



Intel® 6 Series/X79 Express Chipset - Intel® Management Engine Firmware 7.1

1.5MB Firmware Release Notes

7.1.52.1176 – Hot Fix (HF) Release

June 2012

Intel Confidential



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

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

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

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

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

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

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

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

Intel® Active Management Technology requires the computer system to have an Intel(R) AMT-enabled chipset, network hardware and software, as well as connection with a power source and a corporate network connection. Setup requires configuration by the purchaser and may require scripting with the management console or further integration into existing security frameworks to enable certain functionality. It may also require modifications of implementation of new business processes. With regard to notebooks, Intel AMT may not be available or certain capabilities may be limited over a host OS-based VPN or when connecting wirelessly, on battery power, sleeping, hibernating or powered off. For more information, see <http://www.intel.com/technology/manage/iamt/>

Watcom Library Source URL for DOS Manufacturing tools: <http://www.openwatcom.org/index.php/Download>

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.

Intel, vPro, Core, Pentium, Celeron and the Intel logo are trademarks of Intel Corporation in the U.S. and/or other countries.

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

Copyright © 2012, Intel Corporation. All rights reserved.



Contents

1	Introduction	6
1.1	Scope of Document	6
1.2	Intel® IPT Description and Support.....	6
1.3	Acronyms	6
2	Release Kit Summary	8
2.1	Release Kit Details	8
2.2	Build Details	9
2.3	Kit Overview	9
2.4	Contents of Downloaded Kit	10
2.4.1	Intel® ME SW Components.....	10
2.4.2	Image Components.....	11
2.4.3	System Tools	12
2.5	Release Version Numbering Information	13
2.5.1	Firmware Update Blacklist Information	14
3	Important Notes	17
3.1	Important Issues/Notes	18
3.2	KSC Update.....	18
3.3	Intel® LAN Binary Images	18
3.4	FITc XML Compare	19
4	Intel® ME New Features	20
4.1	RCR Update	20
5	Issue Status Definitions.....	24
6	Closed Issues	25
6.1	Closed – Intel® ME Kernel	25
6.2	Closed – Integrated Clock Control (ICC)	36
6.3	Closed – Software / Tools	37
6.4	Closed – Intel® Anti-Theft Technology	52
6.5	Closed – Intel® Upgrade Service	53
6.6	Closed – Not Firmware Issue	54
6.7	Closed – No Plan to Fix	56
6.8	Closed – Documentation Change.....	57
7	Known Issues.....	58
7.1	Open – Intel® ME Kernel	58
7.2	Open – Integrated Clock Control (ICC)	58
7.3	Open – Software / Tools	59
7.4	Open – Intel® Anti-Theft Technology	59
7.5	Open – Intel® Identity Protection Technology	59
7.6	Open – Intel® Upgrade Service	59
7.7	Open – Not Firmware Issue	59
7.8	Open – Documentation Change	60





Revision History

Revision Number	Description	Revision Date
7.1.0.1001	• Engineering Release based off 7.0.0.1095	August 2010
7.1.0.1005	• Engineering Release based off 7.0.0.1110	September 2010
7.1.0.1008	• Engineering Release based off 7.0.0.1133	October 2010
7.1.0.1009	• Beta Release based off 7.0.0.1137	October 2010
7.1.0.1026	• Production Candidate Release (PC) based off 7.0.0.1152	November 2010
7.1.0.1028	• Production Candidate 2 Release	December 2010
7.1.0.1028	• Production Release	December 2010
7.1.1.1039	• Hot Fix Release	December 2010
7.1.2.1041	• Hot Fix 2 Release	January 2011
7.1.2.1041 v2	• Hot Fix 2 Release version 2	January 2011
7.1.3.1053	• Hot Fix 3 Release	February 2011
7.1.10.1065	• Maintenance Release	February 2011
7.1.13.1088	• Maintenance Release Hot Fix 3	May 2011
7.1.14.1107	• Hot Fix 4	July 2011
7.1.20.1119	• Maintenance Release 2 -PV	August 2011
7.1.30.1142	• Maintenance Release	November 2011
7.1.31.1147	• Hot fix Release	December 2011
7.1.40.1161	• Maintenance Release	February 2012
7.1.50.1172	• Maintenance Release	May 2012
7.1.52.1176	• Hot Fix • (CPT client release ONLY / PBG workstation is not included in this release)	June 2012



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 Intel® IPT Description and Support

Intel® ME Firmware 7.1 supports Intel® IPT (restricted to Intel® Core™ CPUs).

Intel® IPT software and collaterals are published as a separate kit in <https://platformsw.intel.com> (Kit #32740)

1.3 Acronyms

Term	Description
BIOS	Basic Input Output System
CRB	Intel Customer Reference Board
FITC	Flash Image Tool
FOV	Fixed Offset Variable
FW	Firmware
GbE	Gigabit Ethernet
HBP	Host Base Provisioning
HECI	Host Embedded Controller Interface. Same as Intel® MEI.
ICC	Integrated Clock Control
Intel® AMT	Intel® Active Management Technology
Intel® AT	Intel® Anti-Theft Technology
Intel® IPT	Intel® Identity Protection Technology
Intel® MEI	Intel® Management Engine Interface (interface between the Management Engine and the Host system)
IMSS	Intel® Management and Security Status Application
LAN	Local Area Network
LMS	Local Manageability Service
MAC	Media Access Control
Intel® MEBx	Intel® Management Engine BIOS Extension



Term	Description
MRC	Memory Reference Code
OS	Operating System
BLU-RAY PLAYBACK	Blu-Ray* Playback
PCH	Platform Control Hub
PKI-CH	Public Key Infrastructure with Certificate Hashing
RCFG	Remote configuration
SOL	Serial over LAN
SPI	Serial Peripheral Interface
TDT	Theft Deterrence Technology. Previous name for AT-p, which is part of the Intel® Anti-Theft Technology.
UNS	User Notification Service
WMI	Windows Management Instrumentation



2 Release Kit Summary

This document covers the following Intel® Management Engine Firmware SKUs for the Cougar Point platforms:

- Intel® Management Engine Firmware 7.1 Intel® 6 Series Express Chipset
 - 1.5MB FW SKU

Kit release information is outlined below:

2.1 Release Kit Details

- * **Release** : Intel® Management Engine Firmware 7.1 Intel® 6 Series Express Chipset Hot Fix (HF) – 7.1.52.1176
- * **Target Platform** : Sandybridge CPU & Cougar Point Chipset Family / PCH
- * **.zip name** : CPT_1.5M_7.1.52.1176.zip

Contents:

- Intel® Management Engine Firmware (for Intel® 6 Series Express 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 Build Details

Kit	Build Details	Changes since previous release 7.1.50.1172 (CPT)?	Reasons for changes
Firmware Version	7.1.52.1176	Yes	FW changes to fix Issue #3707913. See Important Notes Section and separate customer communication for more detail.
CRB BIOS Version (CPT)	S_CPT082.rom	No	N/A
Intel® MEI Driver Version	7.1.21.1134 (WHQL'd)	No	N/A
SOL Driver Version	7.1.21.1154 (WHQL'd)	No	N/A

2.3 Kit Overview

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

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

1. After logging in, click on the link 'View All Kits' on the left side of the web page.
2. Click on the corresponding kit number that is to be downloaded.
3. Select and open the appropriate kit component
4. The Supporting Documentation folder under the selected component contains the following supporting documentation:
 - 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 kit release.
 - b. 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:\)



2.4 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:

Drivers are included in:

CPT_1.5M_7.1.52.1176

2.4.1 Intel® ME SW Components

Installers	Description
ME_SW	<ul style="list-style-type: none">• Intel® MEI is the interface between the host and the Intel® Management Engine firmware.• Drivers and applications on the host that wish to interact with Intel® Management Engine through the host interface use the Intel® MEI host Windows* driver.• Intel® MEI driver is installed by running: C:\[skuName_x.x.xxxx]\Installers\ME_SW\Setup.exe• The Intel® MEI driver can also be installed using the 'Have Disk' method in 'Device Manager', as follows:<ul style="list-style-type: none">○ Right click 'My Computer' and select Properties.○ Select the Hardware tab and click Device Manager.○ Scan for hardware changes.○ Update the particular device driver by pointing to the INF file: C:\[skuName_x.x.xxxx]\ME_SW\Installers\Drivers\MEI\HECI.inf. <p>NOTE: ME_SW installer also installs a Microsoft* Windows* application (Intel® Management and Security Status Application (IMSS)) "The Intel® Management and Security Status icon indicates whether Intel® AMT, Intel® Standard Manageability, Level III Manageability Upgrade and Intel® Anti-Theft are running on the platform"</p>
ME_SW_IS	<ul style="list-style-type: none">• The ME_SW_IS installer will install the same components as ME_SW but using an InstallShield wrapper.
MEI-Only Installer	<ul style="list-style-type: none">• The MEI-Only Installer Only installs the MEI driver.



