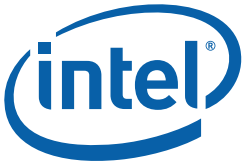

Intel® 6 Series Express Chipset - Intel® Management Engine 7.0

1.5MB Firmware Release Notes

Release 7.0.0.1135 – Production Version (PV) Release

October 2010

Intel Confidential

Contents

Revision History

Revision Number	Description	Revision Date
7.0.0.1012	Pre-Alpha Release	March 2010
7.0.0.1019	Alpha1 Release	March 2010
7.0.0.1041	Alpha2 Release	May 2010
7.0.0.1061	Beta Release	July 2010
7.0.0.1090	Engineering Release	August 2010
7.0.0.1115	Production Candidate (PC) Release	September 2010
7.0.0.1121	Production Candidate 2 (PC2) Release	October 2010
7.0.0.1135	Production Candidate 3 (PC3) Release	October 2010
7.0.0.1135	Production Version (PV) Release	October 2010

§

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
CRB	Customer Reference Board
FITC	Flash Image Tool
FOV	Fixed Offset Variable
FW	Firmware
GbE	Gigabit Ethernet
HECI	Host Embedded Controller Interface. Same as Intel® MEI.
ICC	Integrated Clock Control
IMSS	Intel® Management and Security Status Application
Intel® AMT	Intel® Active Management Technology
Intel® AT	Intel® Anti-Theft Technology
Intel® MEI	Intel® Management Engine Interface (interface between the Management Engine and the Host system)
KVM	Keyboard, Video, Mouse
LAN	Local Area Network
LMS	Local Manageability Service
MRC	Memory Reference Code
OS	Operating System
PAVP	Protected Audio and Video Path
PCH	Platform Controller Hub
SKU	Stock Keeping Unit
SOL	Serial over LAN
SPI	Serial Peripheral Interface
UMA	Unified Memory Architecture

2 Release Kit Summary

This document covers the following Intel® Management Engine 7.0 Firmware SKU for the Cougar Point based platforms:

- 1.5MB FW SKU

Note: The Intel® ME Firmware 7.0 SKU - 1.5MB Firmware does NOT support Intel® Active Management Technology (Intel® AMT) and Intel® Management Engine BIOS Extension (Intel® MEBx) features. Please ignore any references to AMT and MEBx in this document.

2.1 Release Kit Details

Release Name : Intel® Management Engine Firmware 7.0 SKU - 1.5MB FW (4MB SPI) Production Version (PV) Release - 7.0.0.1135

* **Target Platform** : Sandy Bridge CPU & Cougar Point PCH based platform

* **.zip name** : CPT_1.5M_7.0.0.1135_PV.zip

Contents:

- Intel® Management Engine Firmware (for Cougar Point Series Chipset Family /PCH platform)
- GbE PCH SPI components
- Intel Reference System BIOS
- System Tools (for creating an image and programming this image into the flash device)
- Supported drivers and applications

2.2 Kit Dashboard

Items or steppings not listed in the following table mean that they aren't supported for this firmware release.

Component	Description	
Intel® ME FW Kit	This kit is intended for PV level customer validation with Intel® ME FW for Cougar Point based platforms.	
Supported Manageability Power States	☒ S0/M0 (Power Package 1/2) ☐ S3/M3 (Power Package 2) ☐ S4/M3 (Power Package 2)	☐ S5/M3 (Power Package 2) ☒ Sx/Moff (Power Package 1)
Supported Processors	Desktop ☒ Sandy Bridge pre-ES2 (C0) ☒ Sandy Bridge ES2 (D0) ☒ Sandy Bridge QS (D1)	Mobile ☒ Sandy Bridge pre-ES2 (C0) ☒ Sandy Bridge ES2 (D0) ☒ Sandy Bridge QS (D1)
Supported PCHs	Desktop ☒ Cougar Point preES2/ES2 (B0) ☒ Cougar Point preQS (B1) ☒ Cougar Point QS (B2)	Mobile ☒ Cougar Point preES2/ES2 (B0) ☒ Cougar Point preQS (B1) ☒ Cougar Point QS (B2)
Supported Intel® LAN PHYs	☒ 82579 (Lewisville) ES2 (A2) ☒ 82579 (Lewisville) QS (C0)	
Supported Intel® Wireless LAN NICs	☒ Intel® Centrino® Ultimate-N 6300 AGN (Puma Peak 3x3) QS ☒ Intel® Centrino® Advanced-N 6250 AGN (Kilmer Peak 2x2) QS ☒ Intel® Centrino® Advanced-N 6205 (Taylor Peak) QS ☒ Intel® Centrino® Advanced-N 6230 (Rainbow Peak 2) ES1	
Applications	☐ Intel® AMT ☒ Silicon Workaround Capability (SWC) ☒ Integrated Clock Control (ICC) ☒ Thermal Reporting (TR)	☐ KVM ☒ Configuration Feature (CF) ☒ Intel® Anti-Theft Technology ☒ PAVP
Tools	☐ AMT Config Tool ☒ Clock Commander Tool (CCT) for ICC ☐ IUSManuf Tool ☒ Flash Image Tool (FITC/Wizard) ☒ Flash Programming Tool (FPT, FPTW) ☒ Intel® ME Debug Tool* ☒ Intel® ME Test Suite (METS)* ☒ Intel® Automated Power Switch (APS)*	☒ FWUpdate (FWUpdLcl) ☒ MEInfo ☒ MEManuf ☐ UpdParam Tool ☐ Intel® TXT Compliance* ☐ Intel® VT-d Firmware Toolkit*

Note: *available in Intel® ME Compliance and Debug Kit release

2.3 Kit Overview

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

Note: Users require an activated account for contents access and download.

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(s).
4. The Supporting Documentation folder under the selected component contains the following documentation:
   a. 1.5MB 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 release.
   b. BIOS Release Notes – This document provides details of BIOS issues resolved with this release.
5. Click on the Installation Files folder under the selected component and extract the .zip kit into a folder (Example: C:\)

2.4 Contents of Downloaded Kit

Note: The Intel® ME Firmware 7.0 SKU - 1.5MB Firmware does NOT support Intel® Active Management Technology (Intel® AMT) and Intel® Management Engine BIOS Extension (Intel® MEBx) features. Please ignore any references to AMT and MEBx in this document.

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

2.4.1 Intel® ME SW Components

Installers	Description
ME_SW	• Intel® MEI is the interface between the host and the Intel® Management Engine firmware. • Drivers and applications on the host that wish to interact with Intel® Management Engine through the host interface use the Intel® MEI host Windows* driver. • Intel® ME SW Components are installed by running: C:\CPT_1.5M_7.0.0.xxxx\Installers\ME_SW\Setup.exe
ME_SW_IS	• The ME_SW_IS installer will install the same components as ME_SW but using an InstallShield* wrapper.

2.4.2 Image Components Directory

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

Directory	Description
BIOS	• Contains BIOS image for Intel Customer Reference Board (CRB) • supports both desktop and mobile Cougar Point PCH based platforms • After flashing a new BIOS, enter BIOS setup and 'Restore Defaults' (Press F3). Then 'Save Changes and Exit' (Press F4). This is a required step when updating to a new BIOS release. • For latest release information and known issues, refer to the *BIOS ReleaseNotes_CPT*
ME	• The Intel® Management Engine firmware contains code and configuration data for Intel® Management Engine functions.
GbE	• The GbE hardware (LAN) is a component embedded in the PCH. GbE region of the flash contains bits that define the configuration of the GbE hardware. • Example: NAHUM5_LEWISVILLE_VPRO_05.bin. This image can be used with any of the Intel® Management Engine images.

