

Intel® Management Engine Firmware 11 Release for Skylake S/H PCH

Consumer Readme / Release Notes - NDA

June 2015

Revision 11.0.0.1149 S/H Series PV Release

Intel Confidential



INFORMATION IN THIS DOCUMENT IS PROVIDED IN CONNECTION WITH INTEL PRODUCTS. NO LICENSE, EXPRESS OR IMPLIED, BY ESTOPPEL OR OTHERWISE, TO ANY INTELLECTUAL PROPERTY RIGHTS IS GRANTED BY THIS DOCUMENT. EXCEPT AS PROVIDED IN INTEL'S TERMS AND CONDITIONS OF SALE FOR SUCH PRODUCTS, INTEL ASSUMES NO LIABILITY WHATSOEVER AND INTEL DISCLAIMS ANY EXPRESS OR IMPLIED WARRANTY, RELATING TO SALE AND/OR USE OF INTEL PRODUCTS INCLUDING LIABILITY OR WARRANTIES RELATING TO FITNESS FOR A PARTICULAR PURPOSE, MERCHANTABILITY, OR INFRINGEMENT OF ANY PATENT, COPYRIGHT OR OTHER INTELLECTUAL PROPERTY RIGHT.

A "Mission Critical Application" is any application in which failure of the Intel Product could result, directly or indirectly, in personal injury or death. SHOULD YOU PURCHASE OR USE INTEL'S PRODUCTS FOR ANY SUCH MISSION CRITICAL APPLICATION, YOU SHALL INDEMNIFY AND HOLD INTEL AND ITS SUBSIDIARIES, SUBCONTRACTORS AND AFFILIATES, AND THE DIRECTORS, OFFICERS, AND EMPLOYEES OF EACH, HARMLESS AGAINST ALL CLAIMS COSTS, DAMAGES, AND EXPENSES AND REASONABLE ATTORNEYS' FEES ARISING OUT OF, DIRECTLY OR INDIRECTLY, ANY CLAIM OF PRODUCT LIABILITY, PERSONAL INJURY, OR DEATH ARISING IN ANY WAY OUT OF SUCH MISSION CRITICAL APPLICATION, WHETHER OR NOT INTEL OR ITS SUBCONTRACTOR WAS NEGLIGENT IN THE DESIGN, MANUFACTURE, OR WARNING OF THE INTEL PRODUCT OR ANY OF ITS PARTS.

Intel may make changes to specifications and product descriptions at any time, without notice. Designers must not rely on the absence or characteristics of any features or instructions marked "reserved" or "undefined". Intel reserves these for future definition and shall have no responsibility whatsoever for conflicts or incompatibilities arising from future changes to them. The information here is subject to change without notice. Do not finalize a design with this information.

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

Contact your local Intel sales office or your distributor to obtain the latest specifications and before placing your product order.

Copies of documents which have an order number and are referenced in this document, or other Intel literature, may be obtained by calling 1-800-548-4725, or go to: http://www.intel.com/design/literature.htm%20

All products, platforms, dates, and figures specified are preliminary based on current expectations, and are subject to change without notice. All dates specified are target dates, are provided for planning purposes only and are subject to change.

This document contains information on products in the design phase of development. Do not finalize a design with this information. Revised information will be published when the product is available. Verify with your local sales office that you have the latest datasheet before finalizing a design.

Client Initiated Remote Access may not be available in public hot spots or "click to accept" locations. For more information on CIRA, visit Fast Call for Help Overview

No computer system can provide absolute security. Intel® Identity Protection Technology requires an Intel® Identity Protection Technology-enabled system, including an enabled Intel® processor, enabled chipset, firmware, software, and Intel integrated graphics (in some cases) and participating website/service. Intel assumes no liability for lost or stolen data and/or systems or any resulting damages. For more information, visit http://ipt.intel.com/. Consult your system manufacturer and/or software vendor for more information.

KVM Remote Control (Keyboard, Video, Mouse) is only available with Intel® Core™ i5 vPro™ and Core™ i7 vPro™ processors with Intel® Active Management technology activated and configured and with integrated graphics active. Discrete graphics are not supported.

No computer system can provide absolute security. Intel® Platform/Device Protection Technology requires an enabled Intel® processor, enabled chipset, firmware, software and may require a subscription with a capable service provider (may not be available in all countries). Intel assumes no liability for lost or stolen data and/or systems or any other damages resulting thereof. Consult your Service Provider for availability and functionality. For more information, visit http://www.intel.com/go/anti-theft . Consult your system manufacturer and/or software vendor for more information.

Code names featured are used internally within Intel to identify products that are in development and not yet publicly announced for release. Customers, licensees and other third parties are not authorized by Intel to use code names in advertising, promotion or marketing of any product or services and any such use of Intel's internal code names is at the sole risk of the user.

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

Copyright © 2014-2015, Intel Corporation. All rights reserved.



Contents

1 Introduction 5
1.1 Scope of Document 5
1.2 Acronyms 5

2 Release Kit Summary 7
2.1 Release Kit Details 7
2.2 Kit Overview 7
2.3 Contents of Downloaded Kit 8
2.3.1 Intel® SW Components 8
2.3.2 Image Components 8
2.3.3 System Tools 10
2.3.4 Intel® ICCS Tools 11
2.4 Release Version Numbering Information 12
2.5 Firmware Update Information 12
2.5.1 Firmware Update Terminology 12
2.5.2 VCN Firmware Upgrade / Downgrade Table 13

3 Important Notes 14
3.1 Important Notes 14
3.2 Hardware Configurations 14
3.3 Best Known Configuration 15

4 Kit Details 16
4.1 Build Details 16

5 Intel® ME New Features 17
5.1 RCR Update 17

6 Issue Status Definitions 23

7 Closed Issues 24
7.1 Closed – Intel® ME Kernel 24
7.2 Closed – Intel® Software Tools 32
7.3 Closed – Documentation 40
7.4 Closed – Not a Firmware/Software Bug 41
7.5 Closed – External Dependency 42

8 Known Issues 44
8.1 Open – Intel® ME Kernel 44
8.2 Open – Intel® Software Tools 45



Revision History

Revision Number	Description	Revision Date
11.0.0.1086	Alpha Release S Series	October 2014
11.0.0.1097	Alpha Release U/Y/S Series	December 2014
11.0.0.1100	Engineering Release U/Y/S Series	December 2014
11.0.0.1120	WW12 Beta for Microsoft Windows* 10 Release U/Y/S Series	March 2015
11.0.0.1131	Beta 2 Release U/Y/S Series	May 2015
11.0.0.1133	WW19 ENG Drop Release U/Y/S Series	May 2015
11.0.0.1140	PC Release S/H Series	May 2015
11.0.0.1149	PV Release S/H Series	June 2015

§



1 Introduction

1.1 Scope of Document

This document provides component level details of the downloaded kit and the contents of each folder in the kit.

1.2 Acronyms

Term	Description
BIOS	Basic Input Output System
BLU-RAY PLAYBACK	Blu-ray™ Playback
Boot Guard	Intel® Device Protection Technology with Boot Guard (formerly known as Anchor Cove)
CCA	Closed Chassis Adapter
CRB	Intel Customer Reference Board
FOV	Fixed Offset Variable
FW	Firmware
GbE	Gigabit Ethernet
HECI	Host Embedded Controller Interface. Same as Intel® MEI.
Intel® DAL	Intel® Dynamic Application Loader
Intel® FIT	Flash Image Tool
Intel® ICCS	Intel® Integrated Clock Controller Service
Intel® ISH	Intel® Integrated Sensor Hub
Intel® IPT	Intel® Identity Protection Technology
Intel® MEI	Intel® Management Engine Interface (interface between the Management Engine and the Host system)
Intel® NFC	Intel® PROSet/Wireless Near Field Communications Software
Intel® PETS	Intel® Platform Enablement Test Suite
Intel® PTT	Intel® Platform Trust Technology
Intel® RWT	Intel® Remote Wake Technology
Intel® SVT	Intel® Silicon View Technology
Intel® TA	Intel® Technology Access
Intel® TXT	Intel® Trusted Execution Technology
LAN	Local Area Network
LMS	Local Manageability Service
MAC	Media Access Control

Term	Description
MRC	Memory Reference Code
OS	Operating System
PCH	Platform Control Hub
SPI	Serial Peripheral Interface
SUT	System Under Test
SVN	Security Version Number. Used in Firmware Upgrade / Downgrade capabilities
UNS	User Notification Service
VCN	Version Control Number. Used in Firmware Upgrade / Downgrade capabilities
WMI	Windows* Management Instrumentation



2 Release Kit Summary

This document covers the following Intel® Management Engine Firmware SKUs for the Skylake S/H Series platform:

- Intel® Management Engine Firmware S/H Platforms.
  - Consumer

Kit release information is outlined below:

2.1 Release Kit Details

* **Firmware Support** : PAVP, Intel® Device Protection Technology with Boot Guard.