2.4.2 Image Components

NVM Images are included in:

- o CPT_5M_7.1.52.1176

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

Image	Description
BIOS	<ul style="list-style-type: none"> Contains Intel Reference System BIOS Supported devices: Cougar Point Chipset Family PCH After flashing a new BIOS, enter BIOS setup and 'Load Default Settings' (Press F3). Then 'Save and Exit' (Press F4) from Setup. This is a required step when updating to a new BIOS release. For latest release information and known issues on the BIOS, please refer to the following directory: C:\[kit]\Image Component\BIOS\
Firmware	<ul style="list-style-type: none"> The Intel® Management Engine firmware contains code and configuration data for Intel® Management Engine functions. This is one of the regions that are integrated into the final flash image that is built using the Flash Image Tool, and is then programmed into the flash. <p>NOTES:</p> <ul style="list-style-type: none"> For more details on building the flash image, please refer to 1.5MB FW Bringup Guide.pdf, included in the downloaded kit. For more details on the firmware and related issues, please refer to Important Notes section, of this document.
GbE	<ul style="list-style-type: none"> The GbE hardware (PCH LAN) is a component embedded in the PCH. GbE region of the flash contains bits that define the configuration of the GbE hardware. The given Gigabit Ethernet or GbE component image should be integrated with the other images (Firmware and BIOS) using the Flash Image Tool, to create a single binary flash image. The GbE image will be programmed into the SPI flash as part of this integrated image using the Flash Programming Tool. The GbE folder contains images for A1/A2 and B0 PHY silicon. Example: NAHUM5_LEWISVILLE_DESKTOP_11.bin. This image can be used with any of the Intel® Management Engine images.



2.4.3 System Tools

System Tools are included in:

- o CPT_5M_7.1.52.1176

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

Tool	Description
Flash Image Tool – fitc.exe	<ul style="list-style-type: none">• Provides both a GUI and a command line tool.• OS Support – Windows XP, Vista* (32-bit & 64-bit) and Windows 7 (32-bit & 64-bit)• Used to assemble the different elements of the SPI flash (Descriptor, Intel Reference System BIOS, Intel® Management Engine firmware, Gigabit Ethernet (GbE) into a single binary image
Flash Programming Tool – fpt.exe and fptw.exe	<ul style="list-style-type: none">• Provided as DOS and Windows* command line tools• OS Support - MS Dos 6.22, DRMKDos and FreeDOS. The windows version (fptw.exe) will run in Windows* XP (Sp2), Windows PE and Windows Vista* (32-bit & 64-bit), Windows 7 (32-bit & 64-bit).• Used to write the flash image into the SPI flash device
FWUpdate – FWUpdLcl Tools	<ul style="list-style-type: none">• Provided as DOS and Windows* command line tools• DOS Tool is supported on MS-DOS* 6.22, Windows 98 DOS, Free DOS and DRMK• Windows Command line tool is supported on Windows XP SP2, Windows XP x64, Windows Vista* (32-bit & 64-bit), Windows 7 (32-bit & 64-bit)• Used to update the Intel® Management Engine's firmware
MEInfo	<ul style="list-style-type: none">• Provided as DOS and Windows* command line tools• OS Support - MS-DOS 6.22, Windows 98 DOS, FreeDOS, DRMK DOS. MEInfoWin is a command-line executable for Windows (Windows XP SP1/2, Server 2003, Server 2008 R2, Vista* (32-bit & 64-bit) and Windows 7 (32-bit & 64-bit)• Verifies that Intel® Management Engine (Intel® ME) firmware is alive and returns data about Intel® ME
MEManuf	<ul style="list-style-type: none">• Provided as DOS and Windows* command line tools• Used on the manufacturing line to validate an Intel® Active Management Technology device



Tool	Description
UpdParam	<ul style="list-style-type: none">• Provided as a DOS command line tool• UpdateParam tool is used to change certain ME firmware parameters (both AMT and Kernel) after the global valid bit is set and descriptor region is locked.

2.5 Release Version Numbering Information

Typical release version numbering is as follows,

7.X.y.z (for example: 7.1.0.xxxx) where:

'7' refers to the Intel® Management Engine 7.1 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



2.5.1 Firmware Update Blacklist Information

The Blacklist is evaluated during every firmware update (either upgrade or downgrade). Firmware blocks the ability to update to any firmware version that is in the Blacklist. The firmware Blacklist is used to identify versions that have known security flaws or other severe vulnerabilities.

For each current Release, the Build number listed below is in the Blacklist. The effect is that it is not possible to update to the listed Build number or earlier.

SKU	Current Version ¹	Downgrade to ²	Items in the blacklist ³	Comment
1.5MB	7.1.52.1176	For CPT: 7.1.30.1142	For CPT: 7.1.21.x and 7.1.14.1107 and prior	Hot Fix Release
1.5MB	7.1.50.1172	For CPT: 7.1.30.1142 For PBG: 7.1.21.1134 (PBG only)	For CPT: 7.1.21.x and 7.1.14.1107 and prior For PBG: 7.1.40.1161, 7.1.30.1142 and 7.1.20.1089 and prior	Maintenance Release See Issue #3792120 in Important Notes and Closed Issues sections for details in this release which merges CPT and PBG platforms
1.5MB	7.1.40.1161	7.1.30.1142	7.1.14.1107 and prior	Maintenance Release



SKU	Current Version ¹	Downgrade to ²	Items in the blacklist ³	Comment
1.5MB	7.1.31.1147	7.1.20.1119	7.1.14.1107 and prior	Hot Fix Release
1.5MB	7.1.30.1142	7.1.20.1119	7.1.14.1107 and prior	Maintenance Release.
1.5MB	7.1.20.1119	Not allowed	All releases prior to 7.1.20.1119	Security Fix
1.5MB	7.1.14.1107	Not allowed	All releases prior to 7.1.14.1107	Security Fix
	7.1.13.1088	Not allowed	All releases prior to 7.1.13.1088	Security Fix
	7.1.10.1065	Not allowed	All releases prior to 7.1.10.1065	Security Fix
	7.1.3.1053	Not allowed	All releases prior to 7.1.2.1041	FW DPM Fix
	7.1.2.1041	7.1.1.1039	All releases prior to 7.1.0.1028 PV	HF2 -> HF1 Allowed



SKU	Current Version ¹	Downgrade to ²	Items in the blacklist ³	Comment
	7.1.1.1039	7.1.0.1028	All releases prior to 7.1.0.1028 PV	Not allowed. 7.1.1 Security fix
	7.1.0.1028	Anything	N/A	Initial 7.1 Production Version

¹ Current version -> After programming the flash memory with this version...

² Downgrade to - > You can downgrade to these versions (version numbers in black font)

³ Items in the blacklist - > You cannot downgrade to these versions (version numbers in red font)



3 *Important Notes*

This **Hot Fix Release** firmware supports 1.5MB Corporate and Consumer SKU platforms.

Note: Although CPT client and PBG workstation merged in with the previous 7.1.50.1172 MR kit, this Hot Fix Release is for CPT client only. PBG workstation is not part of this release.