2.4.3 Tools Directory

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

Tool	Description
Flash Image Tool – fitc.exe	• Used to assemble and configure the different elements of the SPI Flash (Descriptor, Intel Reference System BIOS, Intel® Management Engine firmware, Gigabit Ethernet (GbE) into a single Flash image
Flash Programming Tool – fpt.exe, fptw.exe and fptw64.exe	• Used to program the Flash image into the SPI Flash device(s)

Tool	Description
FWUpdate – FWUpdLcl Tools	• Used to update the Intel® Management Engine's firmware
MEInfo	• Verifies that Intel® Management Engine (Intel® ME) firmware is alive and returns data about Intel® ME
MEManuf	• Used on the manufacturing line to validate Intel® Management Engine functionality
Clock Commander Tool (CCT)	• ICC Tool to get ICC registers and settings, see *ICC Tools User Guide* for more information

2.5 Release Version Numbering Information

Typical release version numbering is as follows,

7.x.y.z (for example: 7.0.0.1041)

where

'7' refers to the Intel® Management Engine 7.0 Firmware SKU for the Cougar Point based platforms

'x' represents point releases such as 7.1 where new features or changes to existing features may be added

'y' refers to Maintenance and Hot Fix release designations

'z' refers to firmware release revision

3 Important Notes

This **Production Version (PV) Release** firmware supports 1.5MB Consumer SKU platforms.

- All Moff Power flows (PP1) – Supported
- Intel® Anti-Theft Technology – Supported
- BLU-RAY* PLAYBACK - Supported

3.1 Firmware Issue Fixed in 1.5MB FW PC3 Release

There is a firmware issue that impacts Intel® Anti-Theft Technology (Intel® AT). An API that is used during manufacturing process is left accessible to end users and may allow an end user to send a command to the Intel ® Management Engine (ME) to keep the ME in a reset state which may prevent enforcement of the Intel® AT feature. The 1.5MB Firmware has been changed to disable this API once the platform completes the manufacturing process. This fix will be released as a Production Candidate 3 today. The official Production Version (PV) Firmware will be released on ww41.4. Because Intel does not anticipate further changes between PC3 and PV, customers may begin their final regression testing now on PC3 to ensure they have the most time to check out the firmware in advance of QC RTS.

3.2 1.5MB FW Production Candidate 2 will be Released

The Intel® Management Engine Firmware 7.0 SKU 1.5MB Production Candidate 2 for Huron River and Sugar Bay platforms will be released ww40.5. The only FW change implemented is to allow improved communication between the Cougarpoint PCH and the Lewisville PHY for PHY initialization. Without this change, there have been cases where during initialization the Lewisville PHY may not be properly configured. The LAN driver then may not load and will result in a yellow bang on the LAN device in the OS Device Manager. Customers should focus on the following areas when testing with this Firmware:

- Basic S5 to S0 power flows: focusing on WOL from S5
- OS based warm reset and cold reset

Intel is still currently planning on releasing the 1.5MB PV Firmware on WW41.3 (Oct 6).

3.3 Production and Non-Production FW Support

Running Production FW (**CPT_1.5M_Production.BIN**) on Super SKU PCH is now a supported configuration. Thus, Production FW now supports all of the following Cougar Point PCH steppings:

- Fused CPT QS (B1/B2)
- Unfused CPT pre-QS (B1 Super SKU)
- Unfused CPT ES2 (B0 Super SKU)

For PAVP Testing, you must match Production FW with Production Part and Non Production FW with Non Production Parts.

3.4 Deep Sx support on Desktop and Mobile

Deep S4/5 will not be supported in AC mode or AC+DC mode for Mobile Huron River Platforms; deep sleep is supported in DC mode only. Desktop support for Deep S4/5 remains unchanged.

- Reference the WW12_2010_HuronRiver_MoW.pdf for more details – CDI Doc#436996
- CRB BIOS Release 14, included in ME FW kits, does not gray out Deep S4/5 AC mode capability on mobile CRB. This option will be properly removed in future CRB BIOS releases
- There is a known bug in DC mode when power button is pressed from DOS mode, see section 5.1 Issue# 3534647 for more information
- Users must be sure they are using Latest Intel KSC (1.11) when using Intel CRBs.

3.5 CRB BIOS Notes

1. If the system is failing S3 or S4 with integrated graphics display (IGD), try disabling RC6 in the following BIOS setup menu:
   - “Advanced” -> “Power & Performance” -> “GT - Power Management Control" -> "RC6(Render Standby)" = Disabled
2. If Los Lunas Desktop CRB boards fail to boot with multiple USB devices attached, try reducing the number of USB devices attached or reduce it down to 1 device only.
3. Please refer to the BIOS release notes for other general BIOS updates.

3.6 Intel® HD Graphics Driver Requirement

This Release (7.0.0.1135) must use the latest Intel® HD Graphics Driver:

- **Release Name: Intel® HD Graphics Driver Production Version 15.21.0.2219 (VIP Kit# 28099)**
- **Release Name: Intel® HD Graphics Driver Production Version 15.21.64.2219 (VIP Kit# 28100)**

3.7 No video after image flash when changing from C0 to D0 CPU

- With D0 SNB CPU, no IGD observed during system boot. There is a potential problem at customer testing labs if IGD is not displaying to the screen when replacing the CPU to D0 (or later).
- In order to avoid this issue, after installing the CPU D0 (or later), Intel ME needs one good boot (i.e. Intel ME should be enabled) in order for Intel ME to generate a warm reset.

3.8 Intel® LAN Binary Images

Intel® ME 7.0 PC FW kit contains two GbE binaries:

NAHUM5_LEWISVILLE_DESKTOP_13.bin supports Intel® LAN PHY A2 and B0 only. This image is recommended for testing power flows with connectivity. This image is for desktop platforms only.

NAHUM5_LEWISVILLE_MOBILE_13.bin supports Intel® LAN PHY A2 and B0 only. This image is recommended for testing power flows with connectivity. This image is for mobile platforms only.

3.9 FITc Wizard

If you are using Remote Configuration in your testing environment you need to use FITc instead of the Wizard to build you images. See Section 6.3 for further details.

Changes between the Beta 7.0.0.1061 newfiletmpl.xml and PV 7.0.0.1135 newfiletmpl.xml	
Beta 7.0.0.1061 newfiletmpl.xml	**PV 7.0.0.1135 newfiletmpl.xml**
<ftoolRoot version="2**2**">	<ftoolRoot version="2**5**">
<ProcStrapLength value="**0**" edit="false" visible="true" name="Number of PROC straps" help_text="The number of PROC straps to be read. Valid values are 0 to 1."/>	<ProcStrapLength value="**1**" edit="false" visible="true" name="Number of PROC straps" help_text="The number of PROC straps to be read. Valid values are 0 to 1."/>
<**Link**SecDisable value="true" edit="false" visible="true" name="**LinkS**ec Disable" help_text="**LinkS**ec is a hop-by-hop network security solution. It provides Layer 2 encryption and authenticity/integrity protection for packets traveling between **LinkS**ec-enabled nodes of the network."/>	<**Mac**SecDisable value="true" edit="false" visible="true" name="**MACs**ec Disable" help_text="**MACs**ec is a hop-by-hop network security solution. It provides Layer 2 encryption and authenticity/integrity protection for packets traveling between **MACs**ec-enabled nodes of the network."/>
<SmBusMctpAddr value="0x**00**" edit="true" visible="true" name="Intel (R) ME SMBus MCTP Address" help_text="This address is used by Intel (R) ME Anti-Theft Technology FW."/>	<SmBusMctpAddr value="0x**2B**" edit="true" visible="true" name="Intel (R) ME SMBus MCTP Address" help_text="This address is used by Intel (R) ME Anti-Theft Technology FW."/>
<PCIeLaneReversal1 value="false" edit="true" visible="true" name="PCIe Lane Reversal 1" help_text="**PCIe Lane Reversal 1**"/>	<PCIeLaneReversal1 value="false" edit="true" visible="true" name="PCIe Lane Reversal 1" help_text="**This bit lane reversal behavior for PCIe* Port 1 if configured as a x4 PCIe port. false = PCIe Lanes 0-3 are not reversed. true = PCIe Lanes 0-3 are reversed when Port 1 is configured as a 1x4.**"/>
<PCIeLaneReversal2 value="false" edit="true" visible="true" name="PCIe Lane Reversal 2" help_text="This bit **sets the default value for the PCIe Port 5, Device 28 Function 0, offset D8[27] register. false = PCIe Lanes 4-7 are NOT reserved. true = PCIe Lanes 4-7 are reserved** when Port 5 is configured as a 1x4."/>	<PCIeLaneReversal2 value="false" edit="true" visible="true" name="PCIe Lane Reversal 2" help_text="This bit **lane reversal behavior for PCIe Port 5 if configured as a x4 PCIe* port. false = PCIe Lanes 4-7 are not reversed. true = PCIe Lanes 4-7 are reversed** when Port 5 is configured as a 1x4."/>

