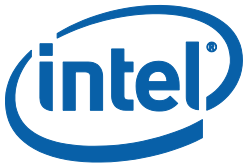

Intel® Converged Security Engine(Intel® CSE) Firmware 13.0 Release Ice Lake Platform

Slim Release Notes - NDA

March 2020

Revision 13.0.33.1481
[Engineering Release]

UN/YN Series

Intel Confidential

Please **read** Important Notes within these Release Notes before Flashing a new image

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.

Intel® Active Management Technology requires activation and a system with a corporate network connection, an Intel® AMT-enabled chipset, network hardware and software. For notebooks, Intel AMT may be unavailable or limited over a host OS-based VPN, when connecting wirelessly, on battery power, sleeping, hibernating or powered off. Results dependent upon hardware, setup and configuration. For more information, visit Intel® Active Management Technology.

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.

Intel® vPro™ Technology is sophisticated and requires setup and activation. Availability of features and results will depend upon the setup and configuration of your hardware, software and IT environment. To learn more visit: http://www.intel.com/technology/vpro.

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.

Contents

Revision History

Revision Number	Description	Revision Date
13.0.0.7021	First release Pre-Si	Jun 2016
13.0.0.7029	Second release Pre-Si	August 2017
13.0.0.7033	Third release Pre-Si	September 2017
13.0.0.7040	Forth release Pre-Si	October 2017
13.0.0.7046	Si release	November 2017
13.0.0.7049	Second Si release	December 2017
13.0.0.7053	Third Si release	January 2018
13.0.0.7057	Forth Si release	January 2018
13.0.0.1002	Pre-Alphe release	February 2018
13.0.0.1003	Engineering release	March 2018
13.0.0.1007	Engineering release	April 2018
13.0.0.1011	Engineering release	April 2018
13.0.0.1016	Engineering release	June 2018
13.0.0.1021	Engineering release	June 2018
13.0.0.1026	Engineering release	July 2018
13.0.0.1027	Engineering release	July 2018
13.0.0.1030	Engineering release	August 2018
13.0.0.1033	Engineering release	September 2018
13.0.0.1034	Engineering release	September 2018
13.0.0.1034	Engineering release for UN / YN Series	October 2018
13.0.0.1037	Engineering release for U / Y Series	October 2018
13.0.0.1040	Engineering release for U / Y and UN / YN Series	November 2018
13.0.0.1040	Engineering release for U / Y and UN / Alpha Release YN	November 2018
13.0.0.1042	Engineering release for U / Y and UN / YN	November 2018
13.0.0.1044	Engineering release for U / Y / YN Alpha BKC UN	December 2018
13.0.0.1046	Engineering release for UN / YN	January 2019
13.0.0.1049	Engineering release for U / Y and UN / YN	January 2019
13.0.0.1051	Engineering release for UN / YN	January 2019
13.0.0.1054	Engineering release for UN / YN	February 2019
13.0.0.1054	Beta release for UN / YN	February 2019

Revision Number	Description	Revision Date
13.0.0.1057	Engineering release for UN / YN	February 2019
13.0.0.1061	Engineering release for UN / YN	March 2019
13.0.0.1066	Engineering release for U / Y and UN / YN	April 2019
13.0.0.1080	Engineering release for U / Y and UN / YN	May 2019
13.0.0.1082	Engineering release for UN / YN	May 2019
13.0.0.1084	Engineering release for UN / YN	June 2019
13.0.0.1085	Engineering release for UN / YN	July 2019
13.0.0.1086	Engineering release for UN / YN	July 2019
13.0.20.1304	Engineering release for UN / YN	August 2019
13.0.20.1308	Engineering release for UN / YN	September 2019
13.0.20.1310	Engineering release for UN / YN	September 2019
13.0.20.1313	Production Cadidate release for UN / YN	October 2019
13.0.21.1314	Engineering release for UN / YN	October 2019
13.0.21.1314	Production Candidate release for UN / YN	November 2019
13.0.21.1319	Engineering release for UN / YN	December 2019
13.0.21.1319	Engineering Update release for UN/YN	January 2020
13.0.21.1319	Engineering Update 2 release for UN/YN	January 2020
13.0.30.1435	Engineering BKC release for UN/YN	January 2020
13.0.30.1435	Engineering release for UN/YN	January 2020
13.0.31.1465	Engineering release for UN/YN	February 2020
13.0.32.1478	Engineering release for UN/YN	February 2020
13.0.32.1481	Engineering release for UN/YN	March 2020

§

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
CCM	Client Control Mode (See: HPC)
CIM	Common Information Model
FW	Firmware
GbE	Gigabit Ethernet
HBC	Host Based Configuration
HECI	Host Embedded Controller Interface. Same as Intel® MEI.
CRB	Intel® Customer Reference Board
Intel® DAL	Intel® Dynamic Application Loader (Intel® DAL)
Intel® FIT	Intel® Flash Image Tool
Intel® ICCS	Intel® Integrated Clock Controller Service
Intel® MSS	Intel® Management and Security Status
Intel® MEI	Intel® Management Engine Interface (interface between the Management Engine and the Host system)
Intel® PETS	Intel® Platform Enablement Test Suite
Intel® PTT	Intel® Platform Trust Technology
ISV	Independent Software Vendor
IUP	Independently Updatable Partitions
LAN	Local Area Network
MAC	Media Access Control
MOF	Managed Object Format
MRC	Memory Reference Code
OS	Operating System
PCH	Platform Control Hub
Pmc	power management controller
SPI	Serial Peripheral Interface

Term	Description
SUT	System Under Test
SVN	Security Version Number. Used in Firmware Upgrade / Downgrade capabilities
VCN	Version Control Number. Used in Firmware Upgrade / Downgrade capabilities
WSI	Web Services Interoperability Organization

2 Release Kit Summary

This document covers the following Intel® Converged Security Engine SKUs for the Ice Lake U/Y, UN / YN Series platform:

- Slim

2.1 Release Kit Details

Firmware Support	PAVP, Intel® ICCS, Intel® Platform Protection Technology with Boot Guard, Intel® SVT
Kit Release	Build Number – 13.0.33.1481
Target Platform	Ice Lake U/Y, UN/YN Platforms

2.2 Kit Overview

The kit can be downloaded from Intel® 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:
   - 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.
   - 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 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.
MEI-Only Installer MSI	• The MEI-Only Installer only installs the Intel® MEI driver.
Intel® MEI Driver	• Intel® MEI is the interface between the host and the Intel® Converged Security 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.
iCLS Service	• iCLS Client is a set of applications, services and dynamic libraries used to establish a trusted connection between FW and Intel's backend.
JHI Service	• Capable of loading and executing code (DAL Application) in a build-in isolated VM environment. • This driver is capable of utilizing Intel® CSME capabilities.
LMS Service	• Provides local apps with a network interface to Intel® AMT • Provide CSME version info on non Intel® AMT platforms
Intel OEM Extention	• Used for inf based installation for Intel® DAL driver

2.3.2 Image Components

Image	Description
Intel® CSE	• The Intel® Converged Security Engine and configuration data for Intel® Converged Security 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 **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.
Pre-Stiched Firmware Update binaries	• The kit release also contains two pre-stitched firmware updated binaries located in the Prestiched folder under Image Components folder. • Base_PreStitched.bin - Contains the following binaries Intel® CSE, PMC, PCHC, IOM and PHY • Full_PreStitched.bin - Contains the following binaries Intel® CSE, PMC, PCHC, IOM, PHY and TBT
PMC	• The pmc firmware contains code for power management controller functions. • This is one of the regions that is integrated into the final flash image that is built using the Intel® FIT tool, and is then programmed into the SPI flash. **NOTES:** For more details on the pmc related issues, please refer to **pmc changes** section of this document.

Image	Description
TCSS	• IOM • MG PHY • Re-Timer • TBT **Notes:** For more details please refer to the TCSS FW Release Notes

2.3.3 System Tools

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® Converged Security Engine firmware, Gigabit Ethernet (GbE) into a single binary image. • Provided as a GUI tool. • **OS Support:** - See Tools PRD.
Intel® Flash Programming Tool	• Used to write the flash image into the SPI flash device. • DOS, EFI and Windows* command line tools provided. • **OS Support:** - See Tools PRD.
Reduced Sized FWUpdate	• Found under: tools\system_tools\FWUpdate_RS • Refer to the system tools for more information
FWUpdate	• Used to update the Intel® Converged Security and Management's firmware. • DOS, EFI and Windows* command line tools provided. • Reduced Sized FWUpdate API Library is available under Tools/System_Tools/FWUpdate_RS • **OS Support:** - Refer to ICL PRD.

Tool	Description
MEInfo	• Verifies that Intel® Converged Security Engine (Intel® CSE) firmware is alive and returns data about Intel® CSE. • DOS, EFI and Windows* command line tools provided. • **OS Support:** - See Tools PRD.
MEManuf	• Used on the manufacturing line to validate platform is configured properly. • DOS, EFI and Windows* command line tools provided. • **OS Support:** - See Tools PRD.
Intel® MEU	• Signing and Manifesting tool • For usage instructions refer to the **Signing and Manifesting Guide** included in the downloaded kit.

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. • DOS, EFI and Windows* command line tools provided. • **OS Support:** - See Tools PRD.
Intel ICC SDK	• Libray of APIs used to configure target clocks parameters e.g frequency, boot settings, etc. • Please see ICC Tools User Guide for more information included in kit for usage and structure

2.4 Release Version Numbering Information

Typical release version numbering is as follows,

13.0.y.z (for example: 13.0.0.zzzz) where:

'13' refers to the Intel® Converged Security Engine 13.0 Firmware SKU for Ice Lake U/Y Series Platform.

'0' represents the associated platform program.

[0-9] – Client platform programs
[10-19] - *Falls Worstations and HEDT
[20-29] - *leys Workstations
[30-99] – Reserved for future program needs

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

'z' refers to firmware release revision.

2.5 Firmware Update Information

Intel® Converged Security Engine 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

ARB SVN (Anti-Rollback Security Version Number) is used to prevent downgrade the current firmware to a firmware with a lower ARB SVN number.

If Hardware ARB SVN committed (FPF fuses burned), systems will not be able to downgrade to a firmware with a lower ARB SVN number even when physical access to the platform is possible.

TCB SVN (Trust Computing Base Security Version Number): The Intel® CSE generates multiple keys that are part of the TCB of Intel® CSME. When critical vulnerabilities are found that compromise the TCB the TCB SVN is subsequently increased and "TCB Recovery" is triggered.

The TCB Recovery revokes the compromised credentials and replaces them with new ones.