- All Moff Power flows (PP1) – Supported
- All M3 Power flows -Supported
- BLU-RAY PLAYBACK - Supported
- WLAN – Supported
- Intel® Rapid Start Technology



3.1 Important Issues/Notes

- **Issue #3707913** – Failure using Media Check Tool due to FW issue with EPID Group ID multiple of 256. This HF release supports a fix for Media Check Tool issue "Media Check Fail: Please check Intel MEI driver installation and ME firmware version; System configuration incorrect for Media Playback".

Refer to the Customer Communication provided separately with this release.

- **7.1.50.1172 Maintenance Release merges the Intel® 6 and C600 Series Express Chipset Intel® Management Engine Firmware 7.1 code branches together.**

The last release for Intel® C600 Series Express Chipset was 7.1.21.1134 (PV). This kit release contains all appropriate updates between PBG 7.1.21.1134 and CPT 7.1.40.1161 MR in addition to new bug fixes and RCRs in 7.1.50.1172 MR.

- **Issue #3792024** - KVM sessions close unexpectedly during local reboot stress has been resolved in a graphics driver update. For more information see highlighted Issue 3792024 below in Closed Issues section.
- **Issue #3792120** - FWUpdate should have the following behavior:

Patsburg:

- Prevent downgrades to any build $\geq 7.1.30$, $< 7.1.50$, and $< 7.1.21.1134$.
- Allow downgrades to anything between 7.1.21.1134 and 7.1.30.
- Prevent upgrades from 7.1.2x to 7.1.3x/7.1.4x

Cougar Point:

Prevent downgrades from 7.1.3x/7.1.4x to $\geq 7.1.21$

3.2 KSC Update

Users must be sure they are using latest Intel KSC (1.16) on mobile platforms and "SMLink1 Thermal Reporting Select" should be set to "true" in FITC

3.3 Intel® LAN Binary Images

Intel® ME 7.1 PC FW kit contains two GbE binaries:

NAHUM5_LEWISVILLE_DESKTOP_13.bin supports Intel® LAN PHY A2, B0 and C0 only and must be used with Cougar Point PCH B2 stepping. 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, B0 and C0 only and must be used with Cougar Point PCH B2 stepping. This image is



recommended for testing power flows with connectivity. This image is for mobile platforms only.

3.4 FITc XML Compare

Changes between the MR 7.1.50.1172 newfiletmpl.xml and HF 7.1.52.1176 newfiletmpl.xml	
MR 7.1.50.1172 newfiletmpl.xml	HF 7.1.52.1172 newfiletmpl.xml
<ftoolRoot version="31">	No changes

- 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:

- Under Descriptor Region node, right-click on VSCC Table, and select 'Add Table Entry...'
- Enter an Entry name.
- 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 Intel® ME New Features

4.1 RCR Update

RCR #	Description / Background	Build
CCG0100009637	Description: WinPE 64bit support for ME7.1 tools Memanuf and MEInfo Background: Key ME tools MEMANUF and MEINFO only worked on 32 bit Windows systems. This RCR enabled support for these tools on environments that used a 64 bit version of Windows PE.	7.1.40.1161
3522840	Description: ME Update Package (MUP) : Unique versioning implemented in ME Update Package (MUP) for every ME FW build. Background: ME FW kit driver package in Mup.xml used to have the same version across different kit releases. This RCR changes and makes it unique & enables the inventory collection and software update mechanism that keeps systems up to date.	7.1.40.1161
CCG0100009257	Description: Due to LAN HW bug on MAC access arbitrator, mutual exclusivity needed to be done between LAN OS driver TDT register writes and ME MAC R/W access Background: LAD found a HW bug in their MAC arbitration between Host and ME (PCIm to PCI) memory accesses. This bug is being exposed in CPT because of clock frequency changes resulting in timing changes. PPT LAN MAC will gain a HW fix for this issue, but LAD request ME changes to fix this issue in CPT, as LAN driver cannot fix this in SW, and ME is triggering the flow that the issue is seen in while performing link manger polling	7.1.20.1119



RCR #	Description / Background	Build
CCG0100150603	<p>Description:</p> <p>Adds ME support for Microsoft Windows 7 SP1</p> <p>Background:</p> <p>ME FW and SW tools, drivers, and SW (FITC, MEINFO, MEMANUF, FWUPDLCL, FPT, IUSMF and ICC tools) have validated support for Microsoft Windows 7 SP1.</p>	7.1.10.1065
CCG0100087681	<p>Description:</p> <p>Removed Workaround to 'Allow SKU/CPU Emulation using Production-Signed firmware on SuperSKU PCH on Production PCH'</p> <p>Background:</p> <p>Customers want to manage ONE single Flash image (BIOS/FW/GbE) for all platforms across their global validation groups. Once customers have CPT B0 (all Super SKU) and B1/B2 (all production fused) in their inventory, managing two images across all platforms would be difficult especially if PCH Stepping is not marked on platform.</p>	7.1.2.1041
CCG0100090560	<p>Description:</p> <p>Workaround to allow Processor Emulation on all PCH Parts built before ww42 and change FW Expiration to WW46.</p> <p>Background:</p> <p>Allow Processor Emulation to work on 7.1 FW running on boards using QS and PRQ PCH parts that were created before ww42</p> <p>If FW is run on parts built after ww42, original rules for Processor Emulation will apply.</p>	7.1.0.1009
CCG0100009080	<p>Description:</p> <p>Add WLAN manageability capability to Level III upgraded HM67 SKU</p> <p>Background:</p> <p>Level III MNG upgrade on HM67 was implemented in ME7.x however WLAN manageability was overlooked for this SKU configuration.</p>	7.1.10.1065



RCR #	Description / Background	Build
CCG0100009042	Description: Security Enhancement: Amendment to Certificate Enrollment Background: Adds additional verifications in 7.0 ME FW during CIRA, 802.1x and when generating Signed Audit logs.	7.1.10.1065
CCG0100009036	Description: Security Enhancement: Partial un-provisioning to remove non-secure DNS suffix and move back to original secure mode Background: User can mistakenly or software running on the host could override the pre-set DNS suffix.	7.1.10.1065
CCG0100009034	Description: Security Enhancement: Host Based Provisioning (HBP) Client Controlled Mode (CCM) Un-provisioning should not remove secured settings Background: After HBP CCM provisioning, the user initiated un-provision option shall prevent removal of secured settings including custom hashes, inactive default hashes and DNS suffix.	7.1.10.1065
CCG0100097817	Description: PCIe to PCIe Peer sharing permanent disable. Background: CSPEC update: PCIe Peer to Peer PCH Strap 9 bits 28 and 29 should be set to a '1' value.	7.1.10.1065
CCG0100008865	Description: Updating Low Power UM67 PCH & ULV/LV CPU FW Identifier based on new ULV/LV Processor Numbers Background: Firmware updated to appropriately support ULV/LV processors for UM67 SKU platforms.	7.1.1.1039



RCR #	Description / Background	Build
CCG0100087747	<p>Description:</p> <p>MEManuf tool will introduce option for customer to ignore 3G related test ("-no3g", similar to "-nowlan" flag already existing).</p> <p>Background:</p> <p>OEMs want to maintain one single BIOS image with 3G enabled, but not all platforms will be shipped with a 3G card. So when MEManuf calls self test, it is told by BIOS that the card exists, but when the test is run on platforms the tool will issue an overall failure.</p>	7.1.0.1009
CCG0100087681	<p>Description:</p> <p>Allow SKU Emulation on Signed FW</p> <p>Background:</p> <p>Customers want to manage ONE single Flash image (BIOS/FW/GbE) for all platforms across their global validation groups. Once customers have CPT B0 (all Super SKU) and B1/B2 (all production fused) in their inventory, it would be very difficult for them to manage two images across all platforms.</p>	7.1.0.1009
CCG0100087402	<p>Description:</p> <p>Change CPU Replacement Confirmation Handling to Lessen Impact on Manufacturing Line.</p> <p>Background:</p> <p>Currently MEBx will prompt if a CPU replacement is detected and present a continue prompt to the user. This behavior negatively impacts manufacturing lines and automated testing since the prompt will remain until a key is pressed.</p>	7.1.0.1008
CCG0100008933	<p>Description:</p> <p>When Partial ME Alt disable is configured Intel® Dynamic Application Loader (Intel® DAL) will not become permanently disabled and can be set to either enabled or disabled as required by the OEM (same as Intel® AT and PAVP).</p> <p>Background:</p> <p>Currently the Intel® Dynamic Application Loader cannot be enabled in the Partial ME Alt disable configuration under the OEMSKURule FOV.</p>	7.1.0.1028
CCG0100008841	<p>Description:</p> <p>Name change from MEDAL to Intel® Dynamic Application Loader (Intel® DAL)</p> <p>Background:</p> <p>This RCR is to change from the internal working name for the technology (MEDAL) to the official external name.</p>	7.1.0.1028