* **Release** : Skylake S/H PV Release – 11.0.0.1149

* **Target Platform** : S/H Platform.

* **.zip name** : ME11.0_Consumer_11.0.0.1149.zip

Contents:

- Intel® Management Engine Firmware (for Skylake S/H Series Platform)
- GbE PCH SPI components
- Intel Reference System BIOS

2.2 Kit Overview

The kit can be downloaded from VIP (https://platformsw.intel.com/).

Note: A username and password are required to access the website and to log in. User must have an account created for access.

1. After logging in, click on the link 'View All Kits' on the left side of the web page.
2. Click on the corresponding kit number that is to be downloaded.
3. Select and open the appropriate kit component.
4. The Supporting Documentation folder under the selected component contains the following supporting documentation:
   1. Consumer FW Release Notes – This document gives an overview of the contents of the entire downloaded component. Also provides the details on closed and open Sightings and bugs with this kit release.
   2. BIOS Release Notes – This document provides details of BIOS issues resolved with the kit.
5. Click on the Installation Files folder under the selected component and extract the .zip kit into a folder (Example: C:\).

2.3 Contents of Downloaded Kit

Download the kit, as previously specified, into the directory (C:\). The details of the contents and directory structure are listed below:

2.3.1 Intel® SW Components

Installers	Description
ME_SW_MSI	• Intel® MEI is the interface between the host and the Intel® Management Engine firmware. • Drivers and applications on the host that wish to interact with Intel® Management Engine through the host interface use the Intel® MEI host Windows* driver. • Intel® MEI driver is installed by running: C:\[skuName_x.x.xxxx]\Installers\ME_SW_MSI\SetupME.exe • To view the installer options, enter the following in a Command window: **setup.exe -?** and the help dialog should appear. • Additional information can be found in the *Intel(R)_ME_SW_Installation_Guide.pdf* document within this kit.

2.3.2 Image Components

NVM Images are included in:

- Intel(R)_ME11.0_Consumer_11.0.0.1149.zip

This folder contains the component images (BIOS image, Intel® Management Engine image and GbE image) that are integrated to form the final flash image. The table below lists the different images and briefly describes them.



Image	Description
BIOS	• Contains Intel Reference System BIOS. • Supported devices: Skylake U/Y/S Series Platform. • After flashing a new BIOS, enter BIOS setup and 'Load Default Settings' (Press F3). Then 'Save and Exit' (Press F4) from Setup. This is a required step when updating to a new BIOS release. • BIOS image components are located in the following directory: C:\[skuName_x.x.xxxx]\Image Components\BIOS\ • For latest release information and known issues on the BIOS, please refer to the Intel® ME BIOS Writer's Guide.
Intel® ME	• The Intel® Management Engine firmware contains code and configuration data for Intel® Management Engine functions. • This is one of the regions that are integrated into the final flash image that is built using the Flash Image Tool, and is then programmed into the flash. **NOTES:** • For more details on building the flash image, please refer to **SPT Consumer FW Bringup Guide.pdf**, included in the downloaded kit. • For more details on the firmware and related issues, please refer to **Important Notes** section of this document.
GbE	• The GbE hardware is a component embedded in the MCP. GbE region of the flash contains bits that define the configuration of the GbE hardware. • The given Gigabit Ethernet or GbE component image should be integrated with the other images (Intel® ME and BIOS) using the Flash Image Tool, to create a single binary flash image. • The GbE image will be programmed into the SPI flash as part of this integrated image using the Flash Programming Tool. • The GbE folder contains images for PHY silicon. **Example:** n7_spt_h_v_non_lan_sw_0.1.bin (for Desktop only). These images can be used with the Intel® Management Engine.

2.3.3 System Tools

System Tools are included in:

- ME11.0_Consumer_11.0.0.1149.zip

This folder contains system tools that are common to all the firmware components. Please refer to the ***System Tools User Guide.pdf*** document for details on tool usage.

Tool	Description
Intel® Flash Image Tool	• Used to assemble the different elements of the SPI flash Descriptor, Intel Reference System BIOS, Intel® Management Engine firmware, Gigabit Ethernet (GbE) into a single binary image. • **OS Support:** - Windows* 7 (32/64-bit) - Windows* Server 2008(R2) – 2012(R2) (32/64-bit) - Windows* 8.1 (32/64-bit) - Mavericks OS (Mac) • Provides both a GUI and a command line tool.
Intel® Flash Programming Tool	• Used to write the flash image into the SPI flash device. • **OS Support:** - MS DOS 6.22 and above. - DRMK, FreeDOS. - UEFI(64bit) - Windows* PE (3.1, 4.0, 5.0, 5.1) - Windows* 7 (32/64-bit) - Windows* Server 2008(R2) – 2012(R2) (32/64-bit) - Windows* 8.1 (32/64-bit) • Provided as DOS, EFI and Windows* command line tools.
Intel® FWUpdate	• Used to update the Intel® Management Engine's firmware. • **OS Support:** - MS DOS 6.22 and above. - DRMK, FreeDOS. - UEFI(64bit) - Windows* PE (3.1, 4.0, 5.0, 5.1) - Windows* 7 (32/64-bit) - Windows* Server 2008(R2) – 2012(R2) (32/64-bit) - Windows* 8.1 (32/64-bit) • Provided as DOS, EFI and Windows* command line tools.



Tool	Description
Intel® MEInfo	• Verifies that Intel® Management Engine (Intel® ME) firmware is alive and returns data about Intel® ME. • **OS Support:** - MS DOS 6.22 and above. - DRMK, FreeDOS. - UEFI(64bit) - Windows* PE (3.1, 4.0, 5.0, 5.1) - Windows* 7 (32/64-bit) - Windows* Server 2008(R2) – 2012(R2) (32/64-bit) - Windows* 8.1 (32/64-bit) • Provided as DOS, EFI and Windows* command line tools
Intel® MEManuf	• Used on the manufacturing line to validate platform is configured properly. • **OS Support:** - MS DOS 6.22 and above. - DRMK, FreeDOS. - UEFI(64bit) - Windows* PE (3.1, 4.0, 5.0, 5.1) - Windows* 7 (32/64-bit) - Windows* Server 2008(R2) – 2012(R2) (32/64-bit) - Windows* 8.1 (32/64-bit) • Provided as DOS, EFI and Windows* command line tools.

2.3.4 Intel® ICCS Tools

Tool	Description
Clock Commander Tool (CCT)	• ICC Tool is used to get Intel® ICCS registers and settings, see *ICC Tools User Guide* for more information. • **OS Support:** - MS DOS 6.22 and above. - DRMK, FreeDOS. - UEFI(64bit) - Windows* PE (3.1, 4.0, 5.0, 5.1) - Windows* 7 (32/64-bit) - Windows* Server 2008(R2) – 2012(R2) (32/64-bit) - Windows* 8.1 (32/64-bit)

2.4 Release Version Numbering Information

Typical release version numbering is as follows,

11.x.y.z (for example: 11.0.0.zzzz) where:

'11' refers to the Intel® Management Engine 11.x Firmware SKU for Skylake S/H Series Platform.

'x' represents point releases where new features or changes to existing features may be added.

'y' refers to Maintenance and Hot Fix release designations.

'z' refers to firmware release revision.

2.5 Firmware Update Information

Intel® ME Firmware Update (either upgrade or downgrade) is evaluated based on the SVN value, the VCN value, or the PV values. These values work in unison and can impose restrictions at the same time.

2.5.1 Firmware Update Terminology

SVN (Security Version Number): will be incremented if there is a high or critical security fix in Intel® ME Firmware. A downgrade to a lower SVN value will be prohibited.

VCN (Version Control Number): will be incremented if there is a security fix, a significant firmware change or a new feature addition. A downgrade to lower VCN value will be prohibited.

PV (Production Version): Intel® ME Firmware will have a PV bit set. Upgrade to a non-PV firmware is not allowed. An update from non-PV version to a PV is allowed.