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® CSME 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: 12.0.0.zzzz PV cannot upgrade to 13.0.0.zzzz Alpha

- 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® CSE FW Version	ARB SVN #	TCB SVN #	VCN #	PV (1 or 0)
13.0.0.7021 (S/H/U/Y)	1	1	0	0
13.0.0.7029 (S/H/U/Y)	1	1	0	0
13.0.0.7033 (S/H/U/Y)	1	1	0	0
13.0.0.7040 (S/H/U/Y)	1	1	0	0
13.0.0.7046 (S/H/U/Y)	1	1	0	0
13.0.0.7049 (S/H/U/Y)	1	1	0	0
13.0.0.7053 (S/H/U/Y)	1	1	0	0
13.0.0.7057 (S/H/U/Y)	1	1	0	0
13.0.0.1002 (S/H/U/Y)	1	1	0	0
13.0.0.1003 (S/H/U/Y)	1	1	0	0
13.0.0.1007 (S/H/U/Y)	1	1	0	0
13.0.0.1011 (S/H/U/Y)	1	1	0	0
13.0.0.1016 (S/H/U/Y)	1	1	0	0
13.0.0.1021 (S/H/U/Y)	1	1	0	0
13.0.0.1026 (S/H/U/Y)	1	1	0	0
13.0.0.1027 (S/H/U/Y)	1	1	0	0
13.0.0.1033 (S/H/U/Y)	1	1	0	0
13.0.0.1034 (S/H/U/Y)	1	1	0	0
13.0.0.1037 (S/H/U/Y)	1	1	0	0
13.0.0.1040 (U/Y/UN/YN)	1	1	0	0
13.0.0.1042 (U/Y/UN/YN)	1	1	0	0
13.0.0.1044 (U/Y/UN/YN)	1	1	0	0
13.0.0.1049 (U/Y/UN/YN)	1	1	0	0
13.0.0.1051 (UN/YN)	1	1	0	0
13.0.0.1054 (UN/YN)	1	1	0	0
13.0.0.1057 (UN/YN)	1	1	0	0
13.0.0.1061 (UN/YN)	1	1	0	0

Intel® CSE FW Version	ARB SVN #	TCB SVN #	VCN #	PV (1 or 0)
13.0.0.1066 (U/Y/UN/YN)	1	1	1	0
13.0.0.1080 (U/Y/UN/YN)	1	1	1	0
13.0.0.1082 (UN/YN)	1	1	1	1
13.0.0.1084 (UN/YN)	1	1	1	1
13.0.0.1085 (UN/YN)	1	1	1	1
13.0.0.1086 (UN/YN)	1	1	1	1
13.0.20.1304 (UN/YN)	2	1	1	1
13.0.20.1308 (UN/YN)	2	1	1	1
13.0.20.1310 (UN/YN)	2	1	1	1
13.0.20.1313 (UN/YN)	2	1	1	1
13.0.21.1314 (UN/YN)	2	1	1	1
13.0.21.1314 (PC UN/YN)	2	1	1	1
13.0.21.1319 (PC UN/YN)	2	1	1	1
13.0.30.1435 (UN/YN)	2	1	1	1
13.0.31.1465 (UN/YN)	2	1	1	1
13.0.32.1478 (UN/YN)	2	1	1	1
13.0.33.1481 (UN/YN)	2	1	1	1

3 General Information

3.1 Important Notes

- This kit includes bug fixes. A new section is added to this kit for Security issues, refer to Chapter 8 for more details.

3.2 Hardware Configurations

This release supports the following HW configurations:

- ICL UN (ES)
- ICL UN (QS)
- ICL YN (ES)
- ICL YN (QS)

3.3 Best Known Configuration

For the latest Client Based Ice Lake U/Y Series Platforms Best Known Configuration (BKC), please contact your platform CE.

4 Kit Details

4.1 Build Details

Kit	Build Details	Changes since previous release
Firmware Version	13.0.33.1481	Yes
Intel® FIT Version	13.0.33.1481	Yes
PMC Version	V27 UN/YN B-Step	Yes
PCHC Version	V1004	No
IOM Version	04.00E.0.00 D-Step	No
NPHY Version	9.0.1.6 B-Step / D-Step	No
TBT Version	Rev 79 D-Step	No
Re-timer Firmware	Fab1 : Rev35_ace2a0-000.031.0.6	No
	Fab2 : Rev37_ ace2b2-2.40.0.11	No
Intel® CSE SW Installer Version	1944.14.0.1370	No
Intel® MEI Driver Version	1944.14.0.1370	No
Intel® OEM Extension	1914.13.0.1063	No
Intel® iCLS service	1.56.87.0	No
Tools	13.0.33.1481	Yes

4.2 Intel® FIT XML Changes

4.2.1 Intel® FIT XML change log

Changes	Firmware Version
Number of Flash Components changed to allow '0' as a setting to allow the Intel® FIT tool to build just the integrated Intel®ME region. BCLK SSC Maximum Percentage value changed to 0.50. SLP_WLAN Power Well settings changed. Help text correction for Intel(R) SMBus Subsystem Vendor and Device ID for ASF setting. Intel(R) RST for PCIe-C2 Select x2 or x4 default changed to x2. PCIe Controller 3 (Port 9-12) default changed to 2x2. PCIe Controller 3 (Port 13-16) default changed to 2x2. Thunderbolt Enable changed to "Yes". xDCI Split Die Enabled setting added. Intel(R) HD Audio Voltage Select default voltage changed to 1.8v.	13.0.0.7053
Legacy Skylake Host CPU / BIOS Read Access Intel Recommended permissions removed. PortF added to HDCP Internal Display Port 1 - 5K and HDCP Internal Display Port 2 - 5K Added GPP_D & GPP_H GPIOs to SRC0-SRC5 CLKREQ# Mapping DCI BSSB over USB3 Port2 Enabled changed to "No" PCIe Controller 4 (Port 13-16) changed to 4x1 as default.	13.0.0.7057
Changed FPF Hardware Binding setting to HW Binding. Addition note added to help text for CLKOUT_SRC settings. Help text updated for PCIe Power Stable Timer (tPCH33) setting. PCIe Controller 3 changed to 1x4.	13.0.0.1002
Removed Anti Rollback settings for OEM Key Manifest, Android OS, IUnit, aDSP and PMC.	13.0.0.1003
Fast Read Clock Frequency default changed to 30MHz Quad I/O and Quad Read defaults changed to Yes Moved IO Manageability Engine Manifest Anti-Rollback Enabled MG PHY Manifest Anti-Rollback Enabled	13.0.0.1007

Thunerbolt(TM) Manifest Anti-Rollback Enabled Under Type-C Firmware Anti-Rollback Configuration section. Corrected missing eSPI / EC Low Frequency Debug Override New FW Update Image Build tab and settings added.	
OEM Binary help text updated. Inte(R) ME Binary File help text updated. Chipset Initialization Binary help text updated. SPI Software Binding Enabled changed to Software Re-Binding Enabled. Second OEM Public Key Hash help text added. Oem Key Revocation Enable help text updated. BCLK Clock Frequency help text updated. BCLK Spread setting help text updated. BCLK SSC Changes Allowed removed. BCLK SSC Maximum Percentage default changed. Intel(R) SMBus ASD Address Enabled help text updated. SMLink1 I2C Target Address Enabled help text updated. eSPI / EC Bus Frequency help text added. eSPI / EC Maximum I/O Mode help text added.	13.0.0.1011
BIOS Region Enable default changed Number of Flash Components default changed Flash Component 1 Size default changed Help text updated for Host CPU Read / Write Access, ME Read / Write Access, GbE Read / Write Access and EC Read / Write Access. Fast Read Clock Frequency default changed Quad I/O Read and Quad Read Enable defaults changed Port F added to HDCP Internal Display Port 1 & 2 5k. Enable Drop Ship Capabillities setting added.	13.0.0.1016
BIOS Enable option removed Top Swap Block Size default changed to 128KB Embedded Host Based Configuration Enabled help text updated. Exclusion Ranges and Desciptor Configuration setting added. Platform Drop Ship Capabilites Support setting removed. ClkoutLPC0 and ClkoutLPC1 settings removed. Help text updated for SMBus and SMLink settings.	13.0.0.1021

Defaults for DCI BSSB over USB3 Port2 Enabled and DCI BSSB over USB3 Port4 Enabled changed. DCI BSSB over GPIO Enabled removed. Type-C SubSystem Authentication Enabled removed.	
Permissions updated to include extended regions. Second OEM Public Key Hash added. BCLK SSC Maximum Percentage value changed to 0.50 Discrete vPro NIC setting added. SMLink0b MCTP settings added. SMLink0 designation changed to SMLink0b	13.0.0.1026
Custom Permissions updated to include extended regions. Intel® Services Configuration options removed. PCIe High and Low Byte profile type entries removed form ICC.	13.0.0.1027
THERMAL_MGMT_DIS_Diff added.	13.0.0.1030
No Change	13.0.0.1033
APWROK Check Enabled setting removed SMLink0b settings reverted back to SMLink0 PCHC Image entries added to FW Update Image Build tab	13.0.0.1034
Type-C default speed capability changed from Gen2 to Gen1.	13.0.0.1037
FIVR changes	13.0.0.1040
Quad I/O and Quad Output Read defaults changed to 'Yes' MG PHY Binary changed to PHY Binary	13.0.0.1042
Wording changed from Descrete vPro NIC to Platform vPro NIC	13.0.0.1044
Intel FPF AntiRollback configuration settings added. Additional help text added to Descrete vPro NIC settings.	13.0.0.1046
Removed IFWI Layout setting PMC_Strap Diff entries added	13.0.0.1049
Platform IMON encoding changed VCCIO_FIVR_Disable_Diff	13.0.0.1051
No Change	13.0.0.1054
Platform IMON setting FIT designation updated and setting options changed from Yes/No to Enabled/Disabled. PD Controller Ports 1 and 2 USB2 Port and Type-C SMBus Address values changed.	13.0.0.1057
No Change	13.0.0.1061

Enable option removed from PCH Configuration under the FW Update Image Build tab.	13.0.0.1066
No Change	13.0.0.1080
No Change	13.0.0.1082
PCH_Strap_GPCOM4_gpio_sstrap_vccio_com4_spare1_Diff PCH_Strap_GPCOM4_gpio_sstrap_vccio_com4_spare0_Diff	13.0.0.1084
No Change	13.0.0.1085
No Change	13.0.0.1086
No Change	13.0.20.1304
No Change	13.0.20.1308
No Change	13.0.20.1310
No Change	13.0.20.1313
No Change	13.0.20.1314
BCLK Clock Configuration section added	13.0.20.1319
No Change	13.0.30.1435
No Change	13.0.31.1465
No Change	13.0.32.1478
No Change	13.0.33.1481

4.2.2 Intel® FIT XML Compare / Delta from previous release

Intel® CSME 13.32.0.1478 Release	Intel® CSME 13.0.33.1481 Release

4.3 PMC Changes

PMC FW –Release Version Numbering Information

- PMC FW is PCH SKU (H vs. LP) dependent.
- Below detail provides release version numbering information of PMC FW binary supported for Ice Lake platform. For each release, it will follow version number as 400.x.yy.zzzz to indicate PMC FW's compatibility with PCH sku as well as PCH stepping , where:
- '400' refers to the Intel® Manageability Engine compatible version for Ice Lake Lake U/Y Series Platform.
- 'x' refers to the Intel® PCH Type Sku PMC FW is supported for
  - 1 = PCH Type LP
  - 2 = PCH Type H
- 'yy' refers to the Compatibility/Maintenance build. This field indicates when PMC FW is updated to comply with new requirements; i.e. HW support or features.
  - 01 = Initial branch support
  - 11 = Maintenance branch and new stepping support
- 'zzzz' refers to the PMC FW release revision. This field indicates PMC FW's compatibility with PCH stepping.