5 *Issue Status Definitions*

This document provides sightings and bugs report for Intel® Management Engine Firmware 7.0 SKU, Software and Tools for Intel® AMT on the Cougar Point Family / PCH platform. The issues are separated into sub-groups to assist in understanding the status of the issues and what action, if any, needs to be done to address the issue. The names and definitions of the sub-groups are detailed below.

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

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

Open Issues: New sightings and bugs will be classified as “Open” issues until the fix is verified with the appropriate firmware version. Open issues are separated into 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 will be 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.



6 Closed Issues

6.1 Closed – Intel® ME Kernel

Issue #	Description	Affected Component/Impact / Workaround/Notes	Fixed in Kit#
3707913	Failure using Media Check Tool due to FW issue with EPID Group ID multiple of 256. This HF release supports a fix for Media Check Tool issue "Media Check Fail: Please check Intel MEI driver installation and ME firmware version; System configuration incorrect for Media Playback".	Affected Component – FW.Kernel Impact: Refer to the Customer Communication provided separately with this release.	7.1.52.1176
3792109	Intel® ME is not accessible after soft reboot cycles in Windows* 7.	Affected Component – FW.Kernel Impact: Loss of Intel® ME until system is rebooted. Workaround: N/A Notes: Typically seen after several thousand cycles. Issue does not occur when booting from DOS. Reproduction Steps: 1. Install Windows* 7 64-bit. 2. Perform continuous warm reboot cycling until Intel® ME is not accessible (may exceed 3000 cycles).	7.1.50.1172
3791949	Firmware could go into recovery when repeatedly running MEMANUF. Frequency: Infrequent	Affected Component – FW.Kernel Impact: Firmware goes in to recovery at random junctures when using MEMANUF Workaround: N/A Notes: N/A Reproduction Steps: Not consistently reproduced	7.1.20.1119
3791554	HCI does not unregister its dynamic HECI connection during certain power management transitions	Affected Component – FW.Kernel Impact: System hang Workaround: N/A Notes: N/A Reproduction Steps: Not consistently reproduced	7.1.20.1119



Issue #	Description	Affected Component/Impact / Workaround/Notes	Fixed in Kit#
3791580	HCI does not wait for worker thread completion before deleting thread during certain warm resets.	Affected Component – FW.Kernel Impact: Global reset Workaround: N/A Notes: N/A Reproduction Steps: Not consistently reproduced	7.1.20.1119
3790836	PM driver causes exception if it receives too many illegal BIOS write interrupts in a short time	Affected Component – FW.Kernel Impact: System hang Workaround: N/A Notes: N/A Reproduction Steps: N/A	7.1.20.1119
3791909	The system causes GRST during S3 stress testing with specific 3G module	Affected Component – FW.MCTP Impact: System goes to S3 Workaround: N/A Notes: Reproduction Steps: When running suspend/resume stress tests with specific 3G straps set and 3G cards populated, platform goes in to perennial S3.	7.1.14.1107
3791713	System Hangs during transition to S3 when ME is enabled	Affected Component – FW.Kernel.Drivers Impact: During the system transition to S3/Moff, ME cannot unload the LME component due to unexpected connection sharing with the FWUpdate component. The resulting hang prevents the ME from entering Moff; which prevents the system from entering S3. Workaround: Power button override Notes: Reproduction Steps: 1. Power on System, and boot to Windows OS. 2. Run S3 cycling test.	7.1.13.1088
3791710 / 3791711 / 3791712	ME FW corruption could occur if power loss occurs during ForceFullReclaim	Affected Component – FW.Kernel.StorageMgr Impact: ME FW corruption could occur when a ME Full Reclaim is performed and then there is a power loss during the reclaim of a data block (Sporadic: 1/500 – 1/3000). Workaround: N/A Notes: N/A	7.1.13.1088



Issue #	Description	Affected Component/Impact / Workaround/Notes	Fixed in Kit#
3791709	ME FW may fail to initialize on boot and FW version fails to be displayed	<p>Affected Component – FW.Kernel</p> <p>Impact: Timing between ME and HW init sequence may cause ME to fail on initialization and FW version fails to display. Occurrence of this issue is very low and is dependent on the combination of chipset and platform design implementations. Issue is observed at initial boot.</p> <p>Workaround: N/A</p> <p>Notes: N/A</p>	7.1.13.1088
3791614	PM driver causes exception if it receives too many illegal BIOS write interrupts in a short time.	<p>Affected Component – FW.Kernel.PowerManagement</p> <p>Impact: High number of writes to BIOSWE register will cause ME to become unresponsive.</p> <p>Workaround: N/A</p> <p>Notes: N/A</p>	7.1.13.1088
3791316	System hang and unexpected shutdown seen on S0 -> S3 and S3 -> S0 transition during stress testing.	<p>Affected Component – FW.Kernel.Drivers</p> <p>Impact: While going into S3/Moff, ME gets stuck going into Moff preventing Kernel Loader to turn off LME component.</p> <p>Workaround: N/A</p> <p>Notes: Reproduction Steps:</p> <ol style="list-style-type: none"> 1. Power on system 2. Run S3 cycling tool e.g. Sleeper 3. Wait for system hang transitioning from S0->S3->S0. Windows will display "Unexpected shutdown occurred..." error message on next Windows bootup. 	7.1.10.1065
3791282	Global reset (GReset) does not occur after CPU replacement after Closemfnf.	<p>Affected Component – FW.Kernel</p> <p>Impact: Global reset initiated by MEBx occurs on second boot if CPU is replaced with different CPUID and CPU Brand</p> <p>Workaround: none</p> <p>Notes:</p>	7.1.10.1065



Closed Issues

Issue #	Description	Affected Component/Impact / Workaround/Notes	Fixed in Kit#
3791166	PCH temperature is 0 degree	Affected Component – FW.Kernel.SMBusDriver Impact: Fixes an issue where PCH thermal data is reported as 0 incorrectly Workaround: none Notes: Reproduction Steps: Monitor SMBus traffic over a long period of time. Eventually 0 PCH temperature readings will be seen from the PCH.	7.1.10.1065
3791145	Heuristics disabled after Level 3 upgrade from STD on B65 SKU systems.	Affected Component – FW.Kernel Impact: System defense heuristics will not be functional after upgrade. Workaround: none Notes:	7.1.10.1065
3791143	ME FW shows Error code is disabled after FWUpdIcl failure.	Affected Component – FW.Kernel Impact: ME FW writes error status to the wrong FWSTS1 field. Workaround: none Notes:	7.1.10.1065
3791141	FWUpdate shows an error message after FWUpdate fails to a blacklisted FW and a reboot does not occur	Affected Component – FW.Kernel.FWUpdate Impact: The FW Update tool shows expected error while downgrade (errors 8741 and 8758) to a blacklisted FW. If an upgrade to a good FW update image is attempted without performing a reboot, FW gives unexpected error 8741("FW Update failed"), followed with "Trying to receive update status". System may hang on this status. When tried to reboot at this time, FW enters recovery mode. Workaround: none Notes:	7.1.10.1065