Update rules:

- If the system is at PV (Production Version) quality firmware that has PV bit set, update to non-PV firmware is not allowed. Only Non-PV to PV is allowed.
  - Example: 11.0.0.zzzz PV cannot upgrade to 11.2.0.zzzz Beta
- Update to firmware that has lower SVN (Security Version Number) is not allowed.
- Update to firmware that has lower VCN (Version control number) is not allowed.
- Update across major point release is not allowed for example 10.x to 11.x.
- If firmware update setting in Intel® MEBX is password protected, Intel® MEBX password must be supplied during the update.



2.5.2 VCN Firmware Upgrade / Downgrade Table

Intel® ME FW Version	SVN #	VCN #	PV (1 or 0)
11.0.0.1149 (PV S/H Series)	1	3	1
11.0.0.1140 (PC S/H Series)	0	0	0
11.0.0.1133 (WW19 ENG U/Y/S Series)	0	0	0
11.0.0.1131 (Beta 2 U/Y/S Series)	0	0	0
11.0.0.1120 (Windows*10 Beta U/Y/S Series)	0	0	0
11.0.0.1100 (Windows*10 Alpha U/Y/S Series)	0	0	0
11.0.0.1097 (Alpha U/Y/S Series)	0	0	0
11.0.0.1086 (Alpha S Series)	0	0	0

3 Important Notes

This **PV Release** firmware supports Consumer SKU platforms.

Supported = ✓ Limited Support = ⚠ Not Supoorted = ✘

Technology	Support
BLU-RAY* PLAYBACK	✓
Deep Sx	✓
Full Moff Power flows (PP1)	✓
WLAN	⚠
Intel® Insider™	✓
Intel® DAL	✓
Intel® NFC	✓
Intel® IPT	✓
Intel® TA	✓

3.1 Important Notes

- Inclusion of Intel® Technology Access added as features supported.
- In order to accelerate testing of the latest stepping of silicon for both SKL-S 4+2 and SKL U/Y 2+2, **we are moving forward with removing support for the following components in the kits.**

  ME Binaries
  A-1 LP bin support
  A-0 H w/ ROM bypass bin.

  ME kit tools
  Intel® FIT A-step tool

- Intel® Integrated Sensor Hub SPI flash requirements have been detailed in section 5.1 RCR Update, please refer to RCR #CCG101569129 for further information.
- Sighting #222555 contains an issue that spans across most Intel® ME software tools and triggers non functional behavior, refer to section 7.5 for details.

3.2 Hardware Configurations

This release supports the following HW configurations:

- MCP **SKL S/H** (Pre-ES2, ES2)



3.3 Best Known Configuration

For the latest Client Based Skylake S/H Series Platforms Best Known Configuration (BKC), please review Document ID#532298

4 Kit Details

4.1 Build Details

Kit	Build Details	Changes since previous release (11.0.0.1140)?	Reasons for changes
Firmware Version	11.0.0.1149	Yes	See FW issues highlighted below
CRB BIOS Version	SKLX085_01	Yes	See BIOS Release Notes
Intel® MEI Driver Version	11.0.0.1141 Certified for Windows* 7/8.1	Yes	See FW issues highlighted below



5 Intel® ME New Features

5.1 RCR Update

CCG1202920413	**Description:** Intel® ME/CSE FW Support for PTT Re-Certification. **Background:** Intel® will distribute TPM Endorsement Credentials for all PTT versions. These credentials are tied directly to the fuses in each Intel PCH. While a new key can be generated from within PTT, at present, there is no ability to generate a new certificate, preventing use of the fuse for remote attestation.	11.0.0.1126
CCG1202355693	**Description:** PlayReady 3.0 Support in Windows* 10. **Background:** Intel® has been collaborating with Microsoft* to architect and develop PlayReady 3.0 support for Windows* 10. PlayReady 3.0 support is requested for Skylake.	11.0.0.1122
CCG1204031176	**Description:** Added EC region support in Intel® FIT. **Background:** The SKL PCH (both LP and H) added support of a new region in SPI flash dedicated for EC to access. This requires adding certain descriptors by Intel® FIT to the SPI descriptor region.	11.0.0.1122
CCG1303818855	**Description:** Allow Intel® AMT HECI and Agent presence to trigger automatic platfrom reboot. **Background:** When a NUC (Next Unit of Computing) PC is deployed as a Conference Room PC (un-attendant device) or a digital sign, it is targeted to be available 24x7 and remotely managed/maintain by Intel® IT. Intel® IT is planning to deploy NUC devices with smart space SW capabilities to conference rooms at Intel starting 2015 and already has a fleet of digital signs. Intel® IT chose to use Intel® vPRO NUC since they are providing the manageability requirements.	11.0.0.1118

	Intel® IT would like to have the capability to identify OS and critical services hanging on the NUC and automatically reboot the device in order to bring it back to normal functional state.	
CCG120939251	**Description:** Control Intel® ME Global Reset on Critical Failure. **Background:** Provide a mechanism whereby the BIOS can notify the Intel® ME to enter a protected BIOS update window in which the Intel® ME will not initiate a global reset for any reason. The BIOS can query Intel® ME to verify if Intel® ME is currently in protected mode. After BIOS update is complete, BIOS will initiate a global reset to exit the protected mode.	11.0.0.1116
CCG1013636234	**Description:** Integrated Touch Support on Skylake. **Background:** Engaged with Touch IC vendors - Ntrig, Synaptics and Flatfrog, Sharp and Atmel. Touch controller integration competitive need, better control over UX, reduces cost & opportunity to lead next gen technology & capabilities.	11.0.0.1116
CCG1403968195	**Description:** Removal of VSCC checking from Intel® FW tools. **Background:** In past generations the VSCC data had to be populated in both BIOS and in Intel® ME. VSCC or "Vendor Specific Control Codes" are basically the commands that each SPI parts understands (i.e. read, write, dual and quad read / write, erase, etc.). The VSCC data population was a purely manual process prone to errors, checks were required to confirm that BIOS and Intel® ME both matched to prevent bad behavior on the platform from a VSCC mismatch. The tool reads in both BIOS and Intel® ME VSCC values and verifies that they both match. In Skylake generation requires SFDP enabled SPI parts. The only reason the VSCC table still exists is to enable Quad mode on SPI parts which do not support Rev A of the SFDP standard.	11.0.0.1109



CCG1202992999	**Description:** Removal of EPID_CP, Service Provider Permits, and Transaction Locker starting Intel® ME11.0. **Background:** Intel® Insider™ EPID DRM hardware content had used EPID-CP commands for the protection media player. As the industry has migrated into UltraViolet CFF, Intel® Insider™ adopted a new DRM by OMA CMLA, and have made a plans to end of life all EPID DRM support with Broadway. All EPID-CP related commands can be removed from Intel® ME11.0.	11.0.0.1109
CCG1017614900	**Description:** Intel® ISH SPI layout requirements. **Background:** OEMs may choose to adopt either a Intel® Integrated Sensor Hub, a discrete sensor hub, or no hub at all. Since flash size is an increasing pain point for OEMs, customers that opt not to use a hub solution, should not take the impact of the flash size that Intel® ISH introduces.	11.0.0.1109
CCG101569129	**Description:** Secure Location Based Services (LBS) **Background:** The goal of Location Based Services DAL applet (LBS) is to provide Secure and Authenticated Platform location information. This will raise the assurance of the PC's location data and allow using location as part of authentication capabilities as another Authentication factor.	11.0.0.1086
CCG1013174446	**Description:** Formalize 16MB Intel® ME UMA requirement for Consumer SKU. **Background:** Microsoft* OS's hold strong requirements for low system reserved memory usage in order to get WHCK certification for the platform. There is not an official requirement for the ME UMA size on the platform. As such, the purpose of this request is to formalize the 16MB Intel®ME UMA size requirement for	11.0.0.1086

