity test
Mandatory/Optional	Optional. Mandatory if a barometer is present
Description	This test confirms the barometer (pressure) sensor is working correctly on the system.
Objective	Test that the barometer sensor is present and responsive to changing elevations
Procedure	Semi-Automated (PETS) Initial state of the SUT should be S0 (OS up). The ISS should be configured in the system FW. 1. Lift the system to a height of 1.5-2.0 meters. Wait 10 seconds. 2. Place the system on the ground. Wait 10 seconds. For each sample data sample - the system gathers RAW and virtual sensor data.
Test Pass/Fail Criteria	Test passes if all sequences show: The pressure sensor recorded a change in altitude relative.

20.9 Light Sensor (ALS) Accuracy Test

Test ID	**ISS_TST_09**
Test Case Title	Light sensor (ALS) accuracy test
Mandatory/Optional	Mandatory
Description	This test reviews the accuracy of the ambient light sensor after it has been characterized.

Test ID	ISS_TST_09
Objective	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. The test is meant to test the accuracy of the ALS after it has been calibrated.
Procedure	Semi-Automated (PETS) 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: 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. The system should be orientated orthogonal to the light source. 1. Light source is tuned to maximum amplitude. ALS reading should be displayed on the screen. Check that the received ALS value is within +/- 10% of the recorded light meter value. The screen brightness should appear not too bright or too dark. 2. Lower the light source to mid-way. Compare again the difference between the ALS and light meter value. The screen brightness should adjust such that it is not too bright or too dark relative to the ambient light level. 3. Tune light source to the lowest level. Compare again the difference between the ALS and light meter value. The screen brightness should adjust such that it is not too bright or too dark relative to the ambient light level. 4. (optional) If a fluorescent light source is available, expose the system to the same "low" light level seen in the previous step. Check that the ALS light levels are correct relative to the light meter. And that the screen brightness is not too bright or too dark.
Test Pass/Fail Criteria	Test passes if all sequences show: For all light levels tested - the ALS is correct within +/- 10%.

20.10 Light Sensor (ALS) Angular Response Test

Test ID	**ISS_TST_10**
Test Case Title	Light sensor (ALS) angular response test
Mandatory/Optional	Mandatory
Description	This test will test the angular response of the ALS sensor to determine if it falls within the requirements of the MSFT HW certification guidelines. MSFT* asks that the light response does not fall by more than 50% when changing the angle of incident light from 0 to 35 degrees. Issues can occur with the sensor angular response due to the light sensor cavity/hole design or other materials covering the light sensor.
Objective	Confirm that the ambient light sensor angular response is greater than 50% at a 35 degree angle of incidence.
Procedure	Semi-Automated (PETS) 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: 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. The system should be orientated orthogonal to the light source. Before starting the test: 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. When running the test: 1. Rotate the system so that the ALS is at a 35 degree angle to the incident light without changing the distance.
Test Pass/Fail Criteria	Test passes if all sequences show: The recorded light level of the ALS does not fall more than 50%.

20.11 360 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	Placing an accelerometer both in the base and lid of the system design enables the system to determine the angle between the lid and base. This algorithm (also called a virtual protractor) tells 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. The goal of this test is to confirm that the lid angles are reported correctly.

Test ID	**ISS_TST_11**
Objective	Confirm that the angle between the base and lid is accurately reported.
Procedure	Semi-Automated (PETS) Initial state of the SUT should be S0 (OS up). The ISS should be configured in the system FW. Place the system on a flat table. Record the reported angle over a 5 second period. 1. 0 degrees. Lid closed (screen facing keyboard). 2. 90deg. Screen open and facing the user. Screen and keyboard are orthogonal with user seeing screen and keyboard at the same time. 3. 180 degrees. Screen and keyboard both facing up. 4. 270 degrees. Screen and keyboard are orthogonal. The user cannot see the screen and keyboard at the same time. 5. 360 degrees. System flat on table. The screen is facing up and the keyboard is facing down.
Test Pass/Fail Criteria	Test passes if all sequences show: The detected angle should be within a ± 10 degrees of accuracy. Over the 5 seconds, the variance of the angle should have been less than +/5 degrees.