Issue #	Description	Affected Component/Impact / Workaround/Notes	Fixed in Kit#
3790985	<p>Buffer overflow vulnerability in the implementation of the System.arraycopy method may be exploited by an untrusted applet to escalate privileges (issue #6009).</p> <p>This is caused by an incorrect check on the parameters src_offset, dst_offset, and length. The implementation fails to detect when the sum src_offset+length or dst_offset+length overflow. In this case, instead of throwing an instance of ArrayIndexOutOfBoundsException, the implementation proceeds to copy the data, thus allowing the applet to access to memory outside the arrays passed in parameters.</p>	<p>Affected Component – FW.Kernel</p> <p>Impact: CVSS score is 6.8 (AV:L/AC:L/Au:S/C:C/I:C/A:C). Increased Privileges for Untrusted Applets</p> <p>Category: Severe</p> <p>All Gen1 releases are affected. The BETA-1 Gen2 release is also affected. Gen1 is used in Intel® DAL (ME 7.1)</p> <p>Workaround: When the applet is reviewed before being digitally signed, the direct or indirect calls to System.arraycopy must be analyzed. If there is a risk that src_offset+length or dst_offset+length might overflow, code must be added before the call to System.arraycopy to check for this condition instead of relying on the implementation of System.arraycopy to catch the error.</p> <p>This must be done also when the code calls one of the following methods because they internally call System.arraycopy:</p> <ul style="list-style-type: none"> •String(char[] value, int off, int len) •String.getChars(int srcBegin, int srcEnd, char[] dst, int dstBegin) •StringBuffer.append(char[] str, int offset, int len) •StringBuffer.getChars(int srcBegin, int srcEnd, char[] dst, int dstBegin) <p>Notes:</p>	7.1.10.1065
3790925	Performing a CPU swap of different steppings while in G3 (with PP2 set) or Sx/M3 (PP2) fails to initiate a global reset and causes Integrated Graphics to fail on the next boot.	<p>Affected Component – FW.Kernel</p> <p>Impact: If change between different CPU steppings, ME will not initiate the expected global reset resulting in internal graphics will not function.</p> <p>Workaround: none</p> <p>Notes:</p>	7.1.10.1065

**Closed Issues**

Issue #	Description	Affected Component/Impact / Workaround/Notes	Fixed in Kit#
3522079	A DPM issue related to Intel® Firmware enabled features has been observed in some customer manufacturing lines as they began ramping their consumer system manufacturing to high volume. While the systems should remain functional, under certain circumstances, one or more Intel Firmware enabled features may not work when provisioned.	Affected Component – FW.Kernel Impact: The worst case Intel Firmware enabled feature DPM is 3900. Due to the number of variables required to see this issue, including the number of Intel firmware enabled features present on the platform, customers should expect to see significantly less than worst case, possibly none. Workaround: none Notes: None	7.1.3.1053
3790829	Firmware does not properly update SPI information when changing from one processor type to another processor type.	Affected Component – FW.Kernel Impact: Medium Workaround: none Notes:	7.1.2.1041



Issue #	Description	Affected Component/Impact / Workaround/Notes	Fixed in Kit#
3790760	AT-P enabled system cannot shutdown after receiving "Poison Pill" over 3G network.	<p>Affected Component – FW.Kernel.SMBusDriver</p> <p>Impact: Medium</p> <p>Workaround: none</p> <p>Notes: Reproduction Steps:</p> <ol style="list-style-type: none"> 1. Boot to OS with WWAN 5550. 2. On the server, using a CMD prompt run 'isv_server ?i server_ip. 3. On the Client, using a CMD prompt run 'isv_client ?i server_ip -e, allow the SUT to enroll. 4. On the server, using a CMD prompt run 'sqlite3 tdt.db < test2.txt' and run 'sqlite3 tdt.db < timers.txt'. Observe several rendezvous's. 5. Stop the isv_client (CTRL-C). Launch the isv_client using the following format: "isv_client ?i server_ip ?g and ?t isv_server SMS phone -r 10000 -q \\.\\com port" 6. Stop the isv_server. On the server, run the following commands: <ul style="list-style-type: none"> - "sqlite3 tdt.db" - "Update slog set state=2;" - "Select Client_id from pinfo;" -> record the client ID - ".quit" 7. On the server, run: "genoob.exe -kill -t 000-000-0000 -c client_id -a 1 -q \\.\\com12" where 000-000-0000 is the ISV Client SMS Phone# and client_id is from the previous step -> (When run this command on server, the client will receive SMS message[step 8] and after few minutes the system should be shutdown). 8. Ensure server received SMS message. 9. Verify the system cannot shut down within a few minutes. (The client system should be shut down). 	7.1.2.1041



Issue #	Description	Affected Component/Impact / Workaround/Notes	Fixed in Kit#
3790809	Intel® 6 Series Chipset POST hang during access to ME resources	<p>Affected Component – FW.Kernel.Bring Up</p> <p>Impact: Critical. System will hang during POST with no recovery via G3 or clear CMOS</p> <p>Workaround: none</p> <p>Notes: After flashing image and booting the system for the first time, ME FW will hang during POST. For additional details please refer to Sightings Alert: Intel 6 Series Chipsets POST Hang During Access to ME Resources Sighting# 3623401</p> <p>Issue may happen in following conditions:</p> <ol style="list-style-type: none"> 1. On CPU replacement flow 2. DID timeout (BIOS Error flow) 3. On HMRFPD flow (manufacturing flow only) 4. Flash Descriptor Override (manufacturing flow only) 5. If 5MB FW is loaded on HW SKU only targeted to 1.5MB FW (OEM manufacturing error) 6. If we have a ULV PCH and non ULV/LV CPU (OEM manufacturing error) 	7.0.2.1164
3790607	RCO commands cannot be issued multiple times in a row during POST or when in BIOS setup.	<p>Affected Component – FW.MCTP</p> <p>Impact: ME will not allow RCO commands sent several times in succession.</p> <p>Workaround: none</p> <p>Notes:</p> <ol style="list-style-type: none"> 1) Provision SUT 2) Reboot to BIOS using SoL. 3) Try rebooting the system via DTK/WebUI. 	7.1.0.1028



Issue #	Description	Affected Component/Impact / Workaround/Notes	Fixed in Kit#
3790513	When AC power supply is removed and inserted back when the system is transitioning from S5/M3 to S0/M0 state, ME FW fails to determine the current power source as AC. PmDrvCtxt says the current power source as DC.	<p>Affected Component – FW.Kernel.PowerManagement</p> <p>Impact: Under certain conditions the ME will not correct read the AC / DC transitions.</p> <p>Workaround: none</p> <p>Notes: Mobile Only</p> <ol style="list-style-type: none"> 1) Activate Network and make sure the Power policy is 2 in MEBx 2) Boot to DOS 3) Connect WebUI and select Remote Control 4) Select command as "cycle power off and on" With Normal boot option. 5) Count for 6 or 7 second and remove AC plug 6) Reinsert the AC power supply after 2 seconds 7) make sure AC/DC detection with PmDrvCtxt. (No change -> Problem) 	7.1.0.1028
3553417	The Firmware Update manifest has been changed to prevent upgrades from the Intel® Management Engine Firmware 7.0 SKU 5.0MB Production Candidate or later FW to a Pre-Production 7.1 Firmware.	<p>Affected Component – FW.Kernel</p> <p>Impact: For quality and security reasons, all Pre-Production FW will not work on PRQ parts.</p> <p>Workaround: none</p> <p>Notes: This change is being made to prevent an end user from using FW Update to load 7.1 pre-production FW onto a system in the field. There is no change to the FW Update code, only the data with the upgrade/downgrade restrictions.</p>	7.1.0.1023
3553317	Firmware Watchdog Global reset occurring during power management S0 <--> S3Mon stress testing after approximately 1100 iterations.	<p>Affected Component – FW.Kernel.PowerManagement</p> <p>Impact: Firmware unexpectedly issues a global reset</p> <p>Workaround: restart</p> <p>Notes: <i>This is Mobile specific</i> Reproduction Steps:</p> <ol style="list-style-type: none"> 1. Burn the image disable reboot standby 2. On OS run a stress S0Mon-S3Mon wake by Pwr button 	7.1.0.1023