Changes between the Beta 7.0.0.1061 newfiletmpl.xml and PV 7.0.0.1135 newfiletmpl.xml	
Beta 7.0.0.1061 newfiletmpl.xml	**PV 7.0.0.1135 newfiletmpl.xml**
<ProcMissing value="No onboard glue logic" value_list="No onboard glue logic,,Glue logic tied to GPIO**30,,Glue logic tied to GPIO28**" edit="false" visible="true" name="PROC_MISSING" help_text="This value will determine if there is glue logic present on the platform to detect a missing processor on desktop platforms."/>	<ProcMissing value="No onboard glue logic" value_list="No onboard glue logic,,Glue logic tied to GPIO**24**" edit="false" visible="true" name="PROC_MISSING" help_text="This value will determine if there is glue logic present on the platform to detect a missing processor on desktop platforms."/>
<ManageAppPerm value="No" value_list="No,,Yes" edit="true" visible="true" name="Manageability Application Permanently Disabled?" help_text="Setting this to Yes permanently disables Intel (R) AMT, Intel (R) Standard Manageability, **Intel (R) RPAT B, Intel (R) RPAT C** and KVM."/>	<ManageAppPerm value="No" value_list="No,,Yes" edit="true" visible="true" name="Manageability Application Permanently Disabled?" help_text="Setting this to Yes permanently disables Intel (R) AMT, Intel (R) Standard Manageability, and KVM."/>
<PavPerm value="No" value_list="No,,Yes" edit="true" visible="true" name="PAVP **2.0** Permanently Disabled?" help_text="Select whether Protected Audio Video Path (PAVP) **2.0** is permanently disabled."/>	<PavPerm value="No" value_list="No,,Yes" edit="true" visible="true" name="PAVP Permanently Disabled?" help_text="Select whether Protected Audio Video Path (PAVP) is permanently disabled."/>
<MctpInfo3G value="0x**00**" edit="true" visible="true" name="MCTP Info 3G" help_text="Defines the 7-bits MCTP address of the 3G NIC card on ME SMBus. This value is needed if there is a 3G NIC card working with Intel AT."/>	<MctpInfo3G value="0x**32**" edit="true" visible="true" name="MCTP Info 3G" help_text="Defines the 7-bits MCTP address of the 3G NIC card on ME SMBus. This value is needed if there is a 3G NIC card working with Intel AT."/>
<RpatEnablerId value="00000000-0000-0000-0000-000000000000" edit="true" visible="true" name="Remote PC Assist Technology Enabler ID" help_text="Unique numeric ID of the party which enabled the service in manufacturing."/>	blank
<RpatEnablerName value="" edit="true" visible="true" name="Remote PC Assist Technology Enabler Name" help_text="Description of the party which enabled the service in manufacturing. Maximum length of 60 characters."/>	blank
<RpatHwButton value="0x01" value_list="0x01,,0x02" edit="true" visible="true" name="Remote PC Assist Technology HW Button" help_text="0x01 = Chassis Intrusion. 0x02 = RCS Trigger."/>	blank

Changes between the Beta 7.0.0.1061 newfiletmpl.xml and PV 7.0.0.1135 newfiletmpl.xml	
Beta 7.0.0.1061 newfiletmpl.xml	**PV 7.0.0.1135 newfiletmpl.xml**
<Hash0>	<Hash0 **name="Hash 0"**>
<Active value="**false**" edit="true" visible="true" name="Hash 0 Active" help_text="false = Not Active true = Active"/>	<Active value="**true**" edit="true" visible="true" name="Hash 0 Active" help_text="false = Not Active true = Active"/>
<FriendlyName value="" edit="true" visible="true" name="Hash 0 Friendly Name" help_text="Enter Hash Name. Maximum of 32 characters."/>	blank
<Stream value="" edit="true" visible="true" name="Hash 0 Stream" help_text="Enter raw hash string or certificate file."/>	blank
<Hash1>	<Hash1 **name="Hash 1"**>
<Active value="**false**" edit="true" visible="true" name="Hash 1 Active" help_text="false = Not Active true = Active"/>	<Active value="**true**" edit="true" visible="true" name="Hash 1 Active" help_text="false = Not Active true = Active"/>
<FriendlyName value="" edit="true" visible="true" name="Hash 1 Friendly Name" help_text="Enter Hash Name. Maximum of 32 characters."/>	blank
<Stream value="" edit="true" visible="true" name="Hash 1 Stream" help_text="Enter raw hash string or certificate file."/>	blank
<Hash2>	<Hash2 **name="Hash 2"**>
<Active value="**false**" edit="true" visible="true" name="Hash 2 Active" help_text="false = Not Active true = Active"/>	<Active value="**true**" edit="true" visible="true" name="Hash 2 Active" help_text="false = Not Active true = Active"/>
<FriendlyName value="" edit="true" visible="true" name="Hash 2 Friendly Name" help_text="Enter Hash Name. Maximum of 32 characters."/>	blank
<Stream value="" edit="true" visible="true" name="Hash 2 Stream" help_text="Enter raw hash string or certificate file."/>	blank
… repeat above pattern for Hash3 to Hash18	… repeat above pattern for Hash3 to Hash18

Changes between the Beta 7.0.0.1061 newfiletmpl.xml and PV 7.0.0.1135 newfiletmpl.xml	
Beta 7.0.0.1061 newfiletmpl.xml	**PV 7.0.0.1135 newfiletmpl.xml**
<Hash19>	<Hash19 **name="OEM Default Certificate"**>
<Active value="false" edit="true" visible="true" name="**Hash 19** Active" help_text="false = Not Active true = Active"/>	<Active value="false" edit="true" visible="true" name="**OEM Default Certificate** Active" help_text="false = Not Active true = Active"/>
<FriendlyName value="" edit="true" visible="true" name="**Hash 19** Friendly Name" help_text="Enter Hash Name. Maximum of 32 characters."/>	<FriendlyName value="" edit="true" visible="true" name="**OEM Default Certificate** Friendly Name" help_text="Enter Hash Name. Maximum of 32 characters."/>
<Stream value="" edit="true" visible="true" name="**Hash 19** Stream" help_text="Enter raw hash string or certificate file."/>	<Stream value="" edit="true" visible="true" name="**OEM Default Certificate** Stream" help_text="Enter raw hash string or certificate file."/>
<Hash20>	<Hash20 **name="OEM Customizable Certificate 1"**>
<Active value="false" edit="true" visible="true" name="**Hash 20** Active" help_text="false = Not Active true = Active"/>	<Active value="false" edit="true" visible="true" name="**OEM Customizable Certificate 1** Active" help_text="false = Not Active true = Active"/>
<FriendlyName value="" edit="true" visible="true" name="**Hash 20** Friendly Name" help_text="Enter Hash Name. Maximum of 32 characters."/>	<FriendlyName value="" edit="true" visible="true" name="**OEM Customizable Certificate 1** Friendly Name" help_text="Enter Hash Name. Maximum of 32 characters."/>
<Stream value="" edit="true" visible="true" name="**Hash 20** Stream" help_text="Enter raw hash string or certificate file."/>	<Stream value="" edit="true" visible="true" name="**OEM Customizable Certificate 1** Stream" help_text="Enter raw hash string or certificate file."/>
… repeat above pattern for Hash21 to Hash22	… repeat above pattern for Hash21 to Hash22
blank	<Hash23 name="Hash 23"> <Active value="false" edit="true" visible="true" name="Hash 23 Active" help_text="false = Not Active true = Active"/> </Hash23>
… repeat above pattern for Hash24 to Hash32	… repeat above pattern for Hash24 to Hash32

Changes between the Beta 7.0.0.1061 newfiletmpl.xml and PV 7.0.0.1135 newfiletmpl.xml	
Beta 7.0.0.1061 newfiletmpl.xml	**PV 7.0.0.1135 newfiletmpl.xml**
<DBRCOM value="0x**080D0834**" edit="true" visible="false" name="DBRCOM" help_text="DBRCOM"/>	<DBRCOM value="0x**0E11175D**" edit="true" visible="false" name="DBRCOM" help_text="DBRCOM"/>
<PI12BiasParms value="0x08880888" edit="true" visible="**false**" name="PI12BiasParms" help_text="PI12BiasParms"/>	<PI12BiasParms value="0x08880888" edit="true" visible="**true**" name="PI12BiasParms" help_text="PI12BiasParms"/>
<SSC2OCPARMS value="0x00000000" edit="true" visible="**false**" name="SSC2OCPARMS" help_text="SSC2OCPARMS"/>	<SSC2OCPARMS value="0x00000000" edit="true" visible="**true**" name="SSC2OCPARMS" help_text="SSC2OCPARMS"/>

Note:

- For information on the values that need to be entered for the setup procedure below, please refer to the **Intel Cougar Point Chipset Family EDS** and the SPI flash's datasheet. Vendor ID, Device ID 0 and Device ID 1 are all derived from the output of the JEDEC ID command which can be found in the vendor datasheet for the specific SPI Flash part. In the Cougar Point EDS, **22.2.7.2 VSCC0—Vendor Specific Component Capabilities 0** describes the 32 bit VSCC register value.
- For access to the Intel Cougar Point Chipset Family EDS document, please contact your Intel representative.