4.3.1 PMC Important Notes

4.3.2 pmc change log

pmc version	Changes	Firmware Version	Stepping Supported
0x0C	N/A	13.0.0.1007	LP A-Step
0x0C	N/A	13.0.0.1011	LP A-Step
0x0E	FW doesn't program SBU pins nad FWD to IOM if it receives a connect message in Sx. Sx stretch timings are honored when DIS_SLP_X_STRCH_SUS_UP is set. Fixed deep Sx Abort flow. Fixed FWD debug override for Type-C connection handling in PCH USB-C* Mux Agent. Updated Workaround for PMC/SPI SB message Storage reset domain.	13.0.0.1016	LP A-Step
V16	Prevent over current in s0ix. Fixed VccST needs to be configured as Max for G3/Sx flows.	13.0.0.1016	LP A-Step

pmc version	Changes	Firmware Version	Stepping Supported
V07	Fixed FW not properly clearing GBLRST_STS on DeepSx entry. Fixed PCH timeout after 15-30 min of S0i3. Fixed System hanging while doing warm reset waiting for TCSS response.	13.0.0.1016	LP B-Step
V03	Prevent overcurrent in S0ix. Fixed Pre-Si environment not booting to BIOS & OS with PMC v0C.	13.0.0.1016	N A-Step
V16	No change	13.0.0.1021	LP A-Step
V08	CrashLog improvements to avoid timeouts in Sx cycling.	13.0.0.1021	LP B-Step
V04	Orientation information doesn't get passed correctly between IOM and PMC. Firmware programs and forwards correct connect message for Sx entry and exit.	13.0.0.1021	N A-Step
V16	No change	13.0.0.1026	LP A-Step
V11	Prevent overcurrent in S0ix Enabling Thermal Management feature in straps causes boot failure PCH PM down timeout with S0ix when C10 is enabled	13.0.0.1026	LP B-Step
V06	PMC FW updating modphy SUS overrides incorrectly during cold reset entry Fix for PMC XTAL clock vs. clock source shutdown in Sx/cold reset FW sending update to IOM for USB-C* instead of usb2 SMS controller not responding with ACK after SMSwrite FW not configuring GPIO pins correctly for PD I2C clock	13.0.0.1026	N A-Step
V16	No change	13.0.0.1027	LP A-Step
V12	Prevent overcurrent in S0ix	13.0.0.1027	LP B-Step
VE9	PMC to check for PD controller readiness in USB-C* SMLink	13.0.0.1027	N A-Step
V13	PMC to clear USB2PHY wake on back 2 back warm reset. PMC programs USB2 port for debug	13.0.0.1030	LP B-Step
V9	No Change	13.0.0.1030	N A-Step

pmc version	Changes	Firmware Version	Stepping Supported
V16	No change	13.0.0.1033	LP A-Step
V13	No Change	13.0.0.1033	LP B-Step
V11	Remove clock request de-assertion in warm reset	13.0.0.1033	N A-Step
V15	Some Clocks were stopping after warm reset leading to display blanking. Avoid triggering global reset while running S0ix cycling for a long time (~4 hours) with audio traffic in between cycles. Voltage Regulation (FIVR) ramp rates are determined by fuses but was overridden by FW in certain cases. FW is programming a usb2 port reserved in soft strap for DBC if early debug not enabled.	13.0.0.1034	LP B-Step
V13	Some Clocks were stopping after warm reset leading to display blanking.	13.0.0.1034	N A-Step
V15	No Change	13.0.0.1037	LP B-Step
V14	Patch with Energy Reporting Enabled 1. Energy reporting feature 2. DbC3 Enumerates devices on USB Type-C **Note:** There are two versions of the PMC binary on with Crashlog and one without.	13.0.0.1037	N A-Step
V16	Fine-tuning of Overcurrent protection and Maximum current in Dynamic management of Fully Integrated Voltage Regulation block (FIVR)	13.0.0.1040	LP B-Step
V16	Patch with Crashlog enabled 1. CrashLog record changes. Patch with Energy Reporting enabled 1. TBT (Thunderbolt)USB-C* 2 port concurrent enumeration works without undergoing loss of enumeration of either ports and subsequent attempts to Re-Enumerate. 2. SUT (System Under Test) always wakes from S3 using LID/Keyboard/Power button without having to attempt reconnection while unplugging USB 2 devices and plugging back to same port.	13.0.0.1040	N A-Step
V16	No Change	13.0.0.1042	LP B-Step
V16	No Change	13.0.0.1042	N A-Step
V18	1. ChipSet Init Updates support new format 2. SUT always wake from S3 using LID/Keyboard/Power button	13.0.0.1044	LP B-Step

pmc version	Changes	Firmware Version	Stepping Supported
	3. HDMI HPD Signal behavior and interrupt in Interconnect FW follows Spec defined by USB-C* Standard when both values are clubbed in single message		
V17	PCI Express Clock Management / Request works correctly for BIOS	13.0.0.1044	N A-Step
V18	Energy Reporting and Crashlogs enabled together. USB-C* Subsystem conforms to VESA DP Alt Mode on USB Type-C Standard in that a single message could capture both a device connect Interrupt as well as device connect logic levels in a single message.	13.0.0.1046	N A-Step
V21	When BIOS enables NorthPeak system trace, PMC FW releases the WAKE status after waiting for Power OK status from North Peak , ensuring it is out of power gated status always. When transit from Mechanical Power Off to S5 , SUS_PWRDN_ACK goes High System does not Wake from Sx when TBT device is disconnected during Sx and that port is configured for wake.	13.0.0.1049	LP B-Step
V19	USB-C* display works after DP Alt Mode display is not coming after S4, S5, Warm Reset. Energy reporting and crashlogs both enabled.	13.0.0.1049	N A-Step
V20	System does not wake from Sx when unplugging Thunderbolt device PMC GCR space registers pertaining to CPU and Voltage regulation & management secured. PMC Trace message XML file includes reset type information in TRACE_HOST_RESET_ENTRY message The Voltage regulator input rail VccinAux when enabled in Sx states behaves according to spec with no hangs	13.0.0.1051	N A-Step
V20	No Change	13.0.0.1054	N A-Step
V21	No Change	13.0.0.1054	N A-Step
V21	No Change	13.0.0.1057	N A-Step
V4	Successful booting after reset while on Connected Standby CPU Thermtrip does not occur when running warm reset cycle	13.0.0.1057	N B-Step
V21	No Change	13.0.0.1061	N A-Step
V6	Updated Dynamic Voltage regulation table with updated Max current thresholds for SPI Audio agents such as Cortana App wakes up from connected standby state	13.0.0.1061	N B-Step

pmc version	Changes	Firmware Version	Stepping Supported
	Powergating of SPI enabled in Sx states		
V31	PMC mailbox command for BIOS-PMC interaction to read PMU registers have included checks for valid address ranges in the interprocessor Communication (IPC1) command IE dock always successfully detected when hot plug dock and plug full device.	13.0.0.1066	LP D-Step
V8	VCCST de-asserted during cold reset to enable USB –C* to function correctly.	13.0.0.1066	N B-Step
V10	Energy reporting Table updates to PMC synchronization has been optimized and made faster.	13.0.0.1080	N B-Step
V10	No Change	13.0.0.1082	N B-Step
V11	When charger is present during boot, it get correctly enumerated and subscribed to port so as to follow correct behavior of subscription policy for facilitating Sx and S0ix states Exiting debug mode and so Voltage regulation parameters will not be overridden by soft straps Thunderbolt Alternate mode transitions are achieved after first going to Safe mode and then transitioning to Alternate mode	13.0.0.1082	N B-Step
V11	No Change	13.0.0.1084	N B-Step
V12	System never hangs in CS mode as Power Good status bits are updated and saved as soon as Fuses are pulled in the system and before the interrupt for fuse pull is cleared. This sequence is after boot and Voltage Auxiliary mode settings are set appropriately After Global reset LAN dongle connections are detected successfully System restarts successfully on connecting a USB USB-C** charger while system is in shutdown. USB-C** to VGA+USB-C* to HDMI monitor connects reliably after resume from S4.	13.0.0.1085	N B-Step
V14	PMC sends System power State information to Retimer while entering Sx and exiting it as well. While system is Sx and there is a USB connection at that time, Retimer needs to know system states in in order to execute USB Compliance mode entry and to perform USB compliance mode exit upon exiting Sx and entering S0.	13.0.0.1086	N B-Step
V16	Soft hang during S3 cycling	13.0.20.1304	N B-Step
V16	No Change	13.0.20.1308	N B-Step
V17	Unexpected power trip seen during S0ix cycling. System would hang when USB-C** 4k monitor was connected. System May Hang with USB-C** Power Adapter	13.0.20.1310	N B-Step
V18	BIOS capsule update succeeds always – A case of global reset caused hangs after capsule update	13.0.20.1313	N B-Step

pmc version	Changes	Firmware Version	Stepping Supported
	;but this is fixed in this patch with correction of boot type variable to reflect proper boot sequence (Global reset after capsule update). This patch handles error cases of messages received from eSPI that exceed the configured size The eSPI controller is notified of the error as well.		
V18	No Change	13.0.20.1314	N B-Step
V19	Crashlog improvements relating to eSPI and Punit data.	13.0.20.1314	N B-Step
V20	Update to deassert interrupt during S0i2	13.0.20.1314	N B-Step
V21	Resolved system stuck entering S0i while package is in C10.	13.0.20.1319	N B-Step
V22	Fixed the issue of Crashlog record extends beyond the end of the allocated region in PMC SSRAM.	13.0.20.1319	N B-Step
V23	Resolved global reset when system is sitting idle	13.0.20.1319	N B-Step
V23	No Change	13.0.30.1435	N B-Step
V24	Global reset detected and thermaltrip eSPI GPIO strength adjustment soft strap updated	13.0.30.1435	N B-Step
V24	No Change	13.0.31.1465	N B-Step
V25	Fixed the issue of idle hang after boot to OS	13.0.32.1478	N B-Step
V27	Resolved global reset detected and thermaltrip Resolved delay when exiting C10+S0i Resolved inability to enter run-time S0i after unplugging power adapter Resolved numerous Bluetooth module resets seen during regular usage Resolved power increase in movie playback	13.0.33.1481	N B-Step

5 Intel® ME New Features - RCR's

RCR #	Change Info	Implemented in Kit #

6 Issue Status Definitions

This document provides sightings and bugs report for Intel® ME Firmware 13.0 SKU for the Ice Lake U/Y/S/H Series Platform. 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).

Closed Issues: This category will only display closed issues within the current Intel® ME Kit release. After each release, old issues will be dropped down to the "Archive" section and then new closed issues will take its place back up top for the next release. If an issue is posted in this section, it will indicate that the issue has been verified and fixed within the kit that is being released.

Known Issues: This category will display all Known Issues since the Alpha release and will remain in this section until fixed or noted otherwise. "Known Issues" are still under investigation and may or may not be root caused.

Archive – Fixes in Previous Kits: This category will display all closed issues that were closed in their respected kit#. This section will serve as a history of fixed issues.

Sightings listed in this document apply to the Ice Lake UN/YN SKU's unless noted otherwise in this document or in the sightings tracking systems.

7 FWUpdate Library deltas

7.1 Introduction

This section addresses changes caused by Closed Issues and RCRs implementations that impacts FWUpdate library.

7.2 Change Log

Issue/RCR#	Description
N/A	FWUpdate_RS directory Changes : • Under the FWUpdate_RS directory; the FWUpdLclAppDeprecated.c file was added, which includes all the deprecated functions built up into a sample code source file (.c). • The FWUpdLclApp.c contains sample code with the new FWUpdate functions.
N/A	Refer to System Tools User Guide for the latest changes in FWUpdate Kit.

8 Closed Issues – 13.0.33.1481

Issue #	Description	Details	Found in Kit # Affected SKU's

8.1 Mitigated Security Vulnerabilities

This section describes security issue mitigations in Intel® CSME in this Intel Platform Update Release (IPU).

QSR	Technical Advisory (TA)	Document Number	Reference Details

8.2 Validation Guidance

This document provides detailed validation guidance associated with Intel Platform Update Release (IPU).