	Consumer SKU and 32MB ME UMA size requirement for Corporate SKU.	
CCG1013251855	**Description:** Intel® Anti-Theft Technology removal. **Background:** When the decision was made to wind down the Intel®AT efforts a few weeks back, the door was left open to potentially continue to support some parts of the Technology in specific segments.	11.0.0.1086
CCG1203593318	**Description:** OEM Certificate file input feature removal. **Background:** Previous versions of Intel®FITC, now Intel®FIT, allowed entry of the OEM certificate by inputting or loading a file into the tool before loading the image. If desired, users could load a certificate file into the certificate stream field to be included in compiled image. They can also enter as a hash stream as well.	11.0.0.1086
CCG101706993	**Description:** Intel® ME Fwupdlcl display changes from ME 10. **Background:** The firmware will provide an accurate estimate, since firmware update is based on an algorithm which takes into account previous update times and the size of the binary to be updated. This phased approach allows the code used for controlling the flow and updating the firmware for full update to be shared.	11.0.0.1086
CCG101707021	**Description:** Intel® MEmanuf Flexibility. **Background:** Intel®MEManuf is a tool which engineers internal and external to Intel® use to verify the state of various Intel®ME firmware features, status registers, and BIST results. The tool architecture needs to be updated in order to be more maintainable, quicker to	11.0.0.1086



	develop, and less error prone throughout various OS's. When a new SKU is added or a Intel® FW capability bit changes for example, all functions must be updated separately.	
CCG101707078	**Description:** Intel® FIT feature based user interface. **Background:** There is a new version of Intel®FITC, called Intel®FIT, which is based on a new table based architecture. This tool currently only supports a command line. Skylake time frame, the tools team is switching to this architecture in order to support a single source base, instead of two which was done on LynxPoint and WildcatPoint.	11.0.0.1086
CCG101234981	**Description:** Extended Strap-set message to CPU. **Background:** Part of Skylake new direction is the removal of the in-die integrated voltage regulator. Skylake has many SKU's and platform topology, 7 external Voltage Regulators with different types of VRs, connectivity, and OEM choices.	11.0.0.1086
CCG120227850	**Description:** DE feature Remote Wake from Consumer SKU. **Background:** Remote Wake was a feature in Consumer SKU and requires code to run in Sx operations (CM3 state). Removing this feature and respective code decreases image size.	11.0.0.1086
CCG101760542	**Description:** EPID Provisioning Progress is to be Reported by Session Manager.	11.0.0.1086

	Background: Initial EPID group public key certificate provisioning can take a significant amount of time and other operations must wait until the initial provisioning has completed. This change extends Session Manager to get additional error codes when provisioning is in progress or when completed.	
CCG1012061562	**Description:** Remove BUP-HECI interface BIOS interface and replace with HECI MKHI BIOS interface. **Background:** Remove FWSTS register based Intel® ME interface and reduce complexity for host/FW.	11.0.0.1086
CCG1202346088	**Description:** CLI messages for administration privilege requirements for running Intel®FWUpdate under Windows* OS. **Background:** When running Intel®FWUpdate via CLI in Windows* OS without administrator privileges, the tool may display: Error 8193: Intel (R) ME Interface : Cannot locate Intel® ME device driver. Those unfamiliar with the tool may misinterpret the error as a platform problem vs. the lack of admin account privileges.	11.0.0.1086



6 Issue Status Definitions

This document provides sightings and bugs report for Intel® Management Engine Firmware 11.0 SKU, Software and Tools for the Skylake U/Y/S Series Platform. Each report contains a snapshot of sightings and critical internal bugs dating to the Friday of the week in which it was released. At the time of a milestone release, this report will be distributed with the Intel® ME Kit and will provide information on new issues and the status of old issues (replacing the Release Notes document).

The issues are separated into sub-groups to assist in understanding the status of the issues and what action, if any, needs to be done to address the issue. The names and definitions of the sub-groups are detailed below.

Closed Issues: Issues will not be classified as "Closed" until the fix is verified with the appropriate firmware version or disposition given below. Closed issues are separated into three different categories:

- **Closed – Fixed in Firmware Kit:** All issues detailed in this section have been fixed in the firmware version identified in the individual sighting details.
- **Closed – No Plan to Fix**: All issues detailed in this section are not planned to be fixed in any revision of the firmware.
- **Closed – Documentation Change:** All issues detailed in this section require a change to either a specification and/or a documentation change. The specific revisions to the appropriate documentation/specification are identified in the issue details.

Open Issues: New sightings and bugs will be classified as "Open" issues until the fix is verified with the appropriate firmware version. Open issues are separated into categories based on suspected component. All issues under Open Issues are still under investigation. Issues may or may not be root caused.

Note: Any issues that are still open for production revisions of the components will be documented in the respective specification update documents.

Sightings listed in this document apply to ALL Skylake CRB SKU's unless otherwise noted either in this document or in the sightings tracking systems.

7 Closed Issues

7.1 Closed – Intel® ME Kernel

Issue #	Description	Affected Component/Impact / Workaround/Notes	Fixed in Kit#
224632	Intel® MEInfo stops responding after manufacturing mode has been closed and committing FPF's.	**Affected Component** – FW.Apps.MCA **Impact:** Intel® MEInfo may hang after committing FPF's. **Workaround:** None **Notes:** 1. Boot to Windows* OS. 2. Run Intel® FPT –closemnf. 3. Reboot. 4. Run Intel® FPT –commitfpf All.	11.0.0.1140
225171	Setting Max spread in the Intel® ICC section via Intel® FIT does not hold spread value after image has been built.	**Affected Component** – FW.ICC **Impact:** Intel® ICC may not hold Max spread value. **Workaround:** None **Notes:**	11.0.0.1140
224622	During an active KVM session, waking a system from Sx to S0 causes the remote system to lose video signal, both mouse and keyboard still operational.	**Affected Component** – FW.OS.Driver&Service.HECI **Impact:** KVM video may disappear on remote system. **Workaround:** None **Notes:**	11.0.0.1140
221932	Partial FW update via Intel® Management Security Status does not initiate.	**Affected Component** – FW.OS.Driver&Service.FWUpdate **Impact:** Intel® Management Security Status may not initiate a partial FW update. **Workaround:** None **Notes:**	11.0.0.1133
224720	Intel® FWUpdate returns an error in DOS after trying to displaying FW information via –fwver command.	**Affected Component** – FW.OS.Driver&Service.FWUpdate **Impact:** Intel® FWUpdate may return errors in DOS. **Workaround:** **Notes:**	11.0.0.1133



Issue #	Description	Affected Component/Impact / Workaround/Notes	Fixed in Kit#
224782	Intel® MEInfo displays ICC as not programmed after waking the platform from an Sx state.	**Affected Component** – FW.ICC **Impact:** Platform may hand after a warm reset. **Workaround:** **Notes:** 1. Boot to Windows* OS. 2. Run Intel® MEInfo, ICC is displayed as programmed. 3. Transition platform to S4 and wake back to S0. 4. Run Intel® MEInfo again, ICC not programmed.	11.0.0.1136
224929	Clearing CMOS may not cause the FW settings to Return to Defaults on a Consumer SKU platform.	**Affected Component** – FW.OS.Driver&Service.HCI **Impact:** CMOS clear may not work on Consumer SKU. **Workaround:** **Notes:**	11.0.0.1136
224620	Non DeepsSx supported platforms may encounter a network wake issue even though the DeepsSx function is not enabled.	**Affected Component** – FW.OS.Driver&Service.MCTP **Impact:** Platform may not stay down properly in each Sx sleep state. **Workaround:** None **Notes:**	11.0.0.1136
224755	A general warm reset causes a platform to hang in S0 sporadically and cannot initiate a reset flow.	**Affected Component** – FW.OS.Driver&Service.PMDriver **Impact:** Warm resets may hang platform in S0. **Workaround:** G3 the platform and continue to boot. **Notes:**	11.0.0.1136
221932	Partial FW update via Intel® Management Security Status does not initiate.	**Affected Component** – FW.OS.Driver&Service.FWUpdate **Impact:** Intel® Management Security Status may not initiate a partial FW update. **Workaround:** None **Notes:**	11.0.0.1133
224720	Intel® FWUpdate returns an error in DOS after trying to diplaying FW information via –fwver command.	**Affected Component** – FW.OS.Driver&Service.FWUpdate **Impact:** Intel® FWUpdate may return errors in DOS. **Workaround:** **Notes:**	11.0.0.1133