Issue #	Description	Affected Component/Impact / Workaround/Notes	Fixed in Kit#
3553117	The system shutdowns during POST when AC power is plugged in after CMOS clear	Affected Component – FW.Kernel.PowerManagement Impact: Platform will not come out of S5 state. Workaround: none Notes: Reproduction steps: 1. Set to DC power source only 2. Use a non DeepSx image and disable DeepSx in BIOS 3. Type wrong password three times to generate a Global reset. The platform does not recover.	7.1.0.1023
3551710	HM65 SKU Mgr Test fails on Pentium and Celeron CPU emulations; Wireless display is shown as enabled when it should be disabled.	Affected Component – FW.Kernel Impact: Unexpected behavior. Wireless display should not be enabled for these configurations. Workaround: none Notes: Reproduction steps: 1. Use FITc to build 4 FW images using FW kit, one each of CPU emulations vPro, Core, Pentium and Celeron 2. Flash SUT with each image, and then check the features.	7.1.0.1005
3551117	Ant MEBx error occurs when trying to enable AMT (Intel manageability) after it has been disabled via FOV.	Affected Component – FW.Kernel Impact: Unexpected behavior. Re-enabling AMT through the MEBx should not result in an error. Workaround: re-flash image Notes: Reproduction steps: 1. Burn native image. (when Global lock bit is disabled) 2. Perform CMOS clear. 3. Edit bios setting according to the latest BKM. 4. Boot to OS. 5. Set FeatureShipmentTimeState (AMT disable/enable) to disable through FOV (id: 000B value: 00000002 (must G3 after)). 5. G3 the platform. 6. Enter MEBx and try to enable AMT back.	7.1.0.1005

Closed Issues



Issue #	Description	Affected Component/Impact / Workaround/Notes	Fixed in Kit#
3550817	Setting any FOV value immediately a platform soft reset (ctrl-alt-del) will cause a global reset and firmware hang on reboot.	Affected Component – FW.Kernel Impact: Unexpected behavior. Workaround: Recovery G3. Notes: Reproduction steps: 1. Burn native image. 2. Perform CMOS clear. 3. Edit bios setting according to the latest BKM. 4. Wait for os load and make restart, (if you are on OS selection menu you can press Alt+Ctrl+delete instead). 5. Try to set any FOV value using FPT tool.	7.1.0.1005



6.2 Closed – Integrated Clock Control (ICC)

Issue #	Description	Affected Component/Impact / Workaround/Notes	Fixed in Kit#
3790913	<p>23Hz refresh rate improved solution for higher security and fewer numbers of pop-ups.</p> <p>To reduce frame judder while playing back 23Hz content, currently display driver programs clock bending through CUI, ICC.dll to ICC HW.</p> <p>For this feature to work without being a nuisance to the end-user, UAC must be set to "never notify". As board designers would be motivated to leave UAC on due to legitimate security concerns, the 23 Hz frame judder will be high as a result.</p>	<p>Affected Component: FW.ICC, PCH HW, Graphic driver – Display clock Bending</p> <p>Impact:</p> <p>Workaround:</p> <p>Resolution:</p> <p>The solution is for ME FW to program SSC4 module with default settings that work for all CE modes for 23/29 and 59Hz for 24b color. When user selects any of the CE modes and 23Hz, display driver will simply program display PLL to use SSC4 output. This avoids CUI and ICC.DLL interaction. UAC settings can remain anything above "never notify" in this case. There is no dependency on it. There are no pop-up messages with this solution either.</p>	7.1.2.1041
3552011	Boot timeout ICC recovery from extreme overclocking does not work.	<p>Affected Component – FW.ICC</p> <p>Impact: Overclocking does not work properly when HT / Core disable capabilities are configured.</p> <p>Workaround: Configure image with HT / Core control disabled</p> <p>Notes:</p> <p>Reproduction Steps:</p> <ol style="list-style-type: none">1. Build Overclocking config2. Use CCDC tool to change BCLK to 120MHz for next boot3. Reboot system	7.1.0.1005



6.3 Closed – Software / Tools

Issue #	Description	Affected Component/Impact / Workaround/Notes	Fixed in Kit#
370913	MEManuf tool has been updated to provide a check for firmware incorrectly reporting EPID Group IDs	Affected Component – SW.Tools.MEManuf Workaround: None. Impact: Refer to the Customer Communication provided separately with this release.	7.1.52.1176
3792110	Memory leak in LMS after installing Microsoft* Installer 4.5 on Microsoft* Windows XP system.	Affected Component – SW.AMT.Services Impact: Degradation of memory resources. Workaround: N/A Notes: Reproduction Steps: 1. Boot to Microsoft* Windows and install Microsoft* Installer 4.5. 2. Install system drivers (Chipset, LAN and graphics). 3. Install ME 4. Disable screen saver. 5. Disable Sleep states in power management. 6. Display "a non-pool page" in Device Manager. Allow system to run and monitor non-pool page for LMS.exe.	7.1.50.1172



Issue #	Description	Affected Component/Impact / Workaround/Notes	Fixed in Kit#
3792078	False empty registry folders created in certain flavors of Windows XP by User Notification Service.	<p>Affected Component – SW.TOOLS</p> <p>Impact: False and empty folders in XP registry.</p> <p>Workaround: N/A</p> <p>Notes: On XP, UNS creates a lot of empty folders in registry HKU\DEFAULT\Software\Microsoft\Windows\CurrentVersion\Internet Settings\Digest\Hosts\..</p> <p>Reproduction Steps:</p> <ol style="list-style-type: none"> 1. Open process monitor 2. Set filter: <ol style="list-style-type: none"> a. Process Name = UNS.exe b. Path contains HKU 3. Insert Disk on Key 4. Perform any Ws-man related operation <p>Expected Results: =====</p> <p>UNS doesn't create empty registry keys</p> <p>Actual Results: =====</p> <p>UNS creates about 15 empty registry keys HKU\DEFAULT\Software\Microsoft\Windows\CurrentVersion\Internet Settings\Digest\Hosts\ and looks for reg key with computer name</p>	7.1.40.1161
3791733	FPT unable to read values of certain NVARs using their FOV name.	<p>Affected Component – SW.Tools.FlashProgrammingTool</p> <p>Impact: Unable to extract value by name</p> <p>Workaround: none</p> <p>Notes:</p> <p>Reproduction Steps:</p> <p>N/A</p>	7.1.30.1142



Issue #	Description	Affected Component/Impact / Workaround/Notes	Fixed in Kit#
3791679	FPT read output file command does not create output file but displays successful	Affected Component – SW.Tools.FlashProgrammingTool Impact: False positives on FPT outputs. Workaround: none Notes: Reproduction Steps: 1. fpt -r <name> 2. fpt -r <name> -o out.txt 3. Variable read info is displayed to user, yet no file has been generated with output	7.1.30.1142



Issue #	Description	Affected Component/Impact / Workaround/Notes	Fixed in Kit#
3791890	MEINFO feature retrieve for OEM Tag with value of zero accepts invalid values	<p>Affected Component – SW.Tools.MEINFO</p> <p>Impact: Using retrieve feature option along with value verify against OEM Tag allows invalid values to pass as a value match</p> <p>Workaround: none</p> <p>Notes:</p> <p>Reproduction Steps:</p> <ol style="list-style-type: none">1. do not set OEM_Tag variable. If set to non-zero value, use FPT to update OEM_Tag FOV to 0x000000002. Use MEINFO feature retrieve and value options against "OEM Tag" feature using expected value "meinfo.exe -feat "OEM Tag" - value 0x00000000"3. Use MEINFO feature retrieve and value options against "OEM Tag" feature using invalid values: 0xx123 x123 youfail !no1 "you>fail <p>See OEMTagbug.txt and oembug7120.png for information regarding the possible commands that are accepted as pass.</p> <p>Expected Results: =====</p> <p>in RED characters "Error 9473: OEM Tag actual value is- 0x00000000"</p> <p>Actual Results: =====</p> <p>Result printed on screen in GREEN: "OEM Tag: Success – Values matches FW value.</p>	7.1.30.1142