QSR	Document Number	Reference Details

9 Open / Known Issues – To Date

Issue #	Description	Details	Affected Sku's

10 Archive - Fixes in Previous Kits

10.1 Kit 13.0.32.1478

Issue #	Description	Details	Found in Kit # Affected Sku's
1307126052	OEM public key hash MEManuf compare actual value is wrong.	**Affected Component:** sw.mfg_tools.memanuf **Symptoms:** MEManuf returning different value than expected. **Affected OS:** All **Workaround:** None	13.0.31.1465 ***All***

10.2 Kit 13.0.31.1465

Issue #	Description	Details	Found in Kit # Affected Sku's
1307192061	Intel® FPT -greset no does not restart automatically.	**Affected Component:** sw.mfg_tools.fpt **Symptoms:** Intel® FPT -greset no option does not initiate warm reset flow as expected. **Affected OS:** All **Workaround:** None	13.0.30.1435 ***All***

10.3 Kit 13.0.30.1435

Issue #	Description	Details	Found in Kit # Affected Sku's
1306998574	HDCP RX enable flags not set correctly for WiDi.	**Affected Component:** **Root Cause:** fw.cp.hdcp_rx **Symptoms:** WiDi failure. **Affected OS:** All **Workaround:** None	13.0.20.1319 ***All***
1307085632	IDLM tracing not working as expected.	**Affected Component:** **Root Cause:** fw.debug_and_trace.npk **Symptoms:** IDLM trace output blocked. **Affected OS:** All **Workaround:** None	13.0.20.1319 ***All***

10.4 Kit 13.0.20.1319

Issue #	Description	Details	Found in Kit # Affected Sku's
1306777325	Frimware status for indicating if flash logs are present showing as empty when the log file has reached maximum.	**Affected Component:** **Root Cause:** fw.os.storage **Symptoms:** The firmware status will incorrectly indicate that the flash log is empty when the log has reached maximum size. **Affected OS:** All **Workaround:** None	13.0.20.1314 ***All***
1306883701	The MAC OS version of the Intel® FIT tool can't open images with the -f parameter on the command line.	**Affected Component:** **Root Cause:** sw.mfg_tools.fit **Symptoms:** Images cannot be decomposed on the command line using the -f option with the MAC OS version of the Intel® FIT tool. **Affected OS:** All **Workaround:** None	13.0.20.1314 ***All***

10.5 Kit 13.0.20.1313

Issue #	Description	Details	Found in Kit # Affected Sku's
1306818840	Firmware failing to authenticate FDV Manifest.	**Affected Component:** **Root Cause:** sw.mfg_tools.fit **Symptoms:** Firmware fails to authenticate FDV Manifest due to issue in Intel® FIT image build process. **Affected OS:** All **Workaround:** None	13.0.20.1310 ***All***

10.6 Kit 13.0.20.1308

Issue #	Description	Details	Found in Kit # Affected Sku's
1306580015	OEM TAG value is incorrect when decomposing an image with the Intel® FIT tool.	**Affected Component:** **Root Cause:** sw.mfg_tools.fit **Symptoms:** The Intel® FIT tool does show the correct value for OEM TAG on decomposed images. **Affected OS:** All **Workaround:** None	13.0.20.1304 ***All***

Issue #	Description	Details	Found in Kit # Affected Sku's
1306623430	Platform reset occurring when using Intel® FPT "–closemnf" with "No" option.	**Affected Component:** **Root Cause:** sw.mfg_tools.fpt **Symptoms:** Using "-closemnf" along with "No" option is not preventing platform reset as expected. **Affected OS:** All **Workaround:** None	13.0.20.1304 ***All***

10.7 Kit 13.0.0.1086

Issue #	Description	Details	Found in Kit # Affected Sku's
1306592979	The Firmware Update RS Library API to get PDT version fails.	**Affected Component:** **Root Cause:** sw.mfg_tools.fw_update **Symptoms:** Firmware Update RS Library API fails with Error 272 when trying to get PDT version. **Affected OS:** All **Workaround:** None	13.0.0.1085 ***All***

10.8 Kit 13.0.0.1080

Issue #	Description	Details	Found in Kit # Affected Sku's
1306392200	Intel® FIT tool does not display the PCHC firmware version.	**Affected Component:** sw.mfg_tools.fit **Root Cause:** Missed requirement **Symptoms:** No version number is shown in FIT for the PCHC firmware. **Affected OS:** All **Workaround:** None	13.0.0.1066 ***All***
1409273074	Intel® FIT cannot build when PD controller Re-timer and SMBus addresses are the same.	**Affected Component:** sw.mfg_tools.fit **Root Cause:** **Symptoms:** Intel® FIT tool does not allow PD Controller Re-timer and SMBus addresses to be the same. **Affected OS:** All **Workaround:** None	13.0.0.1066 ***All***

10.9 Kit 13.0.0.1066

Issue #	Description	Details	Found in Kit # Affected Sku's
1807465844	Remove option disable/enable PCHC from FW update image build tab.	**Affected Component:** sw.mfg_tools.fit **Root Cause:** N/A **Symptoms:** The PCH Configuration binary is a required component for full and update FW and should not have an option to disable. **Affected OS:** All **Workaround:** None	13.0.0.1061 ***All***

10.10 Kit 13.0.0.1061

Issue #	Description	Details	Found in Kit # Affected Sku's
1306241838	MEInfo tool unexpectedly crashing when trying to run –feat option when "%" is present input string.	**Affected Component:** fw.cp.asmf **Root Cause:** Additional check added for invalid character detection. **Symptoms:** MEInfo will crash if the user input string contains "%". **Affected OS:** All **Workaround:** None	13.0.0.1057 ***All***

10.11 Kit 13.0.0.1057

Issue #	Description	Details	Found in Kit # Affected Sku's
1408986715	PAVP issues with the slot configuration used for Apple.	**Affected Component:** fw.cp.asmf **Root Cause:** The slot was configured to heavy mode instead of lite, and transcode fix was applied. **Symptoms:** DRM fails to work as expected. **Affected OS:** All **Workaround:** None	13.0.0.1054 ***All***

10.12 Kit 13.0.0.1054

Issue #	Description	Details	Found in Kit # Affected Sku's
1306158694	MEInfo displays wrong value for EPID GROUP ID feature.	**Affected Component:** sw.mfg_tools.info **Root Cause:** Corrected data copy. **Symptoms:** MEInfo will display incorrect EPID GROUP ID values in the output display to the user. **Affected OS:** All **Workaround:** None	13.0.0.1051 ***All***
1306184165	EK Revoke state in MEInfo tool does not align with System Tools User Guide definition.	**Affected Component:** sw.mfg_tools.info **Root Cause:** Updated MEInfo output to match with System Tools User Guide. **Symptoms:** MEInfo is displaying "enabled/disabled" versus System Tools User Guide "Revoked/Not Revoked. **Affected OS:** All **Workaround:** None	13.0.0.1051 ***All***

10.13 Kit 13.0.0.1051

Issue #	Description	Details	Found in Kit # Affected Sku's
1306138294	FPT failed to flash a new image (ME communication error).	**Affected Component:** sw.mfg_tools.fpt **Root Cause:** FWSTS needs to be read via PMX. **Symptoms:** The FPT tool is unable to flash a new image to the platform. **Affected OS:** All **Workaround:** None	13.0.0.1049 ***All***
1306140464	FPT is returning the wrong message when using the –e command.	**Affected Component:** sw.mfg_tools.fpt **Root Cause:** Corrected flow for –e command line option. **Symptoms:** FPT showing the skip verify output messaging when using the –e "skip erase" command. **Affected OS:** All **Workaround:** None	13.0.0.1049 ***All***

Issue #	Description	Details	Found in Kit # Affected Sku's
1306115243	Firmware needs to set the HDCP link type status for HDMI.	**Affected Component:** fw.cp.hdcp.tx **Root Cause:** Firmware updated to set HDCP link type for HDMI. **Symptoms:** HD content over HDMI potentially affect if playback relies on PAVP setting HDCP link type. **Affected OS:** All **Workaround:** None	13.0.0.1049 ***All***

10.14 Kit 13.0.0.1049

Issue #	Description	Details	Found in Kit # Affected Sku's
1306099147	FPT not recognizing stacked commands when their order is changed.	**Affected Component:** sw.mfg_tools.fpt **Root Cause:** Update to command line parser. **Symptoms:** FPT will show an unknown command failure with the following stacked command valid "fpt -closemnf no -y –verbose". **Affected OS:** All **Workaround:** None	13.0.0.1046 ***All***
1306115266	Windows DRM not working on Slim SKU firmware.	**Affected Component:** fw.cp.play_ready **Root Cause:** Slim SKU firmware updated to include relavent PAVP and datastore. **Symptoms:** Windows DRM will fails to function. **Affected OS:** Windows **Workaround:** None	13.0.0.1046 ***All***
1806447466	Enabling DAM mode through Northpeak not working.	**Affected Component:** fw.debug.hotham **Root Cause:** DAM mode not being intilized properly through Northpeak **Symptoms:** The user will receive "EnableDam: Invalid response" when trying to enable DAM through Northpeak. **Affected OS:** All **Workaround:** None	13.0.0.1046 ***All***

Issue #	Description	Details	Found in Kit # Affected Sku's
1306122239	Naming mismatch of PCHC between MEManuf and MEInfo.	**Affected Component:** sw.mfg_tools.manuf **Root Cause:** String names synced between MEManuf and MEInfo **Symptoms:** Under MEInfo PCHC is displayed as "PCHC FW Version" and under MEManuf as PCHC IPU Version". **Affected OS:** All **Workaround:** None	13.0.0.1046 ***All***

10.15 Kit 13.0.0.1044

Issue #	Description	Details	Found in Kit # Affected Sku's
1306070499	FWUpdlcl generating error.log file even when the Intel® CSME update has no errors.	**Affected Component:** sw.mfg_tools.fw_update **Root Cause:** Updated tool flow so error.log is generated when errors occur instead of warnings. **Symptoms:** The FWUpdlcl tools generates an error.log file even when update has been successful. **Affected OS:** All **Workaround:** None	13.0.0.1044 ***All***
1306070575	MEInfo FPF table output information missing column names.	**Affected Component:** sw.mfg_tools.info **Root Cause:** Changed from verbose to normal for FPF output display. **Symptoms:** MEInfo not showing column names for FPFs on output display. **Affected OS:** All **Workaround:** None	13.0.0.1044 ***All***
1306076688	MEManuf VAR test missing error level output when an error occurs.	**Affected Component:** sw.mfg_tools.manuf **Root Cause:** Error status output added. **Symptoms:** MEManuf VAR test failures do not return expected error levels. **Affected OS:** All **Workaround:** None	13.0.0.1044 ***All***

Issue #	Description	Details	Found in Kit # Affected Sku's
1306087371	FWUpdlcl fails with "Error 63: Unknown or unsupported hardware platform." when then platform experiences two G3s during firmware update.	**Affected Component:** fw.pm.maestro **Root Cause:** Firmware inadvertently setting image failure status **Symptoms:** **Affected OS:** All **Workaround:** None	13.0.0.1044 ***All***

10.16 Kit 13.0.0.1044

Issue #	Description	Details	Found in Kit # Affected Sku's
1306017086	MEInfo displayes unknown value for "TCSS FW partial update Policy configuration" feature.	**Affected Component:** sw.mfg_tools.info **Root Cause:** NVAR Permissions updated. **Symptoms:** MEInfo returns Warning: Failed getting variable "TCSS FW partial update Policy configuration" value. Error 70: TCSS FW PARTIAL UPDATE POLICY CONFIGURATION actual value is - Unknown. **Affected OS:** All **Workaround:** None	13.0.0.1042 ***All***
1306056763	MEInfo Feat command failed with the new FPFs.	**Affected Component:** sw.mfg_tools.info **Root Cause:** FPF data structure updated. **Symptoms:** MEInfo returning Error 67 Feature not found with new FPFs. **Affected OS:** All **Workaround:** None	13.0.0.1042 ***All***

10.17 Kit 13.0.0.1042

Issue #	Description	Details	Found in Kit # Affected Sku's
1306001691	MEInfo displaying "*In use" in an incorrect location.	**Affected Component:** sw.mfg_tools.info **Root Cause:** String list corrected. **Symptoms:** MEInfo OEM Public Key Hash displaying "*In Use" shifted to the right of other entries. **Affected OS:** All **Workaround:** None	13.0.0.1040 ***All***
1306004888	Intel® FPT Commit of Anti Rollback SVN failing.	**Affected Component:** fw.mfg_fw.mca **Root Cause:** Corrected SVN Commit flows. **Symptoms:** Intel® FPT Commit of Anti Rollback SVN shows "Error 9: Commit Anti Rollback SVN failed". **Affected OS:** All **Workaround:** None	13.0.0.1040 ***All***
1306007578	MEInfo -FEAT FPFs failed with "feature not found" error.	**Affected Component:** sw.mfg_tools.info **Root Cause:** String list corrected. **Symptoms:** MEInfo returning failures when using –FEAT FPF command line options. **Affected OS:** All **Workaround:** None	13.0.0.1040 ***All***
1408257094	MEInfo displaying incorrect firmware status information.	**Affected Component:** sw.mfg_tools.info **Root Cause:** Changed parameted order. **Symptoms:** The firmware status returned to the used is incorrect. **Affected OS:** All **Workaround:** None	13.0.0.1040 ***All***