20.12 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	Test requires to go through the system modes configured in the PDT Config by adjusting the system position per each mode definition, while verifying and comparing the actual data reported by the PLM algorithm.
Objective	To verify proper configuration and functionality of the PLM algorithm on customer system in S0
Procedure	1. Boot the system to OS. 2. Set the system in a first position according to the last PLM Mode configured in the PDT Config file. 3. User should manually acknowledge when the system is placed in the position as requested in previous step. 4. User should verify if the actual system position reported by the PLM algorithm is aligned to what user confirmed. 5. Continue to the next PLM Mode looping steps 2-4.
Test Pass/Fail Criteria	Test passes only if all PLM Modes are matching the actual system position. i.e. all PLM Modes are successfully matched.

Test ID	**ISS_TST_12B**
Test Case Title	PLM functionality verification with system power transitions
Mandatory/Optional	Optional. Mandatory if PLM is implemented
Description	Test requires to make system power transitions while going through the system modes as configured in the PDT Config file. User is requested to adjust the system position as defined by each Platform Mode, while verifying and comparing the actual data reported by the PLM algorithm to the system position reported by the user.

Test ID	**ISS_TST_12B**
Objective	To verify proper configuration and functionality of the PLM algorithm on customer system while involving system power transition
Procedure	1. Boot the system to OS. 2. Set the system in a first position according to the last PLM Mode configured in the PDT Config file. 3. User should manually acknowledge when the system is placed in the position as requested in previous step. 4. User should verify if the actual system position reported by the PLM algorithm is aligned to what user confirmed. 5. Change the system state to S3. 6. User set the system in the next position according to the last PLM Mode configured in the PDT Config file. 7. User should manually acknowledge when the system is placed in the position as requested in previous step. 8. User to wake the system to OS/S0. 9. User should verify if the actual system position reported by the PLM algorithm is aligned to what user confirmed. 10. Continue to the next PLM Mode looping steps 5-9.
Test Pass/Fail Criteria	Test passes only if all PLM Modes are matching the actual system position. i.e. all PLM Modes are successfully matched.

20.13 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	The e-compass using the system accelerometer and magnetometer can experience errors for multiple reasons including incorrect sensor calibration. This test is designed to show that the heading accuracy is correct in a number of angles/directions.

Test ID	**ISS_TST_13**
Objective	Confirm that the system reports the correct heading accuracy.
Procedure	Semi-Automated (PETS) Initial state of the SUT should be S0 (OS up). The ISS should be configured in the system FW. If the system is a 2-in-1 device, the test should start with the system in the "PC" context (screen facing user with keyboard facing-up on the table). To test that the system is free of external magnetic influence: 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. Intel® Platform Enablement Test Suite (Intel® PETS) performs the following steps: Test System Flat on Table (Z-UP) With a compass, place the system facing north on a flat table: 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 ***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.
Test Pass/Fail Criteria	Test passes if all sequences show: System heading error should not exceed 10 degrees at any rest position.

20.14 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	Automated (PETS) Initial state of the SUT should be S0 (OS up) with the IISS configured in the system FW. 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. Run the following power transitions from S0: 1. Resume from S3 on AC + DC 2. Resume from S3 on DC 3. Resume from S4 on AC + DC 4. Resume from S4 on DC 5. Resume from S5 on AC + DC 6. Resume from S5 on DC 7. Resume from 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 + DC 11. Resume from G3 on DC 12. 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) 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. ** 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' 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").
Test Pass/Fail Criteria	Test passes if all sequences show: 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. ***Note:*** If the sensor or sensor micro-driver does not support the "built in functional test" (test level 3) then the test returns a warning to the user.

20.15 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	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]. These tests confirms if the sensor activity contexts algorithms within the IISS are working properly.

Test ID	**ISS_TST_15**
Objective	Confirm that the system detects the system user activity contexts.
Procedure	Semi-Automated (PETS) Initial state of the SUT should be S0 (OS up). The ISS should be configured in the system FW. Place the system on a flat table. If the system is a 2-in-1 system start in the tablet form factor. 1. 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	Test passes if all sequences show: The system accurately detected the user contexts.

20.16 Sensor Terminal Contexts

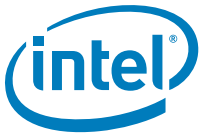
Test ID	**ISS_TST_16**
Test Case Title	Sensor terminal contexts
Mandatory/Optional	Optional. Perform the test if the system holds motion sensors.
Description	The IISS contains terminal context algorithms that can determine how the user is holding the system. This includes determining if the system is held (1) face up / down, (2) portrait up / down, or (3) landscape left / right. These tests confirms if the sensor terminal contexts algorithms within the IISS are working properly.
Objective	Confirm that the system detects the terminal contexts.
Procedure	Semi-Automated (PETS) Initial state of the SUT should be S0 (OS up). The ISS should be configured in the system FW. Place the system on a flat table. If the system is a 2-in-1 system start in the tablet form factor. 1. Place the system face up and face down. 2. Place the system portrait up and portrait down. 3. Place the system landscape left and landscape right.
Test Pass/Fail Criteria	Test passes if all sequences show: The system accurately detected the terminal contexts.