Open the Flash image Tool (double-click on fitc.exe) and follow the steps below:

a. Under Descriptor Region node, right-click on VSCC Table, and select 'Add Table Entry…'
b. Enter an Entry name.
c. Add values for the fields: Vendor ID, Device ID 0, Device ID 1 and VSCC register value. These fields are with respect to the 'Entry Name' entered above in step b.

Please refer to the 1.5MB FW Bringup Guide.pdf for more details. This document is available in the downloaded kit.

4 Issue Status Definitions

These Release Notes provide information on sightings and bugs for Intel® Management Engine Firmware 7.0 SKU - 1.5MB FW release on the Intel® 6 Series Express Chipset (Cougar Point) based platform. This report includes information on new issues and the status of old issues.

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

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

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

Open Issues: New sightings and bugs are classified as "Open" issues until the fix has been verified with the appropriate firmware version. Open issues are separated into the following categories:

- **Open – Under Investigation:** All issues in this status are still under investigation. Issues may or may not be root caused.

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

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

5 Closed Issues

5.1 Closed - Intel® ME Kernel

Issue #	Description	Affected Component / Impact / Workaround / Notes	Fixed in Kit #
3553012	There is a firmware issue that impacts Intel® Anti-Theft Technology (Intel® AT). An API that is used during manufacturing process is left accessible to end users and may allow an end user to send a command to the Intel ® Management Engine (ME) to keep the ME in a reset state which may prevent enforcement of the Intel® AT feature. The 1.5MB Firmware has been changed to disable this API once the platform completes the manufacturing process.	**Affected Component:** FW.Kernel **Impact:** **Workaround:** none **Notes:**	7.0.0.1135
DCN # 1.00.00287	The Intel® Management Engine Firmware 7.0 SKU 1.5MB Production Candidate 2 for Huron River and Sugar Bay platforms will be released ww40.5. The only FW change implemented is to allow improved communication between the Cougarpoint PCH and the Lewisville PHY for PHY initialization. Without this change, there have been cases where during initialization the Lewisville PHY may not be properly configured. The LAN driver then may not load and will result in a yellow bang on the LAN device in the OS Device Manager.	**Affected Component:** FW **Impact:** **Workaround:** **Notes:** Replication Steps ---------- 1. Shutdown to S5, send Magic Packet, system does wake up, but then the LAN is shown as yellow bang on Device Manager 2. Shutdown to G3, then go back to S5, send Magic Packet or Power System with power button, LAN is shown as yellow bang on Device Manager Customers should focus on the following areas when testing with this Firmware: • Basic S5 to S0 power flows: focusing on WOL from S5 • OS based warm reset and cold reset	7.0.0.1121

Issue #	Description	Affected Component / Impact / Workaround / Notes	Fixed in Kit#
3551711	FW PM Causing global reset during FPT tool flashing in some cases	**Affected Component:** FW.Kernel.PowerManagement **Impact:** **Workaround:** **Notes:** Steps to Reproduce: Test Setup 1. HECI driver installed 2. ME disabled from MEBx Procedures - Verify "Chip Erase' option 1. fpt.exe -c 2. fpt.exe -f full_image.bin 3. Reboot System/G3 power cycle Actual Results: Using Win7 64bit OS, when flashing an Image to SUT after doing a chip erase SUT displays message stating it is going to disable ME then reboots.	7.0.0.1115
3551254	Notice to customers who are using one SPI part and plan to change Hyper Threading and Multi Core setting. ME asserts in SPI Driver when flash descriptor offset 0x200 is changed to 0x0000 0000	**Affected Component:** FW.Kernel.SPIDriver **Impact:** **Workaround:** none **Notes:** • For BIOS to be able to change Hyper threading and Multi Core setting on SNB CPUs, it is required to write 0x0000 0000 to descriptor offset 0x200 (see Huron River and SNB MoWs ww21). • When offset 0x200 is changed on a platform with one SPI component, it causes FW exceptions which cause FW to hang. • There is no workaround when using one SPI component. • Please contact your ME FW rep for any additional questions. Step to Reproduce: 1. Build HM57 image for 1.5MB platform with SPI components selected to 1 in FITC. 2. Modify offset 0x200 in hex editor to 0x0000 0000, 0x105 = 0x1, 0x1d =0x1. Although only changing 0x200 should be sufficient to reproduce the failure. This change is required for Hyper Threading and Cores to be setup correctly by BIOS. 3. FW will hang in BUP code on first boot if you are using REL image. If you are using DBG image you will hit assert in MFS code.	7.0.0.1061
3534647	Power Button press in DOS* OS causes reset to occur instead of power down, when Deep S4-S5 is enabled via soft-strap/BIOS policy	**Affected Component:** ExternalDependency **Impact:** **Workaround:** Avoid testing shutdown/S5 transition via power button testing in DOS*. Alternatively, to power down from DOS*, either use switch on power supply or remove power connection. **Notes:** When at the DOS prompt, with Deep S4-S5 enabled, pressing the power button will result in a reset instead of a power down to S5. This does not occur in Windows* OS.	7.0.0.1041

5.2 Closed - Integrated Clock Control (ICC)

Issue #	Description	Affected Component / Impact / Workaround / Notes	Fixed in Kit#
3552011	Boot timeout ICC recovery from extreme overclocking does not work.	**Affected Component** – FW.ICC **Impact:** Overclocking does not work properly when HT / Core disable capabilities are configured. **Workaround:** Configure image with HT / Core control disabled **Notes:** Reproduction Steps: 1. Build Overclocking config 2. Use CCDC tool to change BCLK to 120MHz for next boot 3. Reboot system	7.0.0.1115
3533845	After boot-timeout UOB record is not invalid. After writing UOB with incorrect DIVSET value, DUT stay at 0000 Post Code. After 15 sec, it restarts twice and then re-boot to OS. All registers are programmed to HW default. Also HECI interface has yellow bang and UOB record is still valid.	**Affected Component:** FW.ICC **Impact:** **Workaround:** **Notes:** Steps to Reproduce: ========== 1.Build image with registers set to OC values 2. Boot OS 3. Write UOB record (engage) with DIVSET register with clk2s set to 120MHz (e.g. DIVSET = 0x00455451) 4. Restart 5. DUT stay on 0000 code (15sec) 6. Restart twice 7. DUT boot OS Expected Results: UOB record should be invalid, registers should have OEM values, HECI should work Actual Results: Record is valid, and after next twice power flows boot-timeout is done; HECI doesn't work (yellow bang); registers have HW defaults How to recover from the failure: To get HECI interface back, need to perform G3 power cycle or clear CMOS.	7.0.0.1061
BUP000002	24-MHz and 25-MHz FLEX clock selections unavailable in Flash Image Tool GUI.	**Affected Component:** FW.ICC **Impact:** **Workaround:** The previous workaround is no longer available/necessary in FITC. **Resolution:** 24-, 25-, and 27-MHz Flex Clocks are available in FITC GUI and no workarounds are necessary.	7.0.0.1041