10.18 Kit 13.0.0.1040

Issue #	Description	Details	Found in Kit # Affected Sku's
1305913417	Intel® CSE not responding during GUC interaction image flickering, macroblocks etc.	**Affected Component:** fw.cp.pavp **Root Cause:** Interupt handling not updated to Gen11+ **Symptoms:** Image flickering / macroblocks. **Affected OS:** All **Workaround:** None	13.0.0.1037 ***All***
1305952933	Intel® FIT tool crashing during image decompose.	**Affected Component:** sw.mfg_tools.fit **Root Cause:** Corrected parsing issue when decomposing image. **Symptoms:** GUI automatically closing. CLI displays error "Segmentation fault (core dumped)" **Affected OS:** Mac OS **Workaround:** None	13.0.0.1037 ***All***
1305909060	FWUpdlcl failing during updates.	**Affected Component:** sw.mfg_tools.fw_update **Root Cause:** FWUpdlcl missing updated FW structure changes. **Symptoms:** Error 447: Non-optional IUP (like LOCL, WCOD) inside IUPs list (in FTPR manifest extension) is not in the Flash Image. **Affected OS:** All **Workaround:** None	13.0.0.1037 ***All***
1407895019	The Intel® FIT tool cannot to load Intel® CSME binary from the UI.	**Affected Component:** sw.mfg_tools.fit **Root Cause:** Issue in how The Intel® FIT was handled parsing Intel® CSME binary. **Symptoms:** When attempting to load Intel® CSME binary from the UI users will receive Error 17 [FitAction] Failed to parse CSE region. **Affected OS:** All **Workaround:** None	13.0.0.1037 ***All***

Issue #	Description	Details	Found in Kit # Affected Sku's
1305925217	Type-C State setting is locked in "un-subscription" mode.	**Affected Component:** sw.mfg_tools.fit **Root Cause:** Type-C State lockout tied to PMC-PD controller USB-C* Mode Enabled should be tied to xDCI Split Die Configuration. **Symptoms:** Unable to change the Type-C State setting. **Affected OS:** All **Workaround:** None	13.0.0.1037 ***All***
1305904516	iTouch is not working while loading to OS	**Affected Component:** fw.itouch.heci_commands. **Root Cause:** Touch register writes were occurring when the SPI controller was busy. **Symptoms:** Touch does not work as expected during OS load. **Affected OS:** All **Workaround:** None	13.0.0.1037 ***All***

10.19 Kit 13.0.0.1037

Issue #	Description	Details	Found in Kit # Affected Sku's
1407895019	The Intel® FIT tool cannot to load Intel® CSME binary from the UI.	**Affected Component:** sw.mfg_tools.fit **Root Cause:** Issue in how The Intel® FIT was handled parsing Intel® CSME binary. **Symptoms:** When attempting to load Intel® CSME binary from the UI users will receive Error 17 [FitAction] Failed to parse CSE region. **Affected OS:** All **Workaround:** None	13.0.0.1034 ***All***
1305925217	Type-C State setting is locked in "un-subscription" mode.	**Affected Component:** sw.mfg_tools.fit **Root Cause:** Type-C State lockout tied to PMC-PD controller USB-C* Mode Enabled should be tied to xDCI Split Die Configuration. **Symptoms:** Unable to change the Type-C State setting. **Affected OS:** All **Workaround:** None	13.0.0.1034 ***All***

Issue #	Description	Details	Found in Kit # Affected Sku's
1305910442	Intel® FIT programming wrong OEM registers addresses for Gen4.	**Affected Component:** sw.mfg_tools.fit **Root Cause:** Gen4 Registers offsets were being shifted by 4. **Symptoms:** Gen4 does not operate as expected. **Affected OS:** All **Workaround:** None	13.0.0.1034 ***Slim***
1305909060	FWUpdlcl fails during same FW version update.	**Affected Component:** sw.mfg_tools.fw_update **Root Cause:** FWUpdlcl missing updated FW structure changes. **Symptoms:** Error 447: Non-optional IUP (like LOCL, WCOD) inside IUPs list (in FTPR manifest extension) is not in the Flash Image. **Affected OS:** All **Workaround:** None	13.0.0.1034 ***All***

10.20 Kit 13.0.0.1034

Issue #	Description	Details	Found in Kit # Affected Sku's
1305893242	General error is received when trying to commit CVARs with FPT config file.	**Affected Component:** sw.mfg_tools.fpt **Root Cause:** The config file contained invalid values. FPT error messaging updated to be more informative. **Symptoms:** FPT returns error 274 and error 202 when trying to update CVARs. **Affected OS:** All **Workaround:** None	13.0.0.1033 ***All***
1305897304	MEInfo displays "UNKNOWN" values for BIOS Config Lock and GbE Config Lock	**Affected Component:** sw.mfg_tools.info **Root Cause:** MEInfo updated to use SPIBase address instead of setting to zero. **Symptoms:** MEInfo displays "UNKNOWN" for BIOS and GbE Config Lock values. **Affected OS:** All **Workaround:** None	13.0.0.1033 ***All***

Issue #	Description	Details	Found in Kit # Affected Sku's
1305897752	Preforming full FW update in EFI will fail with a communication error.	**Affected Component:** sw.mfg_tools.fw_update **Root Cause:** HECI was not getting initialized. **Symptoms:** FWUpdlcl returns 'Communication error between application and Intel (R) ME module' **Affected OS:** All **Workaround:** None	13.0.0.1033 ***All***

10.21 Kit 13.0.0.1033

Issue #	Description	Details	Found in Kit # Affected Sku's
1305833314	FPT displays a warning message when dumping flash image (consumer 32M) - Warning: There are some addresses that are not defined in any regions.	**Affected Component:** sw.mfg_tools.fpt **Root Cause:** Change output message to notify instead of warning. **Symptoms:** Warning message being displayed when dumping 32 Meg image. **Affected OS:** All **Workaround:** None	13.0.0.1030 ***All***
1305873771	Some features displayed "UNKNOWN" values in MEInfo.	**Affected Component:** sw.mfg_tools.info **Root Cause:** Invalid NVARs being displayed. **Symptoms:** Certain features are being displayed to the user with an Unknown status. **Affected OS:** All **Workaround:** None	13.0.0.1030 ***All***

10.22 Kit 13.0.0.1030

Issue #	Description	Details	Found in Kit # Affected Sku's
1305796578	MEManuf EOL Config tests displays wrong error for test: FPFs in UEP Committed.	**Affected Component:** sw.mfg_tools.manuf **Root Cause:** MEManuf failed to check the FPF type. **Symptoms:** MEManuf returns incorrect Error 303: ME Region read access permissions don't match Intel recommended values. **Affected OS:** All **Workaround:** None	13.0.0.1027 ***All***
1305815555	MEManuf -EOL config fail to test the FPF: "OEM Public Key Hash"	**Affected Component:** sw.mfg_tools.manuf **Root Cause:** MEManuf Hex to Bin conversion did not take size into account. **Symptoms:** MEManuf returns OEM Public Key Hash – Failed error. **Affected OS:** All **Workaround:** None	13.0.0.1027 ***All***
1305815601	MEManuf -EOL config failed testing the FPFs with "XX" value	**Affected Component:** sw.mfg_tools.manuf **Root Cause:** MEManuf Hex to Bin conversion did not take size into account. **Symptoms:** MEManuf returns Data Size Mismatch error. **Affected OS:** All **Workaround:** None	13.0.0.1027 ***All***
1305817439	FPT failed to compare some FPFs with correct values.	**Affected Component:** sw.mfg_tools.fpt **Root Cause:** FPT Hex to Bin conversion did not take size into account. **Symptoms:** FPT returns Data Size Mismatch error. **Affected OS:** All **Workaround:** None	13.0.0.1027 ***All***
1806298029	GPIO NVAR value is not changed after update and commit from file.	**Affected Component:** fw.io_drivers.gpio **Root Cause:** GPIO attributes updated. **Symptoms:** GPIO values do not update as expected. **Affected OS:** All **Workaround:** None	13.0.0.1027 ***All***

Issue #	Description	Details	Found in Kit # Affected Sku's
1806330589	FPT display error message when updating NVAR with config file.	**Affected Component:** sw.mfg_tools.fpt **Root Cause:** FPT update handle instances where the config file only contains some of the NVARs. **Symptoms:** FPT returns Error 58: The CSE File Component requested, "îw¿Ø", is not valid for this operation. **Affected OS:** All **Workaround:** None	13.0.0.1027 ***All***
1305832123	FWUpdlcl returns an empty text dump with when -verbose command used with –ForceReset.	**Affected Component:** sw.mfg_tools.fw_update **Root Cause:** Exit Handler call added before restart flow. **Symptoms:** FWUpdlcl returns an empty file in verbose more when using –ForceReset. **Affected OS:** All **Workaround:** Do not use –Verbose and –ForceReset options on the same command line.	13.0.0.1027 ***All***
1506444293	The iunit lost after using Intel® FIT 13.0.0.1023 to build with IUNIT binary.	**Affected Component:** sw.mfg_tools.fit **Root Cause:** Corrected issues with enable/disable layout entries mechanism **Symptoms:** IUnit functionality being lost. **Affected OS:** All **Workaround:** None.	13.0.0.1027 ***All***

10.23 Kit 13.0.0.1027

Issue #	Description	Details	Found in Kit # Affected Sku's
1305492628	Sending random data to data registers (1-3) through Northpeak will cause firmware to get stuck.	**Affected Component:** fw.debug.hotham **Root Cause:** Message length was not aligned. **Symptoms:** Firmware will get stuck. **Affected OS:** All **Workaround:** Platform G3.	13.0.0.1026 All

Issue #	Description	Details	Found in Kit # Affected Sku's
1305733144	MEManuf EOL var check sporadically passing when firmware update OEM ID is set incorrectly.	**Affected Component:** sw.mfg_tools.manuf **Root Cause:** CVAR and memory allocation issues. **Symptoms:** Sporadic passing results with incorrect OEM ID set. **Affected OS:** All **Workaround:** None.	13.0.0.1026 All
1305758529	FPT CVAR Commit command failing with Error 491 NVAR access in the system caused general error.	**Affected Component:** sw.mfg_tools.fpt **Root Cause:** FPT error return code output updated. **Symptoms:** FPT showing incorrect Error 491 when trying to access CVARs which can only be configured once. **Affected OS:** All **Workaround:** None.	13.0.0.1026 Slim
1305807551	MEInfo displays "Unknown" value for C-Link status.	**Affected Component:** sw.mfg_tools.info **Root Cause:** Tool updated to include dependency check for corporate. **Symptoms:** MEInfor returns unexpected response to C-Link status. **Affected OS:** All **Workaround:** None.	13.0.0.1026 Slim
1305808137	MEManuf EOL config test failing but shows a Success message.	**Affected Component:** sw.mfg_tools.manuf **Root Cause:** Print error **Symptoms:** EOL config test fails but shows a successful result. **Affected OS:** All **Workaround:** None.	13.0.0.1026 All
1806298720	PAVP is not sending interrupt to the GuC on the correct address.	**Affected Component:** fw.cp.pavp **Root Cause:** PAVP was using address for prior generations. **Symptoms:** PAVP is unable to communicate with GuC. **Affected OS:** All **Workaround:** None.	13.0.0.1026 Slim

10.24 Kit 13.0.0.1026

Issue #	Description	Details	Found in Kit # Affected Sku's
1806212647	Intel® MEManuf returning an internal error message when Intel® CSE is disabled.	**Affected Component:** sw.mfg_tools.manuf **Root Cause:** Error reporting refactorting **Symptoms:** Intel® MEManuf shows internal error when Intel® CSE is disabled. **Affected OS:** All **Workaround:**.	13.0.0.1021 All
1806288426	Intel® FPT returing an incorrect error response when trying to read a non-existing FPF.	**Affected Component:** sw.mfg_tools.fpt **Root Cause:** Issue being cause by firmware. **Symptoms:** An incorrect error will be displayed when trying to read a non-existing FPF. **Affected OS:** All **Workaround:**.	13.0.0.1021 All
1305791368	Intel® FPT Get attributes command and set file failing.	**Affected Component:** sw.mfg_tools.fpt **Root Cause:** FPF flags changed firmware. **Symptoms:** The tool will return a failure when trying using Get attributes and set file commands. **Affected OS:** All **Workaround:**.	13.0.0.1021 All
1506127318	Intel® FIT tool not allowing 4 digit Region Master Access values.	**Affected Component:** sw.mfg_tools.fit **Root Cause:** Tool updated to allow 4 digit Region Master Access values. **Symptoms:** No ability to configure 4 digit Region Master Access values. **Affected OS:** All **Workaround:**.	13.0.0.1021 All
1305758421	Intel® MEInfo returns Error 313: Region does not exist on Slim SKU.	**Affected Component:** sw.mfg_tools.info **Root Cause:** Change print output behavior for errors. **Symptoms:** Unexpected error in tool output - Error 313: Region does not exist. **Affected OS:** All **Workaround:**.	13.0.0.1021 All