Issue #	Description	Affected Component/Impact / Workaround/Notes	Fixed in Kit#
224779	Intel® FWUpdate has issues restoring binaries that have been saved prior.	**Affected Component** – FW.OS.Driver&Service.FWUpdate **Impact:** Restore command may not function with Intel® FWUpdate. **Workaround:** **Notes:**	11.0.0.1131
222851 223628	When proceeding with a locked Intel® FW on a platform, re-flashing Intel® FW via Intel® FW Update to regain access to Intel® ME, is followed by boot failure and no access to Intel® ME.	**Affected Component** – FW.OS.Driver&Service.PMDriver **Impact:** Intel® Software Tools unable to communicate to Intel® ME, Platform boot issues. **Workaround:** None **Notes:** Reproduction Steps: 1. Flash locked Intel® FIT image. 2. Boot to Windows* OS. 3. Verify Intel® FPT cannot access Intel® ME region. 4. Use Intel® FWUpdate to re-flash, reset. 5. Boot issues occur, Intel® FPT nonfunctional.	11.0.0.1128
224142	Once a platform is moved from S0 to Sx CM3-PG, sending an MCTP command for a FW response is delayed and an MCTP discovery occurs.	**Affected Component** – FW.OS.Driver&Service.MCTP **Impact:** Wake abilities lost when moving platform into CM3-PG state. **Workaround:** None **Notes:**	11.0.0.1128
224069	If a Sensor Service EID does not match after an MCTP rediscovery, an HID handshake may not occur.	**Affected Component** – FW.OS.Driver&Service.MCTP **Impact:** Sensor EID difference may not initiate a proper HID handshake. **Workaround:** None **Notes:**	11.0.0.1128
224232	Intel® FPT WLAN Power Well does not update after committing a new value.	**Affected Component** – SW.Tools.FlashImageTool **Impact:** Intel® FPT may not change WLAN Power Well bit correctly, resulting in communication limitation across the network. **Workaround:** None **Notes:**	11.0.0.1126



Issue #	Description	Affected Component/Impact / Workaround/Notes	Fixed in Kit#
224157	When clearing CMOS via jumper or coin battery, global resets occur followed by End Of Post Message during post.	**Affected Component** – FW.Apps.MCA **Impact:** Platform may boot with End Of Post errors after CMOS clear. **Workaround:** None **Notes:** Reproduction Steps: 1. Flash an image to the SUT. 2. Clear CMOS. 3. Boot the system, global resets may occur. 4. G3 the system, and clear CMOS once more. 5. Plug in AC power, a global reset may occur followed by End Of Post message.	11.0.0.1126
224272	Platform instability may occure when a WLAN card is inserted to the system and booted up into S0.	**Affected Component** – FWOS.ProcessMgr **Impact:** WLAN card may cause sporadic behavior duing platform boot. **Workaround:** None **Notes:** Reproduction Steps: 1. Insert WLAN card to SUT. 2. Boot to Windows* OS. 3. Shutdown, G3. 4. Boot to Windows* OS.	11.0.0.1126
223230	Intel® FWUpdLcl has issues with updating WLAN microcode properly.	**Affected Component** – FW.OS.Driver&Service.WLAN **Impact:** Wireless LAN functionality may not function. **Workaround:** None **Notes:** Reproduction Steps: 1. Move platform to S0. 2. Run "FWUpdLcl64.exe -f 'image' -partid WCOD" 3. Move to G3 4. Move to S0 5. Wireless Microcode does not update.	11.0.0.1126

Issue #	Description	Affected Component/Impact / Workaround/Notes	Fixed in Kit#
224043	Disabling Manageability Mode in Intel® MEBX causes hang on black screen when entering Sx state.	**Affected Component** – FW.AMT.General **Impact:** May not be able to return from platform sleept states. **Workaround:** None **Notes:** Reproduction Steps: 1. Boot to Intel® MEBX. 2. Set Manageability Feature to disable. 3. Boot to Windows* OS. 4. Put platform into any Sx state.	11.0.0.1122
223918	When RTC battery has been cleared, on next boot, the system will get stuck in a global reset loop.	**Affected Component** – FW.OS.PolicyManager **Impact:** Continuous global resets may occur. **Workaround:** None **Notes:** Reproduction Steps: 1. Flash image. 2. Boot to Windows* OS. 3. Put the platform in a G3 state. 4. Remove RTC battery, then reattach. 5. Connect AC power. 6. Boot loop occurs.	11.0.0.1122
221717 223204	Intel® FPT fails to read/update NVARS, determines that Intel® ME is in a non-functional state.	**Affected Component** – FW.Apps.MCA **Impact:** Intel® ME may be disabled. **Workaround:** None **Notes:** Reproduction Steps: 1. Boot to Windows* OS. 2. Execute command Intel® FPT –r CfgSrvFqdn. 3. Command fails.	11.0.0.1122
222187	System resets occur when hotkey for Intel® MEBX is pressed.	**Affected Component** – FW.OS.PolicyManager **Impact:** Unable to enter Intel® MEBX screen. **Workaround:** **Notes:**	11.0.0.1117



Issue #	Description	Affected Component/Impact / Workaround/Notes	Fixed in Kit#
223275	System continuously resets when using a Secure Boot profile that is anything other than Profile 0.	**Affected Component** – FW.Bringup.BootGuard **Impact:** Platform may run a reset cycle due to a different Profile set. **Workaround:** None **Notes:**	11.0.0.1117
223519	When AC power is connected just before a G3 state (also without RTC battery), several boot loops may occur.	**Affected Component** – FW.OS.Driver&Service.PMDriver **Impact:** Continous boot loops may occur. **Workaround:** During POST, enter BIOS screen to change the date then exit/save, system should reset and recover into EFI shell. **Notes:**	11.0.0.1117
222248	When platform moves from a G3-S5 state, Intel® ME may not move to its proper CM state.	**Affected Component** – FW.OS.Driver&Service.PMDriver **Impact:** Intel® ME states may not transition in parallel with board Sx state transitions. **Workaround:** **Notes:**	11.0.0.1117
223274	Intel® FIT GUI does not match SPI Programmers Guide, CPU Straps SVID section not seen within Intel® FIT.	**Affected Component** – SW.Tools.FlashImageTool **Impact:** Intel® FW building process confusion may occur due to misguided information. **Workaround:** None **Notes:**	11.0.0.1117
223481	Enabling Intel® PTT may cause a hang in the Intel® FW from a CM0 entry or exit transition.	**Affected Component** – FW.OS.Driver&Service.Crypto **Impact:** Intel® ME may hang from boot or resume from Sx state. **Workaround:** None **Notes:** Reproduction Steps: 1. Build Intel® FW with Intel® PTT enabled. 2. Boot to Windows* OS. 3. Transition into and resume from Sx states. 4. Verify Intel® ME status.	11.0.0.1117

Issue #	Description	Affected Component/Impact / Workaround/Notes	Fixed in Kit#
223318	Intel® MEI drivers yellow bang after several restart cycles.	**Affected Component** – FW.OS.General **Impact:** Intel® MEI functionality loss after restarts. **Workaround:** None **Notes:** Reproduction Steps: 1. Run reboots on platform. 2. Check Device Manager periodically.	11.0.0.1109
221444	Intel® FPT causes system not to boot after close manufacturing flow.	**Affected Component** – SW.Tools.FlashProgrammingTool **Impact:** Unable to initiate manufacturing flow. **Workaround:** **Notes:** Resolved, to be fixed in future release.	11.0.0.1109
223327	System cannot enter Power Gating when HECI driver is disabled.	**Affected Component** – FW.uKernel.Power **Impact:** Unable to enter PG flow. **Workaround:** None **Notes:** Reproduction Steps: 1. Boot to Windows* OS. 2. Run PG test with HECI enabled. 3. Next, run test with HECI disabled. 4. No longer able to enter PG state.	11.0.0.1109
221459/ 221998	Selecting Secure Boot profiles 4 or 5 within the Intel® FIT tool, may cause platform to hang.	**Affected Component** – FW.Bringup.BootGuard **Impact:** May need to disable Secure Boot in order for platform to post. **Workaround:** None **Notes:** Reproduction Steps: 1. Open up Intel® FIT Tool. 2. Load image. 3. Select Secure Boot Profile 4 or 5. 4. Build/flash image onto platform.	11.0.0.1108
222551	Using profile 5 for Bootguard within Intel® FIT, the target platform may hang after warm resets are initiated.	**Affected Component** – FW.Bringup.BootGuard **Impact:** System resets may not function properly. **Workaround:** None **Notes:**	11.0.0.1108