5.3 Closed - Software/Tools

Issue #	Description	Affected Component/Impact / Workaround/Notes	Fixed in Kit#
3552907	Memanuf SMBus Read Byte test fail intermittently	**Affected Component:** SW.Tools.MeManuf **Impact:** **Workaround:** none **Notes:** Steps to Reproduce: 1. Boot system to DOS 2. Run MEManuf -S0 -verbose 3. Check result 4. Repeat step 1,2,3 to get fail log	7.0.0.1115
3551844	"Common Services - MCTP" not included in MEManuf BIST on 1.5M SKU	**Affected Component:** FW.MCTP **Impact:** **Workaround:** none **Notes:** Steps to Reproduce: 1. Boot to DOS (1.5M SKU) 2. Run "memanuf -verbose"	7.0.0.1115
3535231	FW Update - FW Update usage is not clear about -F option	**Affected Component** – SW.Tools.FwUpdLcl **Impact:** Breaks backward compatibility usage model from previous generations. **Workaround:** use –f when updating firmware. **Notes:** Reproduction Steps: 1) Run FW Update tool (windows or Dos) without -F option.	7.0.0.1115
3535231	The FWUpdLcl tool fails when updating firmware if the optional '-F' command is not used.	**Affected Component** – SW.Tools.FwUpdLcl **Impact:** Breaks backward compatibility usage model from previous generations. **Workaround:** use –f when updating firmware. **Notes:** Reproduction Steps: 1) Run FW Update tool (windows or Dos) without -F option.	7.0.0.1115
2753005	FPT tool is able to use the '-erase' and the '-address' option in same command line argument.	**Affected Component** – SW.Tools.FlashProgrammingTool **Impact:** Unexpected behavior. FPT does not return an error as expected when these two options are combined. **Workaround:** Use the –erase and –address option separately **Notes:** Reproduction Steps: 1. Flash image onto platform: Default BIOS/ MEBx settings. Load all necessary drivers. 2. With FPT the following command:FPT.exe -erase -a 0x30000000 3. FPT.exe -greset	7.0.0.1115

Issue #	Description	Affected Component / Impact / Workaround / Notes	Fixed in Kit#
3551327	MEManuf testing shows failure in 'Common Services - General: Wireless enabled on mobile'	**Affected Component:** SW.Tools.MeManuf **Impact:** **Workaround:** none **Notes:** These errors happen on platforms that do not have a wireless card installed so these wireless tests should not be getting executed. Steps to Reproduce: 1. Build image with the FITc default WLAN Power Well Config setting 0x85 2. Flash image onto CRB 3. Boot to USB Key and run MEManuf 4. Run MEManuf - r -verbose CRB.txt to retrieve pass fail information.	7.0.0.1090
3551159	Windows FWUpdLcl crashes during FW update process	**Affected Component:** SW.Tools.FWUpdLcl **Impact:** leads to occasional Windows OS crash when using tool **Workaround:** none **Notes:** Steps to Reproduce: 1. Flash 1.5 MB FW 2. Activate ME network 3. Run FW update with software from another kit release	7.0.0.1090
3535324	FWUpdlcl bypassing user 'Y/N' prompt when performing firmware downgrades without the '-Y' auto accept command line option.	**Affected Component** – SW.Tools.FwUpdLcl **Impact:** Unexpected behavior. FWUpdlcl should prompt the user on firmware downgrade. **Workaround:** none **Notes:** Reproduction Steps: FW downgrade using HECI interface when configuring Manageability Feature Selection (MFS) to Enterprise Mode (Enter Y) 1. With current released FW in Flash 2. In MEBx, set Manageability Mode to None 3. Run MEINFO to verify FWUpdOverrideCounter is not equal to ZERO 4. fwupdlcl.exe -f previous_release_upd.bin <-generic> <-OEMID OEMID_FROM_FITC>	7.0.0.1090

Issue #	Description	Affected Component / Impact / Workaround / Notes	Fixed in Kit#
3535687 3536187	Attempting to set the MEManufacturingModeDone FOV results in this error: "Error 450: Invalid ME Manufacturing Mode Done value entered."	**Affected Component** – SW.Tools.FlashProgrammingTool **Impact:** Unexpected behavior. FPT returns an error with the MEManufacturingModeDone FOV. **Workaround:** none **Notes:** Reproduction steps: 1. Follow the current bring-up guide to build a ME image using FITC. 2. Flash via Dediprog/FPT > G3(unplug power) & Clear CMOS > Reapply Power > Boot to BIOS > Set following Parameters: 2a. Press F3 for Optimized Defaults 2b. Set SATA Mode = IDE [ADV > CONFIG > SATA CONFIG] 2c. F4 to Save and Exit 3. Boot to Windows 4. run FPTW.exe -u -n MEManufacturingModeDone -v 0x01	7.0.0.1061
3535658	In all messages from MEI driver in Source field using the 'HECI/HECIx64' used instead of 'Intel® MEI driver' in windows event viewer.	**Affected Component** – SW.HECI.Driver **Impact:** Incorrect designation being shown for the Intel® MEI driver in windows event viewer **Workaround:** none **Notes:** Reproduction steps: 1. Burn 7.0.0.1019 (Alpha1) image. 2. Clear CMOS. 3. Boot to OS 4. Generate any Intel® MEI message. (Disable/ enable device for ex.)	7.0.0.1061
3535548	When running FPT.exe -Commit the command returns in error. Error 524: Variables not updated by FW yet. Error 4: Error code 524 is unknown Commit Operation: Failed	**Affected Component** – SW.Tools.FlashProgrammingTool **Impact:** Unexpected behavior. The '-commit' command line option not working. **Workaround:** none **Notes:** Reproduction steps: 1. Boot to OS and flash latest kit 7.0.0.1019 (Alpha1) image 2. G-3 SUT 3. Boot to OS and execute FPT -U -ID 1 -V Admin@123 4. Execute FPT -commit and notice error.	7.0.0.1061
3535358	Using the -hashed option along with the FPT -r option for NVAR reading returns an error regarding an invalid parameter.	**Affected Component** – SW.Tools.FlashProgrammingTool **Impact:** Unexpected behavior. Using the –hashed command line option results in an error. **Workaround:** none **Notes:** Reproduction steps: 1. in DOS, run fpt.exe -r mebxpassword –hashed Dependency findings: ---------- -Without the -hashed option included, the command passes as normal	7.0.0.1061

Issue #	Description	Affected Component / Impact / Workaround / Notes	Fixed in Kit#
3535592	Running FPT.exe -f fullimg.bin will result in error of: Error 321: The Address 0x10000000 is outside the boundaries of flash area.	**Affected Component** – SW.Tools.FlashProgrammingTool **Impact:** FPT not able to flash across boundaries when two 8MB flash parts are used. **Workaround:** none **Notes:** Dependency findings: Happens on 16MB (8MB x 2) configuration. Reproduction Steps: 1. Flash 16MB (8MB x 2) image via Dediprog flashing utility 2. Boot system to DOS/FreeDOS 3. Execute FPT -F FullIMG.bin	7.0.0.1061
3535336	Using the FITC Wizard: Selecting Lane 1 or Lane 5 Reversed then selecting a different Lane Configuration leaves Lane Reversed set to true.	**Affected Component** – SW.Tools.FlashImageTool **Impact:** Unexpected behavior. Wizard leaving PCIe lane reversal set to true. **Workaround:** none **Notes:** Setup: ====== Open FITC, verify PCIe Lane Reversal 1 and 2 are set to false (PCH Strap 9) Use FITC Wizard Steps to Reproduce: ========== 1. Open Wizard, use working images and default values 2. On the DMI/PCIe Configuration page 2a. Select "1x4 - One 4 lane PCIe port" in the PCIe Lanes 1-4 section 2b. Check the box "PCIe Lane 1 Reversed" 2c. Select "1x2, 2x1 Port 1 (x2) Port 3(x2), Ports 2, 4 (disabled) 3. Build the image 4. Check PCH Strap 9 for PCIe Lane Reversal values	7.0.0.1061
3535266	When running FPT tools Win/DOS with -compare anyfile.txt the result is the same if the file is full of details or an empty file. Thus the tool reports that it has compared successfully to the file.	**Affected Component** – SW.Tools.FlashProgrammingTool **Impact:** Compare function does not function as expected and returns successful result regardless of file content. **Workaround:** none **Notes:** Reproduction Steps: 1. Boot to OS 2. Execute flash of current kit and driver installation 3. Execute FPT –vars. Verify that the vars list does go to standard output 4. Execute FPT -vars >> varslist.txt 5. Edit varslist.txt and remove all data from the file and save it as varedit.txt 6. Execute FPT –compare varedit.txt	7.0.0.1061