Issue #	Description	Details	Found in Kit # Affected Sku's
1806212647	Intel® MEManuf returning an internal error message when Intel® CSE is disabled.	**Affected Component:** sw.mfg_tools.manuf **Root Cause:** Error reporting refactorting **Symptoms:** Intel® MEManuf shows internal error when Intel® CSE is disabled. **Affected OS:** All **Workaround:**.	13.0.0.1021 All

10.25 Kit 13.0.0.1021

Issue #	Description	Details	Found in Kit # Affected Sku's
1305709019	Max SSC on Standard profile is showing 0 instead of 50.	**Affected Component –** fw.icc.programming **Impact:** Max SSC on Standard profile not being set to the correct value. **Workaround:** None. **Notes:**	13.0.0.1011 All
1806164768	Intel® FPT closemnf command fails when using custom descriptor permissions values.	**Affected Component –** sw.mfg_tools.fpt **Impact:** Users will be unable to assign custom permission values. **Workaround:** None. **Notes:**	13.0.0.1016 All
1806149675	NVARs not being updated after commit command has been sent.	**Affected Component –** fw.mfg_fw.mca **Impact:** NVARs will fail to update when using the commit command. **Workaround:** None. **Notes:**	13.0.0.1016 All
1806191305	Intel® FPT shows the wrong region master access values when using the –I command.	**Affected Component –** sw.mfg_tools.fpt **Impact:** Intel® FPT showing wrong region master access values. **Workaround:** None. **Notes:**	13.0.0.1016 All

Issue #	Description	Details	Found in Kit # Affected Sku's
1305731721	Intel® MEMauf EOL configuration test displaying incorrect warning message	**Affected Component –** sw.mfg_tools.manuf **Impact:** Incorrect warning messages confusing to users. **Workaround:** None. **Notes:**	13.0.0.1016 All
1305700996	Intel® CCT tool not working in EFI shell shows error 8202.	**Affected Component –** sw.icc.cct **Impact:** CCT tool not working in EFI **Workaround:** Use Windows version. **Notes:**	13.0.0.1016 All

10.26 Kit 13.0.0.1016

Issue #	Description	Details	Found in Kit # Affected Sku's
1305709168	Multiple error messages are displayed together, appearing as one error message.	**Affected Component –** sw.mfg_tools.fpt **Impact:** confusion in reading error messages **Workaround:** None.	13.0.0.1011
1305713264	Intel® CCT GetRegister command returns uninformative error when it's given an invalid end point ID.	**Affected Component –** sw.icc.cct **Impact:** non-descriptive message appears. **Workaround:** None.	13.0.0.1011
1505028009	Intel® MEManuf is missing the description -tag in some EOL tests	**Affected Component –** sw.mfg_tools.manuf **Impact:** customer does not understand which test to opt in/out due to lack of description **Workaround:** None.	13.0.0.1011
1407012765	ISH Manifest generation failing with Intel® MEU; cannot import manifest that was previously used.	**Affected Component –** sw.mfg_tools.fpt **Impact:** Cannot build image **Workaround:** None.	13.0.0.1011
1305700750	Intel® FIT tool should not build the image when the data value is not in Hex format.	**Affected Component –** sw.mfg_tools.fit **Impact:** the image is built without any error message generated. **Workaround:** None.	13.0.0.1011

Issue #	Description	Details	Found in Kit # Affected Sku's
1305598934	Dynamic ICC settings reverting back to default after Deep Sx.	**Affected Component –** fw.icc.clocking **Impact:** Dynamic ICC settings do not survive Deep Sx power flows. **Workaround:** None.	13.0.0.1011
1806136219	EFI MEInfo will show communication errors when dumping tool output to a file.	**Affected Component –** sw.mfg_tools.info **Impact:** Users will be unable to dump the output from EFI MEInfo tool to a file. **Workaround:** None.	13.0.0.1013

10.27 Kit 13.0.0.1011

Issue #	Description	Details	Found in Kit # Affected Sku's
1305598934	ICC Dynamic settings does not survive Deep S4.	**Affected Component –** fw.icc.programming **Impact:** ICC Dynamic setting gets reverted after resuming from Deep S4. **Workaround:** None. **Notes:**	13.0.0.1007 All
1305481226	Intel® FPT failing to compare the BootGuard FPF and showing "Error 510: Detected invalid data size".	**Affected Component –** sw.mfg_tools.fpt **Impact:** Intel® FPT unable to do a compare of the BootGuard FPF. **Workaround:** None. **Notes:**	13.0.0.1007 All
1305666123	Intel® Silicon View Technology scripts failing to run on Ice Lake platforms.	**Affected Component –** fw.debug.hotham **Impact:** Currently cannot run Intel® Silicon View Technology on Ice Lake platforms. **Workaround:** None. **Notes:**	13.0.0.1007 All
1305681506	Intel® MEInfo not aligned with current POR for RPMC/RPMB settings.	**Affected Component –** sw.mfg_tools.info **Impact:** Intel® MEInfo output for RPMC/RPMB is currently incorrect. **Workaround:** None. **Notes:**	13.0.0.1007 All

Issue #	Description	Details	Found in Kit # Affected Sku's
1305682286	Intel® MEManuf EOL VAR failing to test encrylpted CVARs. The tool returns "Error 327"	**Affected Component –** sw.mfg_tools.manuf **Impact:** EOL VAR check to test encrypted CVARs not possible. **Workaround:** None. **Notes:**	13.0.0.1007 All
1305685041	Intel® FPT erase command fails with "Error 28" communication error.	**Affected Component –** sw.mfg_tools.fpt **Impact:** Intel® FPT erase command no working as expected. **Workaround:** None. **Notes:**	13.0.0.1007 All
1305359211	There is confusing output information being returned by Intel® MEInfo in FPF HW column before FPFs are committed.	**Affected Component –** sw.mfg_tools.info **Impact:** Intel® MEInfo output FPF HW column contains confusing output information. **Workaround:** None. **Notes:**	13.0.0.1007 All
1305621047	Intel® FPT displaying an incorrect error message "Error 95: system integrator ID: value already set" when attempting to commit ODM ID or Reserved ID more than once.	**Affected Component –** sw.mfg_tools.fpt **Impact:** Intel® FPT displays the wrong error message if ODM ID or Reserved ID are commited more than once. **Workaround:** None. **Notes:**	13.0.0.1007 All
1305690678	ICC help text updated in the Intel® FIT tool.	**Affected Component –** sw.mfg_tools.fit **Impact:** Intel® FIT help text for ICC not up to date. **Workaround:** None. **Notes:**	13.0.0.1007 All
1305691261	The Intel® FIT tool is not updated IOM OEM Config data NVAR.	**Affected Component –** sw.mfg_tools.fit **Impact:** Intel® FIT does not update IOM OEM Config data NVAR as expected. **Workaround:** None. **Notes:**	13.0.0.1007 All

10.28 Kit 13.0.0.1007

Issue #	Description	Details	Found in Kit # Affected Sku's
1305654161	Intel® FIT returning Error 31 when decomposing a dumped image.	**Affected Component –** sw.mfg_tools.fit **Impact:** When trying to decompose and image that was dumped from a platform the Intel® FIT tool returns Error 31. **Workaround:** None. **Notes:**	13.0.0.1003 All
1305653975	Platform is unable to boot after Closemnf has been done.	**Affected Component –** **f**w.mfg_fw.mca **Impact:** The platform does not boot after issuing a –closemnf command with the Intel® FPT tool. **Workaround:** None. **Notes:**	13.0.0.1003 All
1305653316	Intel® MEInfo FPF display output unreadable.	**Affected Component –** sw.mfg_tools.info **Impact:** FPF display output is unreadable to the user. **Workaround:** None. **Notes:**	13.0.0.1003 All
1305634375	Blank Check operation failed and flash new image failed.	**Affected Component –** sw.mfg_tools.fpt **Impact:** Intel® FPT failing on blank check and new image flashing. **Workaround:** None. **Notes:**	13.0.0.1003 All
1305550218	ICC Adaptive profile is not being recognized.	**Affected Component –** fw.icc.programming **Impact:** Customers will not be able to use Adaptive ICC profile. **Workaround:** None. **Notes:**	13.0.0.1003 All
1305566658	RPMC Rebind fails: The machine gets stuck with post code: 10AD on the first boot with the new SPI flash.	**Affected Component –** fw.os.storage **Impact:** RPMC Rebind not working as expected causing platform hang on first boot after flashing new SPI part. **Workaround:** Set Intel® PPT RPMC Supported to "No". **Notes:**	13.0.0.1003 All

Issue #	Description	Details	Found in Kit # Affected Sku's
1305609024	Intel® MEManuf show incorrect message if there is a mismatch on the Firmware Update OEM ID NVAR.	**Affected Component –** sw.mfg_tools.manuf **Impact:** MEManuf returns an incorrect error message for Firmware update OEM ID NVAR when there is a mismatch. **Workaround:** None. **Notes:**	13.0.0.1003 All
1305621619	Intel® MEInfo showing "Error 32:Unexpected result in command response" in display output.	**Affected Component –** sw.mfg_tools.info **Impact:** Intel® MEInfo showing unexpected errors on display output. **Workaround:** None. **Notes:**	13.0.0.1003 All
1305550218	ICC Adaptive profile is not being recognized.	**Affected Component –** fw.icc.programming **Impact:** Customers will not be able to use Adaptive ICC profile. **Workaround:** None. **Notes:**	13.0.0.1003 All

10.29 Kit 13.0.0.1003

Issue #	Description	Details	Found in Kit # Affected Sku's
1305562671	Platform does not boot with Adaptive Profile when SSC configured to 2%.	**Affected Component –** fw.icc.clocking **Impact:** Not able to set BLCK to 100MHz as expected. **Workaround:** None. **Notes:**	13.0.0.1002 All
1305530191	BCLK showing 98MHz instead of 100MHz on Standard Profile.	**Affected Component –** fw.icc.clocking **Impact:** Not able to set BLCK to 100MHz as expected. **Workaround:** None. **Notes:**	13.0.0.1002 All
1305583568	Seeing Intel® PTT commands being delayed after several TPM2_Clear calls.	**Affected Component –** fw.os.vfs **Impact:** After several commands are executed Intel® PTT responses will be significantly delayed. **Workaround:** None. **Notes:**	13.0.0.1002 All

Issue #	Description	Details	Found in Kit # Affected Sku's
1305590379	Intel® FPT is –closemnf failing with Error 312 and Error 372.	**Affected Component –** sw.mfg_tools.fpt **Impact:** Intel® FPT –closemnf command fails to work as expected. **Workaround:** None. **Notes:**	13.0.0.1002 All
1305596745	Intel® FPT –closemnf command shows error message on BootGuard configuration but still shows Successful.	**Affected Component –** sw.mfg_tools.fpt **Impact:** Intel® FPT –closemnf showing an error with BootBuard config but still shows that it successfully completed. **Workaround:** None. **Notes:**	13.0.0.1002 All

10.30 Kit 13.0.0.1002

Issue #	Description	Details	Found in Kit # Affected Sku's
1305524239	OEMKeyManifest and RotKeyManifest configs are missing help text.	**Affected Component –** sw.mfg_tools.meu **Impact:** Help text for OEMKeyManifest and RotKeyManifest missing from XML files generated by the MEU tool. **Workaround:** None. **Notes:**	13.0.0.1002 All
1305560889	Get Clock returning incorrect user frequency on Adaptive profile.	**Affected Component –** fw.icc.clocking **Impact:** Platform would boot with an incorrect frequency when running Adaptive profile. **Workaround:** None. **Notes:**	13.0.0.1002 All
1305560894	Set Clock causing the platform to hang on boot with a CATERR with Adaptive profile.	**Affected Component –** fw.icc.clocking **Impact:** Using Set Clock under Adaptive profile causing the platform to hang with a CATERR. **Workaround:** None. **Notes:**	13.0.0.1002 All