Issue #	Description	Affected Component/Impact / Workaround/Notes	Fixed in Kit#
221411	Intel® ME FW does not restore dynamic changes after Sx and warm reset cycles.	**Affected Component** – FW.ICC **Impact:** Intel® ME FW may not restore dynamic settings. **Workaround:** None **Notes:**	11.0.0.1096
221375	When Intel® FPT is assigned to handle flash, dump, and verify tasks in the OS, platform is subject to hang.	**Affected Component** – FW.OS.Driver&Service.HCI **Impact:** Not all features of the Intel® FPT may function within the Windows* OS. **Workaround:** None **Notes:**	11.0.0.1096
221599	Reset counter does not change after platform reset and verifying with Intel® MEInfo	**Affected Component** – FW.Bringup.FWSTS **Impact:** Wrong Intel® ME FW status displayed. **Workaround:** **Notes:** Reproduction Steps: 1. Boot platform from G3. 2. Check Intel® ME FW status via Intel® MEInfo. 3. Repeat.	11.0.0.1092
220393	Secure Boot fails to shut down the platform even if a request to shut down or reporting of any error is called.	**Affected Component** – FW.Bringup.PMDriver **Impact:** May need to disable Secure Boot in order for platform to post. **Workaround:** None **Notes:**	11.0.0.1090
221518	Intel® ME still functional even after being disabled in BIOS.	**Affected Component** – FW.OS.PolicyManager.SKUMgr **Impact:** Intel® ME cannot be disabled. **Workaround:** None **Notes:** Reproduction Steps: 1. Boot platform to BIOS. 2. Set Intel® ME state to disabled. (Intel Advanced Menu → PCH-FW Configuration) 3. Save changes. 4. Reset platform. 5. Check if Intel® ME state is disabled.	11.0.0.1086

7.2 Closed – Intel® Software Tools

Issue #	Description	Affected Component/Impact / Workaround/Notes	Fixed in Kit#
225183	Generating a CFG file via Intel® FPT –cfggen command to perform any updates causes Intel® FPT access errors.	**Affected Component** – SW.Tools.FlashProgrammingTool **Impact:** Unable to update using dumped CFG file from Intel® FPT –cfggen. **Workaround:** None **Notes:**	11.0.0.1144
225074	Intel® FPT tool hangs when a CFG file has been dumped and then inputted with the –u –in command.	**Affected Component** – SW.Tools.ProgrammingTool **Impact:** Intel® FPT may hang after inputting a CFG file.. **Workaround:** None **Notes:**	11.0.0.1140
224950	Intel® FPT casues Windows* OS to hang at the restart screen when running a -closeMNF followed by a –greset.	**Affected Component** – SW.HECI Driver **Impact:** Platform hang on restart screen during Intel® FPT –greset. **Workaround:** None **Notes:** 1. Flash BIOS/FW. 2. Boot to Windows*. 3. Run Intel® FPT –closemnf NO –y. 4. Followed by Intel® FPT –greset.	11.0.0.1136
224605	Intel® FPT Close Manufacture (EOM), causes HECI communication issues.	**Affected Component** – SW.Tools.FlashProgrammingTool **Impact:** HECI driver communication may disrupt with Intel® FPT –closemnf. **Workaround:** None **Notes:**	11.0.0.1140
224444	Intel® FIT does not set recommended Power Management Configuration for Intel® ICC by default.	**Affected Component** – SW.Tools.FlashImageTool **Impact:** Recommended Intel® ICC values not set. **Workaround:** None **Notes:** 1. Launch Intel® FIT. 2. Add Intel® ME binary. 3. Navigate to Integrated Clock Controller tab.	11.0.0.1133



Issue #	Description	Affected Component/Impact / Workaround/Notes	Fixed in Kit#
224741	Intel® FWUpdate has issues reading FW version file when updating Intel® ISH FW using –PartId command.	**Affected Component** – SW.Tools.FwUpdLcl **Impact:** Intel® FWUpdate may not update Intel® ISH portion of FW. **Workaround:** None **Notes:** 1. Retrieve latest Intel ® FWUpdate tool. 2. Run command: "FWUpdLcl64.exe –f ME.bin –partid ISHC"	11.0.0.1133
224644	When running Intel® FPT –cfggen in the EFI shell, it does not output Intel® ME Network Service in the configuration file.	**Affected Component** – SW.Tools.FlashImageTool **Impact:** Intel® FPT -cfggen may not output network services info. **Workaround:** None **Notes:**	11.0.0.1133
224753	Intel® FWUpdate spontaneously resets the platform once the same Intel® ME region is flashed.	**Affected Component** – SW.Tools.FwUpdLcl **Impact:** Platform may reset unexpectedly after an Intel® FWUpdate. **Workaround:** None **Notes:** Run FWUpdLcl64.exe –f <me region> -ALLOWSV -Y	11.0.0.1133
224749	Intel® FIT encounters a build size error when trying to replace a decomposed Intel® ME region.	**Affected Component** – SW.Tools.FlashImageTool **Impact:** Intel® FIT may not build image with a replaced Intel® ME binary. **Workaround:** None **Notes**	11.0.0.1131
224505	Intel® CCT "–h" or "?" command display errors.	**Affected Component** – SW.Tools.FlashImageTool **Impact:** Intel® CCT help command may not function. **Workaround:** None **Notes**	11.0.0.1128
224073	Disabling Intel® ME via Windows* Device Manager or the Intel® FPT –disableme command, cause reboot/shutdown hangs in the OS.	**Affected Component** – SW.HECI Driver **Impact:** Windows* OS may hang during a shutdown or reboot when Intel® ME is disabled. **Workaround:** None **Notes:**	11.0.0.1126

Issue #	Description	Affected Component/Impact / Workaround/Notes	Fixed in Kit#
223289	Intel® FWUpdate Tool hangs when multiple Save operations are performed.	**Affected Component** – FW.OS.Driver&Service.FWUpdate **Impact:** Intel® FWUpdate hangs when saves are performed. **Workaround:** None **Notes:**	11.0.0.1126
224081	Touch functionality may stop working after a warm reset has occurred.	**Affected Component** – FW.OS.Driver&Service.iTouch **Impact:** Touch panel stops working after warm reset. **Workaround:** None **Notes:**	11.0.0.1122
223974	Intel® MEInfo returns no information when ran on both EFI and Windows*	**Affected Component** – SW.Tools.MEInfo **Impact:** Intel® MEInfo may not any output information. **Workaround:** None **Notes:**	11.0.0.1122
223395	Intel® FIT should not allow images to build when Intel® ISH OEM Public Key Hash are set to zeros.	**Affected Component** – SW.Tools.FlashImageTool **Impact:** Intel® FIT may retrieve build errors when changing Intel® ISH Value. **Workaround:** None **Notes:**	11.0.0.1122
221978	Intel® FIT has issues decomposing any pre-built images	**Affected Component** – SW.Tools.FlashImageTool **Impact:** May not be able to decompose/edit pre-built images via Intel® FIT. **Workaround:** None **Notes:**	11.0.0.1122
223839	Intel® MEI Driver folder structure has incorrect paths, along with missing symbols.	**Affected Component** – SW.HECI Driver **Impact:** Driver folders may be missing or in the incorrect path. **Workaround:** None **Notes:**	11.0.0.1122



Issue #	Description	Affected Component/Impact / Workaround/Notes	Fixed in Kit#
223258	Under Network & Connectivity tab within Intel® FIT, user is able to set an out of range address to both MAC SMBus, and PHY SMBus addresses without error, causing Intel® FIT build image to fail without necessary info of failure.	**Affected Component** – SW.Tools.FlashImageTool **Impact:** Incorrect value can be entered within Intel® FIT, blocking build of Intel® FW with little error info. **Workaround:** None **Notes:** Reproduction Steps: 1. Start Intel® FIT. 2. Go to Networking & Connectivity tab. 3. Change either GbE MAC SMBus, or GbE PHY SMBus address to an incorrect value. 4. Build image. 5. Image fails to build unknowingly to users.	11.0.0.1122
223351	Intel® FIT does not display "CPUPCIBCLK" under: Integrated Clock Controller → Profile → Clock Output Configuration.	**Affected Component** – SW.Tools.FlashImageTool **Impact:** Cannot access settings for overclocking. **Workaround:** None **Notes:**	11.0.0.1122
223376	When renaming or deleting the "fparts.txt" file within Intel® FPT, Intel® FPT outputs special characters that does not translate to the issue of modifying that file when run.	**Affected Component** – SW.Tools.FlashProgrammingTool **Impact:** Unexpected error code may appear when running Intel® FPT. **Workaround:** Do not rename/delete "fparts.txt" **Notes:** Reproduction Steps: 1. Rename or delete the fparts.txt. 2. Execute Intel® FPT –i command. 3. Unexpected error occurs.	11.0.0.1117
223644	Intel® vPro Downgrade returns a success message when EOP is disabled even though a downgrade has not been preformed.	**Affected Component** – FW.OS.Driver&Service.HCI **Impact:** Invalid downgrade message. **Workaround:** **Notes:** Reproduction Steps: 1. Burn SPI image to platform.	11.0.0.1117