Issue #	Description	Affected Component / Impact / Workaround / Notes	Fixed in Kit#
3534157	FPT crashes with a Windows illegal operation error when using the following commands '-U -ID <invalid ID>' negative test case.	**Affected Component** – SW.Tools.FlashProgrammingTool **Impact:** **Workaround:** **Notes:** Reproduction Steps: 1. Flash image onto platform, Load default BIOS/MEBx settings. 2. Load latest MEI drivers. 3. Locate FPT –Win folder: fptw –u -id 112312312313 fullimage.bin	7.0.0.1061
3533932	FPT Tool fails to work under the WinPE 64 bits environment.	**Affected Component** – SW.Tools.FlashProgrammingTool **Impact:** FPT does not work in WinPE 64bit. **Workaround:** **Notes:** Reproduction Steps: while running fptw.exe on Windows PE 64bit including MEI driver, receive the below errors: - Windows PE 2.0 64bit with MEI driver fptw.exe -> Returned "The system cannot execute the specified program." error.	7.0.0.1061
2751665	When executing FPTw with the '-Commit' command switch an application error occurs and FPTw closes.	**Affected Component** – SW.Tools.FlashProgrammingTool **Impact:** FPTw crashes when the –Commit switch is used. **Workaround:** none. **Notes:** Reproduction Steps: 1. flash latest firmware to system 2. Load OS 3. Install Drivers 4. Reboot 5. Load command prompt to location of FPT-Win application 6. Create and modify FOV input file (fovslist5.txt). Change "Idle Timeout - ME" and "KVM settings" Enabled = 0x01 (Enable field in the fov file should be set to 1). 7. Change "Idle Timeout - ME" value and "KVM settings" value 8. fptw.exe -u -in fovslist5.txt 9. fptw.exe -commit	7.0.0.1061
3535030	MEManuf.exe -S4, for 1.5MB SKU expected outcome of test is supposed to display invalid option or error. System shuts off instead.	**Affected Component:** SW.Tools.MeManuf **Impact:** Low **Workaround:** None **Notes:**	7.0.0.1041

Issue #	Description	Affected Component / Impact / Workaround / Notes	Fixed in Kit#
3535052	Get error message (Unknown value found for Processor Emulation. Setting to "No Emulation") after configuring the value "EMULATE Intel vPro? capable Processor" to the parameter "Processor Emulation" and building image in FITC. Some languages do not support the extended ASCII set necessary for this to show the copyright and trademark symbols.	**Affected Component:** SW.Tools.FlashImageTool **Impact:** **Workaround:** Set PC to English language to use FITC to build Flash image **Notes:** Step to reproduce: 1. Execute FITC tool which is included in ME FW release kit. 2. Select QM67 SKU in FITC. 3. Open the option ME Region\Configuration\ME in FITC 4. Change the value of Parameter "Processor Emulation" to "EMULATE Intel vPro? Capable Processor". 5. Build image 6. An error message box will appear and show you the following error message (Unknown value found for Processor Emulation. Setting to "No Emulation")	7.0.0.1041

5.4 Closed - Intel® Anti-Theft Technology

Issue #	Description	Affected Component / Impact / Workaround / Notes	Fixed in Kit#
3535028	Once 3G WWAN NIC has been DISABLED using AT+CFUN=0, there's NO way of turning the NIC back ON unless a G3 is performed.	**Affected Component** – FW.TDT **Impact:** In such scenario, Bios recovery is impossible since ME cannot execute AT+CFUN=1 when InitializeNIC is issued by the Bios. **Workaround:** G3 **Notes:** Steps to Reproduce: N/A	7.0.0.1115
3551303	FW not reading FITC 'Heci Me Region Unlock' or 'Flash Protection Override' NVAR values	**Affected Component** – FW.TDT **Impact:** **Workaround:** none **Notes:** ME FW is not reading the FITC NVAR HECI ME Region Unlock value. Depending on this setting FW has to allow or Not allow Flash Protection Overrride. Steps to Reproduce: ========== 1. Use FITC to set EOM, Heci Me Region Unlock = true and ATFpopSoft=Allowed When AT Not Provisioned or Always Allowed 2. Enter BIOS and set FW Image Re-Flash to Enabled 3. Boot to OS, read FWSTS1	7.0.0.1090
3535133	Performing BIOS WWAN Recovery over SMS on the first attempt and on the second attempt it takes a very long time.	**Affected Component** – FW.TDT **Impact:** Recovery from stolen state over SMS does not function as expected. **Workaround:** Retry BIOS WLAN recovery over SMS. **Notes:** Steps to Reproduce: Send BIOS WLAN Recovery command over SMS.	7.0.0.1090

Issue #	Description	Affected Component / Impact / Workaround / Notes	Fixed in Kit#
3535723	TDT is in active state after clearing CMOS with recovery policy set to PBAM after end of POST.	**Affected Component** – FW.TDT **Impact:** Platform being set to stolen state after CMOS battery removal. **Workaround:** none **Notes:** Steps to Reproduce: 1. Flash platform with build 7.0.0.1019 (Alpha1). Set Default AT-p BIOS settings 3. Install permit (provision AT-p) 4. Set/Get public keys, set Credentials 5. Set PBA_Config policy - PBA_AFTER_EOP - PBA_IS_USED - S3 AUTH DISABLED - Platform action policy set to disable delayed 6. Set the timer interval PBA Logon timer to 6600 secs 7. Reboot the platform 8. Set TDT Disable Timer Policy to Disable_NOW with blob action DISABLE ACCESS 9. Set the assertstolen policy with platform action set to disable delayed 9a. set the disable timer and grace timer value to 2minutes and 3 minutes respectively. 10. Set the blob length for TSP, BIOS and PBAM to 300, 800 and 1020 respectively. 11. Retrieve all 3 Blob Types-TSP , BIOS and PBAM and verify content and length matches. 12 Disable DTimer using the following with disable timer value 0xFFFFFFFF 13. Shut down the platform, G3. 14. Clear CMOS jumper 15. Load BIOS default values and boot to OS 16 Get TDT state 17. Verify three blobs can be disabled after clearing CMOS.	7.0.0.1061

Issue #	Description	Affected Component / Impact / Workaround / Notes	Fixed in Kit#
3535288	G3 is required to reset the max attempts for 'setSuspendLocal' failure where Warm Reset is not sufficient.	**Affected Component** – FW.TDT **Impact:** Unexpected behavior. Firmware returns TDTHI_COMPCODE_INVALID_OPERATION TDT is in suspend state. **Workaround:** **Notes:** Steps to Reproduce: 1. Flash the current CougarPoint 8MB Q67 image to a Los Lunas board. 2. Boot and set SATA to IDE in BIOS 3. Load to windows 4. Activate a TDT Permit with FSTApp 5. Send TDTHI GetPublicKey to get TMK and send the setpublickey 5b. Set recovery passphrase credentials for TDTAM 5c. Use setcredential to configure SRTK 6. Reboot and go to BIOS screen-> and disable the EOP command(Advanced-> ME Configuration -> EOP Disabled 7.Getstate to verify TDT is in active state. 8. Send the suspendmodelocal(enter) command using No_Security_Failure 9. Check the state of TDT. 10. Send the suspendmodelocal(Exit) command using BAD_SRTK_TOKEN 11. Check the state of TDT. 12. Send the suspendmodelocal(Exit) command using BAD_SRTK_TOKEN 13. Check the state of TDT 14. Send the suspendmodelocal(Exit) command using BAD_SRTK_TOKEN 15. Check the state of TDT 16 Send the suspendmodelocal(Exit) command using No_Security_Failure 17 Reboot the platform 18. Send the suspendmodelocal(exit) command using No_Security_Failure 19. Check the state of TDT.	7.0.0.1061