Issue #	Description	Affected Component/Impact / Workaround/Notes	Fixed in Kit#
3792001	Fwupdlcl tool returns a value of zero for the ERRORLEVEL variable when the tool is used to update from a 1.5 MB image to a 5MB image even though an error message is generated.	Affected Component – SW.Tools.FWUpdLCL Impact. May impact manufacturing line if the ERRORLEVEL variable is used to determine whether the FWupdlcl tool passed or failed Workaround: none Notes: Reproduction Steps: 1) Flash 1.5 MB FW image. 2) Use Fwupdlcl tool to update with a 5 MB FW image 3) Tool exits with Error message but leaves ERRORLEVEL variable at 0	7.1.30.1142
3791881	In IUSMANUF tool, the System Integrator Index displays the following:(0: for first empty slot: >0 for specific slot):	Affected Component – SW.Tools.IUSManuf Impact: User is supposed to use one of three specific slots for the integrator index but tool is only displaying zero as the specific slot and for the first empty slot. Workaround: none Notes: Reproduction Steps: <ol style="list-style-type: none"> Flash SUT with latest 7.1 FW Set default BIOS settings. Using IUSMANUF tool from the latest kit, use the following command: ISUmWin.exe -setid Result: System integrator ID: 909090 System Integrator Index (0: for first empty slot: >0 for specific slot):	7.1.30.1139



Issue #	Description	Affected Component/Impact / Workaround/Notes	Fixed in Kit#
3791846	MEMANUF -EOL -VERBOSE -PAGE fails to pause, only occurs in DOS	<p>Affected Component – SW.Tools.MEMANUF</p> <p>Impact: MEMANUF information is garbled with certain handles.</p> <p>Workaround: none</p> <p>Steps to Reproduce:</p> <ol style="list-style-type: none"> 1. Flash image. 2. Boot to DOS. 3. Execute MEMANUF -EOL -VERBOSE -PAGE <p>Expected Results: =====</p> <p>EOL test executes, and debug information is displayed on STOUT with pauses after each page of data.</p> <p>Actual Results: =====</p> <p>No pause occurs. EOL test executes and all information scrolls out on STOUT without interruption.</p>	7.1.30.1142
3791964	MEInfo using invalid trademark name for DAL (Dynamic Application Loader)	<p>Affected Component – SW.Tools.MeInfo</p> <p>Impact:</p> <p>Workaround:</p> <p>Notes: Trademark name for Dynamic Application Loader DAL is now displayed when using MEInfo</p>	7.1.20.1119
3791370	updparam tool fails when trying to change passwd and network access	<p>Affected Component – SW.Tools.UpdParam</p> <p>Impact: Updparam changed password after sending Complete configuration. However, when FW sees complete configuration request and the password is the default MEBx password, it returns an error.</p> <p>Workaround: The fix is to change the password first before sending complete configuration.</p> <p>Notes: N/A</p>	7.1.20.1119



Issue #	Description	Affected Component/Impact / Workaround/Notes	Fixed in Kit#
3791484	MEFW update failure/Unable to access MEBx on BIOS update	<p>Affected Component – SW.Tools.FWUpdLcl</p> <p>Impact: On some systems after applying a BIOS update which contains an MEFW update systems the following error message is seen during the update: "ME Firmware Update Failed!" "Could not access the firmware storage device"</p> <p>On reboot MEBx is no longer accessible and system is not AMT manageable.</p> <p>Workaround: N/A</p> <p>Notes: N/A</p>	7.1.20.1119
3791553	The option to name an output file when using the NVAR Retrieve function uses '-f <>' instead of '-o <>'	<p>Affected Component – SW.Tools.FlashProgrammingTool</p> <p>Impact: By convention, the Flash Programming Tool, FPT, uses the '-o <fileName>' command line option to specify an output file is desired. For the NVAR Retrieve function it is specified using '-f <>'.</p> <p>Workaround: N/A</p> <p>Notes: N/A</p>	7.1.20.1119
3791497	Due to a tool implementation issue, MEInfo tool may incorrectly report PCH Revision ID.	<p>Affected Component – SW.Tools.MeManuf</p> <p>Impact: Previous MEInfo versions may display incorrect chipset information.</p> <p>Workaround:</p> <p>Notes: Optional MEInfo fix.</p> <p>N/A</p>	7.1.13.1088
3791285	Immediately after reboot, FPT Display option "-i" (FPT -i) returns error with EFI and 64-bit versions of FPT.	<p>Affected Component – SW.Tools.FlashProgrammingTool</p> <p>Impact: Fixes two errors when running FPT -i prior to other ME tools (e.g. MEInfo or MEManuf). Operator will see "Signature: INVALID!" and "Error 400: Flash descriptor does not have correct signature."</p> <p>Workaround: Run MEInfo prior to running FPT Display option in EFI or 64-bit versions.</p> <p>Notes:</p> <p>Reproduction Steps: 1. Run 'ftp -i' after bootup and prior to running MEInfo or MEManuf</p>	7.1.10.1065



Issue #	Description	Affected Component/Impact / Workaround/Notes	Fixed in Kit#
3791081	When selecting an image greater than 16MB in FITC, (for example 2 SPI devices with total density > 16MB, produced image does not have correct Flash Region Register Base and Limits for any region above 16MB. The base and limit that is in the descriptor does not correspond to what's in the .map file.	Affected Component – SW.Tools.FlashProgrammingTool Impact: Regions overlap, which results in platform not able to boot or ME errors. Workaround: none Notes: Reproduction Steps: 1. Open FITC 2. Select Number of Flash Components = 2 3. Under Component Section, select each flash density 16MB (can also be 1=16MB. Total image size has to be greater than 16MB 4. Include ME, BIOS, and PRD region 5. Open the output.map file 6. Open output.bin (32MB) with hex editor 7. Compare base and length defined in the .bin file starting at offset 0x40 with the addresses in the .map file. 8. Notice that any region that resides at offset greater than 16MB will have incorrect limit or base or both because FITC doesn't set bits 12 or 28 which map out to be bit 24 of the base address or base ending address	7.1.10.1065
3791018	MEManuf -S5 will not work with non-vPro CPU; displays message "Error 9296: MEManuf Operation Failed (1000)"	Affected Component – SW.Tools.MeManuf Impact: Low. Workaround: Executing "MEMANUF – S0 –no3g" skips this test. Notes: Reproduction Steps: 1. Run command MEManuf –S5 MEManuf tool will display "Error 9296: MEManuf Operation Failed (1000)"	7.1.10.1065



Issue #	Description	Affected Component/Impact / Workaround/Notes	Fixed in Kit#
3553415	Flash Programming Tool (FPTW.exe) fails to disable ME causing system to hang intermittently.	<p>Affected Component – SW.Tools.FlashProgrammingTool</p> <p>Impact: When erasing the ME region in flash the ME must be disabled. This was being done for most accesses except when doing a Chip Erase (FPTW.exe -c).</p> <p>Workaround: none</p> <p>Notes:</p> <p>Reproduction Steps:</p> <ol style="list-style-type: none"> 1. Flash FW with current SPI image 2. Reset system (G3) 3. Boot OS as normal 4. At command prompt <ol style="list-style-type: none"> a. Run fpt.exe -c b. Run fpt.exe -b c. Run fpt.exe -f full_image.bin -desc d. Run fpt.exe -f full_image.bin -bios e. Run fpt.exe -f full_image.bin -me f. Run fpt.exe -f full_image.bin -gbe g. Run fpt.exe -f full_image.bin -pdr h. Run fpt.exe -verify full_image.bin 5. Reboot System/G3 power cycle 6. At command prompt run meinfo.exe to verify FW version <p>Expected Results:</p> <ol style="list-style-type: none"> 1. After each command there should be a message indicating the operation was successful. 2. At step 5. The system should restart and load OS normally. 3. The FW version number in step 6. Should be the same as what is in the binary_image.bin. <p>Actual Results:</p> <ol style="list-style-type: none"> 1. From step 4.A. through 4.E. the system will intermittently lock or hang. 2. The execution of 4.A. initiates system instability. 	7.1.10.1065