Issue #	Description	Affected Component/Impact / Workaround/Notes	Fixed in Kit#
221693 222086	Intel® FIT SPI image decomposing after image dump from platform causes tool to force close.	**Affected Component** – SW.Tools.FlashImageTool **Impact:** May be unable to decompose image within Intel® FIT tool. **Workaround:** **Notes:** Reproduction Steps: 1. Burn SPI image to platform. 2. Dump SPI image from platform. 3. Decompose the SPI from platform to Intel® FIT tool.	11.0.0.1117
220572	HECI disable command may not work correctly when input.	**Affected Component** – FW.OS.Driver&Service.HECI **Impact:** Disabling HECI through command may not work. **Workaround:** **Notes:**	11.0.0.1117
222431	Using invalid VSCC entries within Intel® FIT does not display a build failure message as a safety measure.	**Affected Component** – SW.Tools.FlashImageTool **Impact:** Users may not receive a build failure when building with the wrong VSCC. **Workaround:** **Notes:** If VSCC has the parts listed within the database, users should not see an impact.	11.0.0.1117
220761	Intel® FIT defaults boot profile to 0 when a non-existent profile is selected within Intel® FIT.	**Affected Component** – SW.Tools.FlashImageTool **Impact:** Users may choose profile 0 by mistake. **Workaround:** Type profile name within XML file. **Notes:**	11.0.0.1117
221125	Intel® FIT SSC bits changed after overclocking profile has been loaded in Intel® FIT.	**Affected Component** – SW.Tools.FlashimageTool **Impact:** Intel® FIT overclocking settings instabilities. **Workaround:** **Notes:** ICC clock design for PCIE doesn't allow clock changes.	11.0.0.1117
223480	Intel® MEI driver may cause a BSOD after a certain amount of Sx transition cycles.	**Affected Component** – SW.HECI Driver **Impact:** When returning from an Sx state, Windows* Blue Screen error may occur. **Workaround:** **Notes:**	11.0.0.1117



Issue #	Description	Affected Component/Impact / Workaround/Notes	Fixed in Kit#
223352	When flashing a full SPI binary, Intel® FPT may fail to disable write protection for BIOS.	**Affected Component** – SW.Tools.FlashProgrammingTool **Impact:** Unable to flash images. **Workaround:** **Notes:**	11.0.0.1109
222440	Intel® FPT flash and erase commands exhibit errors 86 and 8193.	**Affected Component** – SW.Tools.FlashProgrammingTool **Impact:** Unable to flash or erase FW. **Workaround:** **Notes:**	11.0.0.1109
222756	Intel® FIT displays a warning indicating that it has failed to detect a SKU upon building an image.	**Affected Component** – SW.Tools.FlashImageTool **Impact:** Indicates that a failure occurred when building an image, even though it is not supposed to be an error. **Workaround:** **Notes:** Intel® FIT reports a SKU warning due to the fact that certain Intel® ME FW may not have a SKU set, which displays the message during build. The error message is meant to be a notification rather than an error.	11.0.0.1109
222959	Intel® FIT cannot decompose a ROM image when the PDR region is enabled within the Intel® FW.	**Affected Component** – SW.Tools.FlashImageTool **Impact:** ROM may not decompile when opened in Intel® FIT. **Workaround:** **Notes:**	11.0.0.1109
222817	GetCurrentClockSettings function call supported by ICC Library fails with unsupported FW error and disables HECI. Any functionality related to this function call will be broken.	**Affected Component** – SW.ICC.SDK **Impact:** Intel® ME may be disabled. **Workaround:** To enable HECI, please re-install Intel® MEI driver, however functionality related to GetCurrentClockSettings call cannot be used. **Notes:** Resolved, to be fixed in future release.	11.0.0.1107
221118	Intel® MEI displays incorrect events in Windows* Event Viewer.	**Affected Component** – SW.HECI Driver **Impact:** Windows* Event Viewer displaying incorrect information. **Workaround:** **Notes:** Reproduction Steps: 1. Disable Intel® MEI Driver. 2. Open Windows* Event Viewer.	11.0.0.1103

Issue #	Description	Affected Component/Impact / Workaround/Notes	Fixed in Kit#
3527890 3527884 3527834	Intel® ME Tools rendered sporadic behavior to unusable within the EFI shell, tools hang majority of the time while others have major delays when running.	**Affected Component** – SW.System.Tools **Impact:** No functionality of the Intel® ME Tools within the EFI shell environment. **Workaround:** **Notes:** Reproduction Steps 1. Boot platform to EFI shell. 2. Run Intel® FPT –I command 3. Tool will hang.	11.0.0.1096 11.0.0.1088 11.0.0.1082
221673	Decomposing an image within the Intel® FIT Tool produces a warning and automatically sets flash components.	**Affected Component** – SW.Tools.FlashImageTool **Impact:** Incorrect warning may display and default component size may change. **Workaround:** **Notes:**	11.0.0.1093
221355 221204	Intel® MEInfo response idle after continuous usage.	**Affected Component** – SW.Tools.Meinfo **Impact:** Intel® MEInfo may not respond. **Workaround:** **Notes:**	11.0.0.1093
221468	Intel® MEInfo displays incomplete results when ran.	**Affected Component** – SW.Tools.Meinfo **Impact:** Intel® MEInfo does not display all information. **Workaround:** **Notes:**	11.0.0.1091
220590	Intel® MEI system file not signed effecting Windows* 7 driver install.	**Affected Component –** SW.HECI Driver **Impact:** Windows* sees driver as unofficial. **Workaround:** **Notes:**	11.0.0.1090
221570	Platform fails to boot to Windows* OS if PG is enabled in Intel® ME FW and have Intel® MEI driver installed.	**Affected Component –** SW.HECI Driver **Impact:** May be unable to boot to Windows*. **Workaround:** **Notes:** Reproduction Steps: 1. Install latest BKC. 2. Install Intel® MEI Driver. 3. Restart system.	11.0.0.1090

Closed Issues



Issue #	Description	Affected Component/Impact / Workaround/Notes	Fixed in Kit#
221597	Blue Screen displayed in Windows* 7 OS when installing Intel® MEI Driver.	**Affected Component –** SW.HECI.Driver **Impact:** Blue screen may display when launching Windows* 7. **Workaround:** **Notes:**	11.0.0.1090
3527887	Intel® FPT Master Access value displays an incorrect value when verified by running Intel® FPT –I.	**Affected Component** – SW.Tools.FlashProgrammingTool **Impact:** Intel® FPT may experience read/write issues when dealing with Intel® FW. **Workaround:** **Notes:**	11.0.0.1088
220778	Intel® FPT hangs when in EFI shell.	**Affected Component** – SW.Tools.FlashProgrammingTool **Impact:** May not be able to dump Intel® binaries. **Workaround:** **Notes:** 1. Reproduction Steps. 2. Load image. 3. Boot to EFI. 4. Dump bin file using FPT –d.	11.0.0.1088
221402	"Stopped Working" error message seen on Intel® Flash Programming Tool when updating FOV variable.	**Affected Component** – SW.Tools.FlashProgrammingTool **Impact:** FOV variable unable to update. **Workaround:** **Notes:**	11.0.0.1086
221484	Intel® MEInfo displays incorrect OEM ID value set from Intel® FIT.	**Affected Component** – SW.Tools.Meinfo **Impact:** Intel® MEInfo does not display all information. **Workaround:** **Notes:** Reproduction Steps: 1. Flash an image with default OEM ID. 2. Boot system and open up command line. 3. Run Intel® MEInfo –feat OEM ID.	11.0.0.1086