Issue #	Description	Affected Component / Impact / Workaround / Notes	Fixed in Kit#
3535287	SetSuspendLocal(EXIT) is allowed 3 max attempts before Invalid Operation while SetSuspendLocal(ENTER) is only allowed 2 max attempts before Invalid Operation	**Affected Component** – FW.TDT **Impact:** Unexpected behavior. Firmware returns TDTHI_COMPCODE_INVALID_OPERATION. **Workaround:** **Notes:** Steps to Reproduce: 1. Flash the current CougarPoint 8MB Q67 image to a Los Lunas board. 2. Boot and set SATA to IDE in BIOS 3. Load to windows 4. Activate a TDT Permit with FSTApp 5. Send TDTHI GetPublicKey to get TMK and send the setpublickey 5b. Set recovery passphrase credentials for TDTAM 5c. Use setcredential to configure SRTK 6. Reboot and go to BIOS screen-> and disable the EOP command(Advanced-> ME Configuration -> EOP Disabled 7. Getstate to verify TDT is in active state. 8. Send the suspendmodelocal(enter) command using No_Security_Failure 9. Check the state of TDT. 10. Send the suspendmodelocal(Exit) command using BAD_SRTK_TOKEN 11. Check the state of TDT. 12. Send the suspendmodelocal(Exit) command using BAD_SRTK_TOKEN 13. Check the state of TDT 14. Send the suspendmodelocal(Exit) command using BAD_SRTK_TOKEN 15. Check the state of TDT 16 Send the suspendmodelocal(Exit) command using No_Security_Failure 17 Shutdown,G3 and poweron the platform 18. Send the suspendmodelocal(exit) command using No_Security_Failure 19. Check the state of TDT. 20. Send the suspendmodelocal(Enter) command using BAD_SRTK_TOKEN 21. Check the state of TDT. 22. Send the suspendmodelocal(Enter) command using BAD_SRTK_TOKEN 23. Check the state of TDT 24. Send the suspendmodelocal(Enter) command using BAD_SRTK_TOKEN 25. Check the state of TDT 26 Send the suspendmodelocal(Enter) command using No_Security_Failure	7.0.0.1061

Issue #	Description	Affected Component / Impact / Workaround / Notes	Fixed in Kit#
3535213	After setting the platform to Suspend state sending platform through Sx states including clear CMOS will cause HECI to fail.	**Affected Component** – FW.TDT **Impact:** Unexpected behavior. GetState fails with 'SetupDiGetDeviceInterfaceDetail failed' failed to open HECI client. **Workaround:** **Notes:** Steps to Reproduce: 1. Flash FW, Set Default BIOS settings 2. Provision AT-p, GetPublicKey, SetPublicKey, SetCredential 3. GetState, SetSuspendModeRemote, GetState 4. Transition into and out of the following PM states; S5 GetState, G3 GetState, WarmReset GetState, GlobalReset GetState, MeReset GetState, S5 .. G3 .. clear CMOS .. Set BIOS default settings...boot to OS 5. GetState error	7.0.0.1061
3535124	Removing the CMOS battery while a platform is enrolled (AT) will cause it to become un-bootable.	**Affected Component** – FW.TDT **Impact:** System un-usable if CMOS battery removed while enrolled. **Workaround:** Re-flash platform **Notes:** Steps to Reproduce: 1. Flash board with QM67 ALL SKU FW 2. Enroll in AT using Kit 3.0.0.1 3. Set policies to DTIMER - Delayed action, ASSERTSTOLEN - Delayed actions 4. Set all timers to 200 secs 5. Shut down system 6. Remove CMOS battery	7.0.0.1061
3535004	Firmware is always enabling the '3G WWAN NIC' by sending 'AT+CFUN=1' on each boot cycle instead of allowing the Windows Driver handle the NIC Activation.	**Affected Component** – FW.TDT **Impact:** Unexpected behavior. Firmware should not be setting during OS runtime. **Workaround:** none **Notes:** Steps to Reproduce: N/A	7.0.0.1061
3534987	TDT: ConfigureSMS FAILS on 1.5MB HM67 SKU (Blocking 3G testing on this Sku)	**Affected Component:** FW.MCTP **Impact:** **Workaround:** None **Notes:**	7.0.0.1041

5.5 Closed – Intel® Upgrade Service (Softcreek)

Issue #	Description	Affected Component / Impact / Workaround / Notes	Fixed in Kit#
3534838	ME RESET is being counted toward PCH MTP Period Boot Count.	**Affected Component** – FW.CLS **Impact:** MTP period boot count would expire earlier than expected. **Workaround:** **Notes:** Steps to Reproduce: Flow-A ========== 1. Flash PCH MTP (ExpTime=90mins, ExecTime=30mins, PeriodType=1, Period=3) 2. Boot to OS Verify MTP is in Applied state 3. Wait for the Default "7days/mins" to expire. Once expired, Period Boot Count should being counting. 4. Warm Reset (BootCount=1) 5. Verify MTP still in Applied state 6. S3 (BootCount=2) 7. S4 (BootCount=3) 8. ME Reset(Should not be counted toward Boot Count). However, this ME Reset results in GRESET and GetPermitInfo returns MTP NO LONGER in APPLIED state. Flow-B ========== 1. Issue ActivateMTP(Period=3 Boots) 2. WarmReset (BootCount=1) 3. Verify MTP is in APPLIED state 4. WarmReset (BootCount=2) 5. ME Reset (Does not result in GRESET) 6. ME Reset (Results in GRESET) MTP Permit is De-Activated after 2nd ME Reset, although ME Reset should not have been counted.	7.0.0.1115

Issue #	Description	Affected Component / Impact / Workaround / Notes	Fixed in Kit#
3551656	IsUpgradeAllowed returns FALSE for HM67 Sku Prior to Installing PCH Upgrade Permit	**Affected Component:** FW.CLS **Impact:** **Workaround:** none **Notes:** Steps to Reproduce: ========== 1. Flash an HM67 5M image on mobile platform with emulation set to core in FITc. via Dediprog/FPT > G3(unplug power) > Reapply Power > Boot to BIOS > Set following Parameters: 2. Press F3 for Optimized Defaults 3. Set SATA Mode = IDE [ADV > CONFIG > SATA CONFIG] 4. F4 to Save and Exit; 5. Boot to OS 6. Check the ISUpgradeAllowedfeature via FstApp tool.	7.0.0.1090

Issue #	Description	Affected Component / Impact / Workaround / Notes	Fixed in Kit#
3550947	Warm resets or S5 does not cause the CPU fuse override to be applied after CPU permit is installed	**Affected Component:** FW.CLS **Impact:** **Workaround:** none **Notes:** WARM Reset or S5-Shutdown is performed after CPU permit installation. On the next boot, FstApp tool reports that permit attribute is in Applied (or Approved state), but the CPU fuse over-ride is not applied. On performing several WARM resets or S5 does not cause the upgrade to become applied. The CPU fuse override gets applied only on G3 and the correct CPU upgrade are observed. G3 makes the upgrade happen everytime. This happened on multiple mobile platforms. The following issue is not reproducible on Desktop. Steps to Reproduce: ========== 1. Flash an HM67 5M image on Mobile platform via Dediprog/FPT > G3(unplug power) > Reapply Power > Boot to BIOS > Set following Parameters: 2a. Press F3 for Optimized Defaults 2b. Set SATA Mode = IDE [ADV > CONFIG > SATA CONFIG] 2c. F4 to Save and Exit; Use SoftSKuable CPU C0 3. Boot to OS 4 Check the PCIE Device with RWEverything Tool at Bus 00/Device 00 /Function 00 offset E8 to be 90 00 00 14 5. Install CPU standard permit with FOV value= 0x1000000 and FOM value =0x1E00000. User approval required set to N. 6 Reboot the platform 7. Verify the permit attribute of CPU Standard permit is in approved state. 8. Check the PCIE Device with RWEverything Tool at Bus 00/Device 00 /Function 00 offset E8 Expected Results: ========== PCIE Device with RWEverything Tool at Bus 00/Device 00 /Function 00 offset E8 should change to 90 00 00 15 from 90 00 00 14.i.e CPU Fuse Override is applied. Actual Results ========== PCIE Device with RWEverything Tool at Bus 00/Device 00 /Function 00 offset E8 remained at 90 00 00 14.i.e CPU Fuse Override is not applied.	7.0.0.1061

5.6 Closed - Not Firmware Issue

Issue #	Description	Affected Component / Impact / Workaround / Notes	Fixed in Kit#
3534467	If emulating Q or QM skus, the IGD graphics driver hangs.	**Affected Component:** ExternalDependency **Impact:** **Workaround:** Two workarounds exist: 1) Set SKU emulation in FITC to Super SKU DID 2) wait for Alpha version or later IGD graphics driver **Notes:**	7.0.0.1041