Issue #	Description	Details	Found in Kit # Affected Sku's
1305579944	Intel® FPT is not updating Key Manifest ID but still returning an operation successful result.	**Affected Component –** sw.mfg_tools.fpt **Impact:** Intel® FPT is not able to program the Key Manifest ID. **Workaround:** None. **Notes:**	13.0.0.1002 All
1305581708	Intel® MEManuf using "-EOL VAR" fails to read OEM Tag variable.	**Affected Component –** sw.mfg_tools.manuf **Impact:** Intel® MEManuf failing to read back OEM Tag NVAR when using "-EOL VAR" command line option. **Workaround:** None. **Notes:**	13.0.0.1002 All
1305591720	Intel® MEManuf configuration file is missing Firmware Update OEM ID entries.	**Affected Component –** sw.mfg_tools.manuf **Impact:** Intel® MEManuf configuration file does not contain the Firware Update OEM ID test entries. **Workaround:** None. **Notes:**	13.0.0.1002 All
1406798412	Intel® ME is not acknowledging GUC wake requests.	**Affected Component –** fw.io_drivers.vdm **Impact:** GUC wake requests are not being acknowleged by Intel® ME. **Workaround:** None. **Notes:**	13.0.0.1002 All
1504715909	The Intel® FIT tool is not setting USB 2 ports back to Type-A / Type-C when the associated PD controller is disabled.	**Affected Component –** sw.mfg_tools.fit **Impact:** Intel® FIT does not revert the USB2 port settings back to Type-A / Type-C when their associated PD controller is disabled. **Workaround:** None. **Notes:**	13.0.0.1002 All

10.31 Kit 13.0.0.7057

Issue #	Description	Details	Found in Kit # Affected Sku's
1305173629	Intel® AMT is setting PG override right after entering CM0-PG.	**Affected Component –** fw.amt.alarm_clock **Impact:** The Intel® ME will not enter PG as expected in Simic. **Workaround:** None. **Notes:**	13.0.0.7053 Simic
1305407632	The error message returned by Intel® FPT when doing "–closemnf" with the "–no" option is unclear.	**Affected Component –** sw.mfg_tools.fpt **Impact:** Intel® FPT error message not clear when adding "–no" option at the end of "–closemnf". **Workaround:** None. **Notes:**	13.0.0.7053 All
1305472633	Intel® FPT returns a General error when trying to update more than 16 NVAR at once.	**Affected Component –** sw.mfg_tools.fpt **Impact:** Intel® FPT unable to handle more than 16 NVAR changes at the same time. **Workaround:** Update less than 16 NVARs simulaniously. **Notes:**	13.0.0.7053 All
1305535112	Errors messages returned by Intel® MEManuf appear with incorrect colors.	**Affected Component –** sw.mfg_tools.manuf **Impact:** Users could potentially miss failures returned by Intel® MEManuf because they are not highlighted in red. **Workaround:** None. **Notes:**	13.0.0.7053 All
1305546139 1305527005	Incorrect errors are being returned by Intel® MEInfo when using the "-feat" command line option.	**Affected Component –** sw.mfg_tools.info **Impact:** Incorrect errors when using the "-feat" command are confusing to users. **Workaround:** None. **Notes:**	13.0.0.7053 All
1305167609	Intel® MEU List of all the manifests available for export showing garbled names.	**Affected Component –** sw.mfg_tools.meu **Impact:** Intel® MEU list of avalible manifests shows grabled output for the names. **Workaround:** None. **Notes:**	13.0.0.7053 All

Issue #	Description	Details	Found in Kit # Affected Sku's
1305528707	Intel® FPT allowing user input of invalid values for the BootGuard FPF.	**Affected Component –** sw.mfg_tools.fpt **Impact:** Intel® FPT allowing invalid values to be accepted for BootGuard FPF. **Workaround:** None. **Notes:**	13.0.0.7053 All
1305527317	The Type-C Subsystem NVAR is not being updated by the Intel® FIT tool during image build.	**Affected Component –** sw.mfg_tools.fit **Impact:** Intel® FIT is not updating the Type-C Subsystem NVAR as expected during image build. **Workaround:** None. **Notes:**	13.0.0.7053 All
1305449011	Intel® MEManuf EOL VAR test failing when comparing against the value 0x01.	**Affected Component –** sw.mfg_tools.manuf **Impact:** Intel® MEManuf EOL VAR fails when comparing against the value 0x01. **Workaround:** Change value in XML file to 0x1. **Notes:**	13.0.0.7053 All
1305449020	Intel® MEManuf EOL VAR test compares against a null value instead of comparing to the provided input long value.	**Affected Component –** sw.mfg_tools.manuf **Impact:** Intel® MEManuf EOL VAR comparing to null values when checking against a input long value. **Workaround:** None. **Notes:**	13.0.0.7053 All
1305493141	Intel® FIT tool crashes when writing Thunderbolt™ data over 1,452 bytes in length.	**Affected Component –** sw.mfg_tools.fit **Impact:** Intel® FIT crashes with an error message when trying to write Thunderbolt™ data that is over 1,452 bytes long. **Workaround:** None. **Notes:**	13.0.0.7053 All

10.32 Kit 13.0.0.7053

Issue #	Description	Details	Found in Kit # Affected Sku's
1305505829	The Intel® ME is timing out during init stage during system boot.	**Affected Component –** fw.bringup.storage **Impact:** Intel® ME times out with a HECI failure during platform boot. **Workaround:** None. **Notes:**	13.0.0.7046 All
1305505368	The Intel® FIT tool is using the wrong GPIOs for SRC0-SRC5 CLKREQ#.	**Affected Component –** sw.mfg_tools.fit **Impact:** Intel® FIT tool using the wrong GPIOs for SRC0-SRC5 CLKREQ# settings. **Workaround:** None. **Notes:**	13.0.0.7046 All
1305497550	The Firmware tools are failing to run as expected under the Simics environment.	**Affected Component –** sw.mfg_tools.info **Impact:** Firmware tools failing to run properly under Simics environment. **Workaround:** None. **Notes:**	13.0.0.7046 Simics Only
1305460810	Intel® MEInfo shows a failure with error code 85 when running firmware in debug mode.	**Affected Component –** sw.mfg_tools.info **Impact:** Intel® MEInfo fails with error code 85 when debug firmware. **Workaround:** None. **Notes:**	13.0.0.7046 All
1305416816 1305495560	Intel® MEManuf truncating values expected when doing EOL checks.	**Affected Component –** sw.mfg_tools.manuf **Impact:** Intel® MEManuf truncating values when doing EOL checks. **Workaround:** None. **Notes:**	13.0.0.7046 All
1305412387	Intel® FPT should read and display all NVARs values in ascending order.	**Affected Component –** sw.mfg_tools.fpt **Impact:** Intel® FPT not displaying NVARs in ascending order as expected. **Workaround:** None. **Notes:**	13.0.0.7046 All

Issue #	Description	Details	Found in Kit # Affected Sku's
1305360617	Intel® MEInfo does not parse the RPMC bits in the FWSTS register, as other information.	**Affected Component –** sw.mfg_tools.info **Impact:** Intel® MEInfo is not showing RPMC bits in the FWSTS output display. **Workaround:** None. **Notes:**	13.0.0.7046 All
1305254311	Updating user consent language fails as expected when FWU client is busy, but no failure event appears.	**Affected Component –** sw.amt.lms.windows **Impact:** IMSS fails to update the user consent language however no event is seen in the log. **Workaround:** None. **Notes:**	13.0.0.7046 Corp
1305322758	LMS doesn't update the hosts file when changing Intel® AMT host name.	**Affected Component –** sw.amt.imss **Impact:** The Windows Host file is not being updated by LMS when the Intel® AMT host name is changed **Workaround:** None. **Notes:**	13.0.0.7046 Corp
1305143119	Intel® MEManuf BIST Test failes with - "Internal error - SMBus Read Byte PEC failure" (SIMICS ONLY).	**Affected Component –** fw.io_drivers.smbus **Impact:** Intel® MEManuf will fail with internal errors on Simics. **Workaround:** None. **Notes:**	13.0.0.7046 Simics only
1305472660	Intel® FPT displays an incorrect error message when Intel® ME is in recovery mode.	**Affected Component –** sw.mfg_tools.fpt **Impact:** Incorrect error message gets displayed when Intel® ME is in recovery mode. **Workaround:** None. **Notes:**	13.0.0.7046 All
1305471849	Intel® FPT returns an unclear error when trying to update the Delayed Authentication Mode CVAR.	**Affected Component –** fw.mfg_fw.mca **Impact:** Intel® FPT error when trying to set Delayed Authentication Mode CVAR prevents the settings from being configured. **Workaround:** Use Intel® FIT tool to enable Delayed Authentication Mode in platform image. **Notes:**	13.0.0.7046 All

Issue #	Description	Details	Found in Kit # Affected Sku's
1305472938	Intel® FIT tool returing errors for USB2 Port Connector Type settings on start-up.	**Affected Component –** sw.mfg_tools.fit **Impact:** Intel® FIT tool returning errors for USB2 Port Connector Type settings when started. **Workaround:** None. **Notes:**	13.0.0.7046 All

10.33 Kit 13.0.0.7046

Issue #	Description	Details	Found in Kit # Affected Sku's
1305195263	Platform fails to enter Deep S5 using power button override.	**Affected Component –** fw.pm.maestro **Impact:** Platform cannot enter Deep S5 when using the power button override. **Workaround:** Enter Deep S5 via host OS. **Notes:**	All
1305195612	Intel® ME fails to enter Deep Sx when provisioned and set to power policy 2.	**Affected Component –** fw.pm.maestro **Impact:** Intel® ME does not enter Deep Sx state when provisioned with power policy 2. **Workaround:** None. **Notes:**	Corp
1305341093	Intel® FIT tool showing invalid value warning messages when decomposing images.	**Affected Component –** sw.mfg_tools.fit **Impact:** Intel® FIT tool showing invalid value warning messages for USB3 Port 1 when decomposing images. **Workaround:** None. **Notes:**	All
1305341133	Intel® FPT cannot update KVM variable setting using configuration file.	**Affected Component –** sw.mfg_tools.fpt **Impact:** Intel® FPT is not able to update the KVM variable setting when using the configuration file. **Workaround:** Update the KVM variable setting individually with Intel® FPT on the command line. **Notes:**	Corp

Issue #	Description	Details	Found in Kit # Affected Sku's
1805492454	Intel® FIT tool not aligned with current list of available GPIOs for Intel® Percise Touch and Stylus.	**Affected Component –** sw.mfg_tools.fit **Impact:** Intel® FIT tool is not aligned with the current list of available GPIOs for Inte® Percise Touch and Stylus pin. **Workaround:** None. **Notes:**	All
1305357044	Delayed Authentication Mode not being enabled when SKU emulation is set to No Emulation.	**Affected Component –** sw.mfg_tools.fit **Impact:** Delayed Authentication Mode does not get enabled when SKU emlulation is set to No Emulation in the Intel® FIT tool. **Workaround:** Set SKU emulation in the image. **Notes:**	All
1305252544	Changing the length of IO Manageability Engine and Thnderbolt™ for the input binaries in the Intel® FIT tool does not have any affect.	**Affected Component –** sw.mfg_tools.fit **Impact:** Changing the region length IO Manageability Engine and Thnderbolt™ in the Intel® FIT tool does not have any affect. This could potentially allow region length sizes smaller than the input binaries. **Workaround:** Leave region length settings at default. **Notes:**	All
1305271750	Intel® ME writes the wrong value for the firmware version to the IOM Engine status registers.	**Affected Component –** fw.ip_loading.tcss **Impact:** Incorrect firmware version for gets populated into IOM status registers for IOM, MG and TBT. **Workaround:** None. **Notes:**	All
1305386508	Powergating exit failing on ICL-U platforms.	**Affected Component –** fw.os.crypto **Impact:** ICL-U platform will fail to properly from exit powergating. **Workaround:** None. **Notes:**	All