20.17 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 confirms if the sensor gesture contexts algorithm within the IISS are working properly.
Objective	Confirm that the system detects the system user gesture contexts.
Procedure	Semi-Automated (PETS) Initial state of the SUT should be S0 (OS up). The ISS should be configured in the system FW. Place the system on a flat table. If the system is a 2-in-1 system start in the tablet form factor. Lift the system from the table and look at the system.
Test Pass/Fail Criteria	Test passes if all sequences show: The system accurately detected the terminal contexts.

20.18 Wake on Shake Test

Test ID	**ISS_TST_18**
Test Case Title	Wake on shake test
Mandatory/Optional	Mandatory
Description	Wake on different events is a mandatory feature in Win10. As such a test that focuses on the ability to wake the system from S0i3 (CS) is a must.
Objective	Test that ISH can send a wake event to Win OS and the OS waken from S0i3 to S0
Procedure	1. Make sure that system is set in CS state (S0ix). 2. Make sure that shake event is defined in PDT and in Windows* (use SDT to check it). 3. Shake the system. 4. Windows* should wake and log on screen should appear. 5. Repeat the test 3 times. 6. There is a timeout (usually 2 minutes) until Win* goes to SC again, unless the configuration of the specific copy of Windows* on the device set the timer to a different value.
Test Pass/Fail Criteria	Test passes if Windows* awakes all 3 times.



20.19 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	Initial state of the SUT should be S0 (OS up). The ISS should be configured in the system FW. User should hold the tablet/notebook while he/she stands. User should check SDT or any other sensor data report SW on the OS for the current number of step counter. User should start walking while counting his/her steps in a straight line. After counting 50 steps user should stop. 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…). Remark: the step counter starts acting of 10 seconds of stepping, so tests that takes 10 seconds or would not be able to check the counter.
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.

§ §

21 Platform SKU Emulation Check

Overview:

The test case in this chapter was created to verify that the image being used on platforms using ES silicon is using SKU Emulation. This is done verify that the to ensure that customer are using the correct SKU configuration for the platform design(s) they are planning to ship.

Tools for Testing:

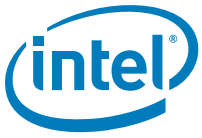
- **Intel® Platform Enablement Test Suite (Intel® PETS)**: Use latest version of this kit. Refer to the Intel® PETS user guide available in the Intel® CSME Compliancy kit for details instructions on how to load and setup the Intel® PETS software.
- **ME Information tool:** EFI (MEInfo.efi), Windows* 32-bit (MEInfoWin.exe), and Windows* 64-bit operating systems (MEInfoWin.exe64).

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).

21.1 Test Coverage Summary

Test ID	Test Case Title	PETS/Manual	Form Factor	Network Factor
SKUEM_001	SKU Emulation check for ES Silicon	PETS	DT/MB	N/A



21.2 Descriptor Mode Test

Test ID	**SKUEM_001**
Test Case Title	SKU Emulation check for ES Silicon
Mandatory/Optional	Mandatory
Description	Proper emulation of the target platform SKU is needed in order to ensure that customer design and layout aligns properly with the HSIO lanes available for USB, PCIe*, and GbE. This test will confirm that the platform image is not set to Super SKU mode.
Objective	Verify that the platform image is using SKU emulation on ES silicon.
Procedure	1. Boot to the target OS. 2. Run MEInfo and check the PCH Device ID.
Test Pass/Fail Criteria	Test passes if PCH Device ID is not one of the following Super SKU values.

PCH Type	PCH Device ID
TGP-H	4381h
	4382h
TGP-LP UP3	A081h
TGP-LP UP4	A086h

Emulated SKU IDs

The customer should verify that the correct SKU emulation setting is being used for their platform design.

Emulated SKU IDs:

PCH Type	Emulated SKU	PCH Device ID
TGP-H	Q590	4384h
	Z590	4385h
	H570	4386h
	B560	4387h
	H510	4388h
	WM590	4389h
	QM580	438Ah
	HM570	438Bh
TGP-LP UP3	Premium UP3	A082h
TGP-LP UP4	Premium UP4	A087h

§ §