5.7 Closed - Documentation

Issue #	Description	Affected Component / Impact / Workaround / Notes	Fixed in Kit#
3534716	Executing FPT with the '-c' command line parameter results in 'error 27' being returned.	**Affected Component** – Documentation.SystemToolsUserGuide4MB **Impact:** FPT returns an error 27 Host CPU does not have erase access to target flash area. **Workaround:** Either limit the area to the area available using the -length command *or* create a 2 SPI component image. You know it will error out when you receive the message in FPT: "Warning: There are some addresses that are not defined in any regions. Read/Write/Erase operations are not possible on those addresses" **Notes:** Reproduction Steps: 1. From dos command line in FPT-Win...FPT.exe -c	7.0.0.1090

5.8 Closed - No Plan to Fix

Issue #	Description	Affected Component / Impact / Workaround / Notes	Reason
3551709	MEManuf-win tool End-of-line test – (Variable checks) always passes even with bad or incorrect values	**Affected Component:** SW.Tools.MeManuf **Impact:** **Workaround:** none **Notes:** Steps to Reproduce: ========== 1. HECI driver installed 2. Normal Platform setup for MEManuf-Win 3. Disable End Of Post in the Intel Menu 4. Set Manufacturing Mode to disabled by running FPTW -closemnf 5. Edit MEManuf.cfg set Subtestname=" Anytest " , ReqVal= "invalid value' 6. Run MEManuf-win.exe –EOL _verbose	Incorrect tool usage
3535737	FPT accepting RPATEnablerID FOV values with invalid hex-character lengths.	**Affected Component** – SW.Tools.FlashProgrammingTool **Impact:** Unexpected behavior. FPT allowing invalid character length is used for the RPATEnablerID. **Workaround:** none **Notes:** Reproduction steps: 1. Burn image. 2. Clear CMOS, set BIOS. 3. Go to OS. 4. Try to set EnablerID string with length 31 chars long only. (F. ex. >fptw -u -n RPATEnablerID -v ffeeddccbbaa0099887766554433221)	RPAT feature removed
2752633	The FWupdlcl tool fails to update over LMS when the platform is provisioned with the error 'Error 8707: Firmware update failed due to an internal error.'	**Affected Component** – SW.Tools.FwUpdLcl **Impact:** Firmware cannot be updated if the platform is provisioned. **Workaround:** Un-provision the platform prior to FW update. **Notes:** Reproduction Steps: 1. Flash FW Default BIOS settings/MEBx Provision ME 2. Make sure ping and WebUi is working from both host/target machines. 3. Use the following command: fwupdLcl.exe -f upd.bin -allowsv -user admin -pass Admin@98 (-wsman/-dash/-eoi) -oemid xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx	Obsolete by RCR

Issue #	Description	Affected Component / Impact / Workaround / Notes	Reason
2751283	Running firmware Update using –eoi will result in an update failure when platform has been provisioned in Kerberos mode.	**Affected Component** – SW.Tools.FwUpdLcl **Impact:** Firmware update fails to work with the –eoi command line switch in Kerberos. **Workaround:** none. **Notes:** **The –dash and wsman switch options function properly.** Reproduction Steps: 1. Kerberos and target setup. 2. Flash image and install drivers (Default BIOS, Set MEBx settings according Kerberos setup.) 3. In Kerberos (Configure target and server, Run Configserver.exe.) 4. Assure ping between them. 5. Check MEInfo on Target. 6. Assure you can open webui and logon from remote. 7.In 1166 Fwupd. fwupdlcl.exe XXXX_upd.bin -allowsv -host dut.intel.com -eoi -oemid xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx	Obsolete by RCR
3535644	GetGpsLocation (HECI) returning an'TDTHI_COMPCODE_INVALID_OPERATION' error while AT-p in stolen state after end of POST.	**Affected Component** – FW.TDT **Impact:** The platform does not return the expected TDT is in stolen state response. **Workaround:** none **Notes:** Steps to Reproduce: 1. Configure FW using FITC to enable PCH strap2 MCTP with address 0x30 2. Flash platform and install AT-P permit Using TDT_KCTest: 3. Execute Get/Set Public Key, Set SRTK Credential 4. Set the policy to PBAM after EOP and platform action policy to disable delayed. 5. GetMEIntegrityKey 6. Execute ConfigureSms 7. Enter stolen state using TDTHI assertstolen command 8 Check TDT state 9. Verify GetNonce can be sent successfully while in stolen state 10. Execute GetGpsLocation	Incorrect tool usage

Issue #	Description	Affected Component / Impact / Workaround / Notes	Reason
3535026	A global reset is occurring after 30-165 iteration of S3/M3 (5MB FW) or S3/Moff (1.5MB FW) with DeepSx disabled.	**Affected Component** – ExternalDependency **Impact:** Platform will unexpectedly global reset after multiple pass S3 cycle testing. **Workaround:** none **Notes:** Reproduction Steps: 1. Flash No DeepSx Image (4 or 8M) 2. Setup BIOS, save and exit 3. Enter MEBx and setup as usual (8M only) 4. Boot up to OS 5. Start S3 cycle testing	Cannot reproduce

6 Known Issues

6.1 Open - Intel® ME Kernel

Issue #	Description	Affected Component / Impact / Workaround / Notes
		Affected Component: **Impact:** **Workaround:** **Notes:**

6.2 Open - Integrated Clock Control (ICC)

Issue #	Description	Affected Component / Impact / Workaround / Notes
BUP000001	27-MHz FLEX Clock (for switchable graphics) has unexpected output value, unless Display PLL ownership is transferred to Intel® ME. Symptom: Upon boot or SX resume, on-board graphics down devices will not function as expected. Note: No official support for switchable graphics is currently provided with 27-MHz from Cougar Point PCH.	**Affected Component:** FW.ICC **Impact:** **Workaround:** The following bits need to edited as specified to utilize on-board graphics down devices that use 27-MHz FLEX clock from Cougar Point: • PLLEN bit 9 = 1b (Enable ME Ownership) • DPLLBC bit 30 = 1b (Enable DPLLB) Optional steps 3 and 4 If 27-MHz SSC clock is needed from CPT: • DPLLAC bit 30 = 1b (Enable DPLLA) • DPLLAC bits 26:24 = 011b (Enable 27M spread on DPLLA) This editing can be done in one of two ways: • Invoke Flash Image Tool with a commandline option **fitc.exe /iccext**, and edit the parameters directly in the FITC GUI. This option causes all ICC Registers to appear as dword values only, so raw dword values must be edited - there are no GUI bit-by-bit enhancements available as is when FITC is invoked without the **/iccext** commandline option. • Edit the parameters in the SPI Flash Image binary configuration XML file used by FITC. Note that this XML file is not the ICC Configuration XML, which has been deprecated and is no longer used by FITC. You must edit these parameters in the XML file and save the XML before starting FITC. The recommended method of doing so is making a copy of newfiletmpl.xml and editing the copy. Note that IccProfile1 corresponds to Profile 0 in SPI Flash, IccProfile2 to Profile 1, and so on. Note that 27-MHz Flex Clocks are available in both versions of the FITC GUI, with and without **/iccext** and no workarounds specified in previous kits are necessary.

6.3 Open - Software/Tools

Issue #	Description	Affected Component/Impact / Workaround/Notes
3553022	Installation of MEI driver will fail, if trying to install it after uninstall	**Affected Component:** SW.HECI Driver **Impact:** **Workaround:** **Notes:**

6.4 Open - Intel® Anti-Theft Technology

Issue #	Description	Affected Component/Impact / Workaround/Notes
		Affected Component: **Impact:** **Workaround:** **Notes:**

6.5 Open – Intel® Upgrade Service (Softcreek)

Issue #	Description	Affected Component/Impact / Workaround/Notes
		Affected Component: **Impact:** **Workaround:** **Notes:**

6.6 Open - Not Firmware Issue

Issue #	Description	Affected Component/Impact / Workaround/Notes
		Affected Component: **Impact:** **Workaround:** **Notes:**

6.7 Open - Documentation

Issue #	Description	Affected Component / Impact / Workaround / Notes
		Affected Component: **Impact:** **Workaround:** **Notes:**

§