Issue #	Description	Affected Component/Impact / Workaround/Notes	Fixed in Kit#
3527883	Changing Intel® FIT Master Access Read/Write access binaries causes platform not to boot.	**Affected Component** – SW.Tools.FlashImageTool **Impact:** Changing Read/Write access within Intel® FIT may cause platform not to boot. **Workaround:** **Notes:**	11.0.0.1084
220727	Intel® MEI driver failure after enable/disable stress testing within the Windows* OS.	**Affected Component** – SW.HECI Driver **Impact:** Intel® MEI yellow bang in Windows* OS **Workaround:** Disable/enable driver for functionality. **Notes:**	11.0.0.1083
3527826	Intel® FIT unable to load its own saved XML file after the tool has been closed and reopened again, causing the FW settings in the XML unable to populate its own values within Intel® FIT.	**Affected Component** – SW.Tools.FlashImageTool **Impact:** XML image unable to load within Intel®FIT. **Workaround:** **Notes:** Reproduction Steps: 1. Open Intel® FIT. 2. Populate Intel® ME, GBE, and BIOS regions. 3. Save file as "Test.xml" 4. Close and reopen Intel® FIT. 5. Open "Test.xml" 6. Error message displays.	11.0.0.1082

7.3 Closed – Documentation

Issue #	Description	Affected Component/Impact / Workaround/Notes	Fixed in Kit#
222441	Intel® FPT functionality is limted on EFI 2.x Shell, full stability requires EFI Toolkit to be in the root directory of Intel® FPT.	**Affected Component** – Documentation.SystemTools UserGuide1.5MB **Impact:** Intel® FPT may not function without Toolkit under EFI Shell. **Workaround:** **Notes:**	11.0.0.1131



Issue #	Description	Affected Component/Impact / Workaround/Notes	Fixed in Kit#
220997	When building a FW within Intel® FIT tool, disabling GbE region causes platform not to boot.	**Affected Component** – SW.Tools.FlashImageTool **Impact:** Platform will not boot with Intel® LAN port disabled. **Workaround:** None **Notes: Fixed** Reproduction Steps: 1. Open Intel® FIT Tool 2. Create/open image. 3. Under flash layout, change "GbE Region Enable" to disable. 4. Build image then flash onto platform.	11.0.0.1086

7.4 Closed – Not a Firmware/Software Bug

Issue #	Description	Affected Component/Impact / Workaround/Notes
221548	When setting ErrAction to ErrorStop within an XML for an Intel® MEManuf EOL CONFIG test, the disabled Intel Recommended EOL Config tests should be displayed, with their names as Skipped Tests. Instead a generic warning about "some" Intel Recommended tests were skipped is displayed.	**Affected Component** – SW.Tools.MeManuf **Impact:** Skipped tests and their names are not displayed. **Workaround:** **Notes:** The issue only occurs when ErrorStop is the ErrAction set in the xml file.

Issue #	Description	Affected Component/Impact / Workaround/Notes
221553	Intel® MEInfo outputs incorrect Intel® ME Reset Reason.	**Affected Component** – FW.OS.Drivers&Service.FWUpdate **Impact:** Intel® MEInfo displaying incorrect info. **Workaround:** **Notes:** This is not a bug as testing was performed on a Consumer platform during warm reset cycling and a global reset does not occur unlike a corporate SKU during G3, will perform a full global reset. Reproduction Steps: 1. Flash image and boot to Windows* 8.1 2. Run MEInfoWin.exe 3. Instead of "Last ME reset reason" to show correct value depending on boot up, Intel® MEInfo displays "Firmware reset " as the "Last ME reset reason".
220738	Adding new ICC Profile in Intel® FIT tool, causes new profile to behave as default selection.	**Affected Component** – SW.Tools.FlashImageTool **Impact:** Unable to switch between profiles. **Workaround:** None. **Notes:** This is not a bug as it is per design.

7.5 Closed – External Dependency

Issue #	Description	Affected Component/Impact / Workaround/Notes
222901 222966 222993	When FDO jumper is set to disable Intel® ME, the Windows* OS may hang during boot up.	**Affected Component** – FW.Bringup.ICC **Impact:** Operating system my not boot. **Workaround:** None **Notes:**

Closed Issues



Issue #	Description	Affected Component/Impact / Workaround/Notes
222555	PMX Driver unable to read certain SPI registers causing tool failure from read/write.	**Affected Component** – ExternalDependency **Impact:** Intel® Software Tools may not run correctly. **Workaround:** **Notes:** This PMX Driver issue relates with various Intel® Software Tools that may not run correctly such as Intel® FPT, MEInfo and, MeManuf due to this PMX Driver problem.
3527998	Intel® MeInfo has sporadic behavior when ran.	**Affected Component** – SW.Tools.FlashImageTool **Impact:** Intel® MeInfo may not run. **Workaround:** **Notes:** Issue caused by Integrated Sensor Hub (ISH) enabled boards.
222826	Serial Over Lan (SOL) redirection does not output video within putty window for remote capability.	**Affected Component** – FW.AMT.Redirection **Impact:** Remote functionality for Desktop/BIOS is limited. **Workaround:** None. **Notes:** Hardware issue found as limiting factor for SOL.
221495	Frequent connectivity loss when CCA is connected to board via USB.	**Affected Component** – FW.NPK **Impact:** May be unable to retrieve Intel® ME FW messages. **Workaround:** None **Notes:** CCA driver update may be needed for full functionality.

8 Known Issues

8.1 Open – Intel® ME Kernel

Issue #	Description	Affected Component/Impact / Workaround/Notes
225421	Intel® MEInfo –fwsts shows a mismatch on FW Status 6 only when Intel® ME is disabled via FW or Service Mode jumper.	**Affected Component** – FW.Bringup.BootGuard **Impact:** Incorrect Power Management flows may occur. **Workaround:** **Notes:**
225315	Decomposing an image within Intel® FIT that had prior Intel® ICC changes, throws errors during the decomposition.	**Affected Component** – FW.Bringup.BootGuard **Impact:** Intel® FIT may not open images with Intel® ICC changes. **Workaround:** **Notes:** 1. Change Intel® ICC settings via Intel® FIT. 2. Create image. 3. Decompose back into Intel® FIT.
225242	Disabling Intel® PTT via Intel® FPT by inputting the correct bit followed by a warm reset, still shows that Intel® PTT is enabled and fuctions as normal.	**Affected Component** – FW.PTT.Main **Impact:** Cannot disable Intel® PTT **Workaround:** **Notes:** 1. Flash image with Intel® PTT enabled. 2. Verifiy Intel® PTT functionality through Windows* OS, "TPM.MSC" 3. Run Intel® MEInfo –verbose to verify value. 4. Run Intel® FPT –r –FeatureShipState, take the value, and set it to 0. 5. Run Intel® FPT –u –n FeatureShipState –v "Value from Step 4". 6. Run Intel® FPT –commit, platform will reboot. 7. Check to see if Intel® PTT disabled via Intel® MEInfo.



Issue #	Description	Affected Component/Impact / Workaround/Notes
223494	When Intel® TXT and Intel® ME are enabled, a promotion of warm reset (expected) to global reset (unexpected) causes the system to continuously reset.	**Affected Component** – FW.Bringup.BootGuard **Impact:** System enters an endless reset loop. Intel® TXT testing is blocked. **Workaround:** Intel® ME Kit 11.0.0.1136 has a fix for this issue on systems using Boot Guard Profile 0. **Notes:**

8.2 Open – Intel® Software Tools

Issue #	Description	Affected Component/Impact / Workaround/Notes
225464	Running Intel® FPT –closemnf states ME Manufacturing Mode bit was successful, but fails to perform a global reset.	**Affected Component** – SW.Tools.FlashProgrammingTool **Impact:** Improper Close Manufacture flow. **Workaround:** None **Notes:**
225496	Running Intel® FWUpLcl sporadically gets stuck during update process, a restart indicates update has succeeded via Intel® MEInfo.	**Affected Component** – SW.OS.Driver&Service.FWUpdate **Impact:** Intel® FWUpdLcl may get stuck during update. **Workaround:** None **Notes:**
222915	Intel® FWUpdate tool has a mismatch of general errors between basic tool commands.	**Affected Component** – SW.Tools.FwUpdLcl **Impact:** Error/warnings may not match the specific type of command. **Workaround:** None **Notes:**

Issue #	Description	Affected Component/Impact / Workaround/Notes
223310	Intel® FIT Power Plane parameters can always be modified regardless of the VR value.	**Affected Component** – SW.Tools.FlashImageTool **Impact:** Each EdramVrType value set within the parameter does not lock. **Workaround:** None **Notes:** 1. Start FIT GUI. 2. Go to CPU Straps feature tab. 3. For each "EdramVrType" parameter possible values (0x0 and 0x1) 4. Set EdramVrType to the possible value. 5. Change EdramPowerPlaneTopology to a new value. 6. Value is always changeable when it should be unmodified.

§ §