Issue #	Description	Details	Found in Kit # Affected Sku's
1406524128	Unable to enter MEBx when using OEM based BIOS.	**Affected Component –** fw.amt.provisioning **Impact:** The user will be unable to enter the MEBx when using OEM specific BIOS implementations. **Workaround:** None. **Notes:**	Corp

10.34 Kit 13.0.0.7040

Issue #	Description	Details	Found in Kit # Affected Sku's
1305006937	Deep S5 Entry fails during transitioning G3\Moff->S5\CMoff.	**Affected Component –** fw.pm.maestro **Impact:** When going from G3: after running from Simics console **icl.mb.sb.power_supply->signals_SLP_SUS,** the value is 0x1. system state: S5\CMoff. **Workaround:** None. **Notes:**	All
1305243967	Intel® FIT tool needs to removed the "Disabled" option from SATA/PCIe Combo ports.	**Affected Component –** sw.mfg_tools.fit **Impact:** Setting the Disable option for the SATA/PCIe Combo ports could cause hangs. **Workaround:** None. **Notes:**	All
1406442837	Intel® ME firmware fails to use WebUI via Wired LAN on ICPLP-A0 silicon.	**Affected Component –** fw.amt.web_storage **Impact:** Cannot use WebUI while Management console could send ping to SUT with Windows OS. **Workaround:** None. **Notes:**	Corp
1305252492	Intel® FIT CLI mode building image without Thunderbolt binary present in the final output when using –tbt command line option.	**Affected Component –** sw.mfg_tools.fit **Impact:** Intel® FIT CLI mode not merging the Thunderbot binary when specified using the –TBT command line option. **Workaround:** Use Intel® FIT GUI mode. **Notes:**	All

Issue #	Description	Details	Found in Kit # Affected Sku's
1305282309	The Intel® FPT tool shows CVARs which were not updated along those which were updated when using –verbose command line option.	**Affected Component –** sw.mfg_tools.fpt **Impact:** Intel® FPT tool is showing CVARs which were not set along with those which were set in output information with –verbose option. **Workaround:** None. **Notes:**	All
1805166492	Intel® ME firmware sporadically fails to load when running with audio package.	**Affected Component –** fw.ip.loading.adsp **Impact:** Sporadic failures seen when running audio package. **Workaround:** None. **Notes:**	All

10.35 Kit 13.0.0.7033

Issue #	Description	Details	Found in Kit # Affected Sku's
1305252492 1305259838	Thunderbolt™ not being incorporated in output image when using Intel® FIT in CLI mode with –tbt switch option. Also failing in GUI mode.	**Affected Component –** sw.mfg_tools.fit **Impact:** Intel® FIT CLI and GUI modes not properly integrating Thunderbolt™ binary into final image. **Workaround:** None. **Notes:**	All
1305254311	Updating user consent language fails as expected when FWU client is busy, but no failure event appears.	**Affected Component –** sw.amt.imss **Impact:** No indication of an error is given to the user if FWU client is busy when consent language change in done. **Workaround:** Retry consent language change again. **Notes:**	Corp
1406356340	Early DBC not working currently on Ice Lake.	**Affected Component –** fw.rbe **Impact:** Early DBC debugging not currently working. **Workaround:** None. **Notes:**	All

Issue #	Description	Details	Found in Kit # Affected Sku's
1805166492	Intel® ME Firmware Sporadically fails to load when running with audio package.	**Affected Component –** fw.ip_loading.adsp **Impact:** Intel® ME Firmware sporadically not load when the audio package is being used. **Workaround:** None. **Notes:**	All

10.36 Kit 13.0.0.7029

Issue #	Description	Details	Found in Kit # Affected Sku's
1305113016	Intel® FIT tool allowing image to be built without PMC patch binary.	**Affected Component –** sw.mfg_tools.fit **Impact:** By allowing an image to be built without PMC present would get platforms into a potential no boot scenario. **Workaround:** When building the image make sure that the PMC patch binary is loaded in the Intel® FIT tool. **Notes:**	All
1305137868	MEU doesn't calculate 'partition hash' value in file manifest. (this hash value is checked only in firmware update flow).	**Affected Component** – sw.mfg_tools.meu **Impact:** As a result of this bug, partition files that get generated using earlier versions of MEU (like IOMP, MGPP, TBTP) have hash value = 0. This will prevent firmware update from working properly. **Workaround:** Use updated MEU tool. **Notes:**	All
1305155421	Incorrect hardware Product Family and ICC hardware SKU returned by ICC GetClockCapability API.	**Affected Component** – sw.icc.cct **Impact:** CCT tool incorrectly showing the wrong product family in console display output. **Workaround:** None. **Notes:**	All

Issue #	Description	Details	Found in Kit # Affected Sku's
1305166669	Intel® FPT tool will return the wrong error when reading corporate only CVARs on when running on consumer firmware.	**Affected Component** – sw.mfg_tools.fpt **Impact:** Intel® FPT returing the wrong error response code when using –r All command to list CVARs. **Workaround:** None. **Notes:**	Cons
1305174421	No TLS ISO support on Consumer images.	**Affected Component –** fw.sku.sku_manager **Impact:** TLS disabled in consumer images. **Workaround:** None **Notes:**	Cons
1305166732	The Intel® FPT -R command when used with All argument will not read RCFG CVAR.	**Affected Component –** sw.mfg_tools.fpt **Impact:** Intel® FPT tool not returning the value for RCFG CVAR when –R command is used with All modifier. **Workaround:** Use –R command with RCFG CVAR to retrieve current value. **Notes:**	All
1305146885	Intel® Fwupdlcl tool not working on Icelake platforms.	**Affected Component –** sw.mfg_tools.fw_update **Impact:** Firmware updates currently not possible on Icelake. **Workaround:** None. **Notes:**	All
1305188452	Intel® FIT shows wrong Intel® ME version (Major Version and Minor Version).	**Affected Component –** sw.mfg_tools.fit **Impact:** Intel® FIT tool currently not returing correct Intel® ME versioning. **Workaround:** None. **Notes:**	All
1305201452	Intel® FIT tool fails to decompose images from kit.	**Affected Component –** sw.mfg_tools.fit **Impact:** Intel® FIT tool not able to decompose images from FW kit release. **Workaround:** None. **Notes:**	All

Issue #	Description	Details	Found in Kit # Affected Sku's
1305225946	Intel® FIT does not provide command line specifier for ISH and -w option fails.	**Affected Component –** sw.mfg_tools.fit **Impact:** Intel® FIT tool doesn't accept a command line parameter for path to ISH binaries like it does for most of the other binaries. **Workaround:** None. **Notes:**	Corp / Cons
1305228761	TCSS causing hangs during boot.	**Affected Component –** fw.ip_loading.tcss **Impact:** Unable to boot with TCSS enabled. **Workaround:** None. **Notes:**	Corp / Cons

10.37 Kit 13.0.0.7021

Issue #	Description	Details	Found in Kit # Affected Sku's
1209715402	Incorrect Strap offsets used by FIT tool version 7008 for USB related straps	**Affected Component:** **sw.mfg_tools.fit** **sw.mfg_tools.fpt** **sw.mfg_tools.ftool** **sw.mfg_tools.fw_update** **sw.mfg_tools.manuf** **sw.mfg_tools.meu** **sw.mfg_tools.info**	Cons
1209742769	FIT is using wrong GPIO lines for iTouch SPI bus configuration on ICP	**Affected Component:** **io_drivers.gpiofw.itouch.sensor sw.mfg_tools.fit** **sw.mfg_tools.fpt** **sw.mfg_tools.ftool** **sw.mfg_tools.fw_update** **sw.mfg_tools.info** **sw.mfg_tools.manuf** **sw.mfg_tools.meu**	Corp / Cons
1304849953	ISH aliveness test fails in lite sku with simics version ww4 5.0.81	**Affected Component:** **sw.ip_loading.ish**	Cons
1304949577	TCSS loading flow can be called before DID and fail	**Affected Component:** **fw.ip_loading.tcss** **fw.pm.maestro**	Corp / Cons

Issue #	Description	Details	Found in Kit # Affected Sku's
1305033881	RBE code doesn't handle UEP in case of FPGA build - causing FW Update to fail on ICL HFPGA	**Affected Component: fw.rbe**	Corp / Cons
1305035678	All susram files don't survive global reset	**Affected Component: fw.os.vfs**	Cons
1304985204	Missing PFW file for ME13.0 in LMS folder blocking WCOD and LOCL updates by IMSS	**Affected Component: ip.system.build.product**	Corp
1305041510	FIT is not aligned to ICL UEP - this blocks FPF automation scripts for all projects	**Affected Component: sw.mfg_tools.fit**	Corp / Cons

11 Archive - Intel® CSME RCR's

RCR #	Change Info	Implemented in Kit#
1806776879	**Description:** Intel® CSME size increase by 400KB. **Background:** There is no remaining buffer size for Intel® CSME 13.x for post PV issues and Security fixes.	13.0.0.1051
1405745543	**Description**: Certify Intel® PTT to FIPS 140-2 Level 1 Standard. **Background**: Prior generations Intel® PTT did not support FIPS 140-2 Level 1. This prevented Intel® PTT from being certified. In addition to missing the certification OEMs were not able to provide Intel® PTT for secure accounts (i.e. Government).	13.0.0.1040
1305720367	**Description**: Remove automatic activation of DAM as a result of connecting CCA. **Background**: DAM allows to make system ready for debugging while authentication of the user can happen at any time. DAM is useful for Run Control debugging, but it changes behavior of multiple components in CSE FW. For better support of debugging the customers' platfroms returned by he end users DAM is activated automatically on CCA connection.	13.0.0.1033
1305613719	**Description**: Remove System Integrator ID. **Background**: No longer required for functionality by iCLS and DAL.	13.0.0.1033
1305559706	**Description**: ICC to consume the PCH configuration data from a new Sub-Partition. **Background**: On generations prior to Ice Lake the ICC data was contained within the Intel® CSME binary. Due to this tight coupling anytime ICC data had to be updated it required a new Intel® CSME release to customers when only ICC data was being changed.	13.0.0.1030
1806178366	**Description**: Redesign and simplify the external firmware update API Library. **Background**: Intel® CSME is providing to OEMs a FW Update Library (SW Lib) that contains external API. OEMs are using the external API to write their own FW Update Tool. The implementation of the API is very complicated and not easy to use.	13.0.0.1030
1406385434	**Description:** Manufacturing Tools to report unique error codes for system errorlevel events. **Background:** When Manufacturing Tools report an error, system ERRORLEVEL only shows 0x1. The requested change it to add error handling logic to programmatically respond to Manufacturing Tools errors with meaningful unique error codes sent to system ERRORLEVEL.	13.0.0.1027

RCR #	Change Info	Implemented in Kit#
1305613719	**Description:** Remove System Integrator ID settings. **Background:** System Integrator ID settings are not longer required for CLS and DAL services.	13.0.0.1027
1305559706	**Description:** ICC to consume the PCH configuration data from a new Sub-Partition. **Background:** PCH settings programming is being done by CSE. The problem is that CSE architecture team does not control this content the PCH architects dictate what to program and how, but CSE has handle this.	13.0.0.1026
1305122001	**Description:** Add new Intel® MEManuf test to check whether any firmware fatal error logs exist. **Background:** Provide a way for customers to determine if there are any firmware fatal errors present in the Intel® CSE data partition for error logging.	13.0.0.1026
1406385434	**Description:** Manufacturing tools to report unique errorlevels back to the OS that reflect the actual error that occured. **Background:** When Manufactuing Tools report errors back to the system the ERRORLEVEL returned is always 0x1 regardless of the actual error that occurs.	13.0.0.1007
1406374555	**Description:** Firmware updated to comprehend mux-select for Gen4 Capable SRC buffers clock source. **Background:** Current definition of Gen4Strap is not sufficient for iSClk to comprehend SRC buffers. iSClk needs muxselects definition to support Gen4Platform.	13.0.0.1007