Issue #	Description	Affected Component/Impact / Workaround/Notes	Fixed in Kit#
3790870	MEManuf reports failure of WLAN BIST when using Condor Peak WLAN	<p>Affected Component – SW.Tools.MeManuf</p> <p>Impact: MEManuf performs WLAN BIST with non-vPro systems when Condor Peak WLAN card is detected.</p> <p>Workaround: none</p> <p>Notes:</p> <p>Reproduction Steps:</p> <ol style="list-style-type: none"> 5. Configure 5 MB QM67 image with WLAN Power Well Config set to 0x80 (disabled) in ME Region->Configuration->ME. 6. Flash on mobile system 7. Run MEManuf 8. MEManuf will fail on WLAN BIST 	7.1.10.1065
3790750	The Intel ® DAL permanent disable value does not decompose to the correct value.	<p>Affected Component – SW.Tools.FlashImageTool</p> <p>Impact: Intel ® DAL permanent disable unexpectedly set to "No" after decomposing 7.1 images despite value set to "Yes".</p> <p>Workaround: none</p> <p>Notes:</p> <p>Reproduction Steps:</p> <ol style="list-style-type: none"> 1. Create a flash image in FITC with "Intel ® DAL" permanent disable set to "Yes". 2. Drag and drop the binary image into FITC to decompose it. The value of Intel ® DAL will be reset back to "No" instead of "Yes". 	7.1.2.1041
3790489	FW Update Tool error message is unclear when downgrading to blacklisted firmware version.	<p>Affected Component – SW.Tools.FwUpdLcll</p> <p>Impact: The Unclear error message would confuse end users.</p> <p>Workaround: none</p> <p>Notes:</p> <p>Reproduction Steps:</p> <ol style="list-style-type: none"> 3. Use FWUpdLcl.exe in either Windows or DOS, try to downgrade from PC (1014) to an older version (like 1009). 4. The Update will fail as expected, but the message provided does not clearly state WHY the downgrade failed. 	7.1.0.1023



Issue #	Description	Affected Component/Impact / Workaround/Notes	Fixed in Kit#
3553383	FPT displays Intel(R) QM67 Express Chipset Revision: Unknown	Affected Component – SW.Tools.FlashProgrammingTool Impact: FPT tool cannot display CPT Revision ID if it is B2 stepping or later. Workaround: none Notes: Reproduction Steps: 1. Flash ME FW 7.1.0.1014 signed image to system 2. Boot to DOS 3. FPT -d Dump_1014.bin	7.1.0.1023
3553251	7.0 MEInfo -feat "^"OEM Tag "^"-fails even when correct value is supplied	Affected Component – SW.Tools.MeInfo Impact: The OEM Tag option using '-feat' fails when using the correct value Workaround: none Notes: Reproduction Steps: 1. Flash Image, Setup BIOS setup as normal 2. FPT -u -n "^"OEM_Tag"^-v "^"TestValueBit31 set"^- {sets up OEM Tag} 3. FPT -commit {Commits variable to system} 4. Meinfo -feat "^"OEM Tag"^- {returns value set buy FPT} 5. Meinfo -feat "^"OEM Tag"^-value "^" TestValueBit31 set ^"	7.1.0.1023



Issue #	Description	Affected Component/Impact / Workaround/Notes	Fixed in Kit#
3553233	After Manufacturing mode has been disabled, running the DOS fpt -closemnf command again does not return an error as expected.	<p>Affected Component – SW.Tools.FlashProgrammingTool</p> <p>Impact: The DOS FPT tool does not generate an error when the -closemnf is executed again.</p> <p>Workaround: none</p> <p>Notes:</p> <p>Reproduction Steps:</p> <p>On either Desktop or Mobile CRB. Build an image with any SKU. Under Windows 7 (32bit) or Windows Vista (32bit).</p> <ol style="list-style-type: none">1. open command line as admin2. run fptw -closemnf no3. manually perform G34. boot to OS, run MEInfowin -fwsts and confirm manufacturing mode has been disabled5. Run fptw -closemnf no again and receive the below error: <p>Error 26: The host CPU does not have read access to the target flash area. To enable read access for this operation you must modify the descriptor settings to give host access to this region.</p> <p>Unable to perform closemnf.</p> <p>Error 26: The host CPU does not have read access to the target flash area. To enable read access for this operation you must modify the descriptor settings to give host access to this region.</p> <ol style="list-style-type: none">6. Run fpt -closemnf no under DOS will receive a pass with below message: The ME Manuf Mode Bit and the Region Access Permissions are already set. FPT Operation Passed	7.1.0.1023



Issue #	Description	Affected Component/Impact / Workaround/Notes	Fixed in Kit#
3552907	MEManuf SMBus Read Byte test fails intermittently	Affected Component – SW.Tools.MeManuf Impact: The tool fails operate as expected. Workaround: none Notes: Reproduction Steps: 1. Boot system to DOS 2. Run MEManuf -S0 -verbose 3. Check result 4. Repeat step 1,2,3 to get fail log	7.1.0.1005
3551884	The '-forcereset' command does not trigger reset on the fwUpdLclEfi tool.	Affected Component – SW.Tools.FwUpdLcl Impact: The -forcereset command does not reset the platform on the EFI tool. Workaround: none Notes: Reproduction Steps: 1. use FwUpdLclEfi to perform update using the -forcereset option	7.1.0.1005
3551843	Changing the slew rate for Flex1 on the "FITC Wizard - ICC Profile n Single Ended Clocks" page does not trigger a corresponding update to ICC Parameter values	Affected Component – SW.Tools.FlashImageTool Impact: Workaround: Need manually change the value using the FITC interface. Notes: Reproduction Steps: 1. Load valid images 2. Go the "FITC Wizard - ICC Profile n Single Ended Clocks" page 3. Change the value of Flex1 Slew Rate	7.1.0.1005
3551804	When using the blank check (-b) option in FPTEFI it is returns 'assertion' error.	Affected Component – SW.Tools.FlashProgrammingTool Impact: Tool will unexpectedly error out when using -b switch. Workaround: Enable Descriptor Override Notes: Reproduction Steps: 1. boot to bootable USB containing EFI tool files for FPTEFI 2. run 'FPTEFI -b'	7.1.0.1005



Issue #	Description	Affected Component/Impact / Workaround/Notes	Fixed in Kit#
3551803	The FPT '-commit' option returns warning error with the following FOVs: 0x000E -- SetWLANPowerWell 0x2008 -- MEIdleTimeout 0x6001 -- ATFPOPHard 0x6002 -- ATFPOPSoft	Affected Component – SW.Tools.FlashProgrammingTool Impact: Unexpected behavior. Warnings being returned however values still get programmed correctly. Workaround: none Notes: Reproduction Steps: 1. use FPT to update FOVs: - SetWLANPowerWell (0x000E) - MEIdleTimeout (0x2008) - ATFPOPHard (0x6001) - ATFPOPSoft (0x6002) 2. immediately after FOV update, use the -commit option to commit changes	7.1.0.1005
3551653	System reboots when using FPTEFI in EFI without ME disabled. Reboot does not occur when using FPT in DOS without ME disabled.	Affected Component – SW.Tools.FlashProgrammingTool Impact: Platform unexpectedly reboots when using FPTEFI when ME is enabled. Workaround: Disable ME Notes: Reproduction Steps: 1. Boot to EFI with ME enabled in MEBx 2. fs0: 3. cd into correct folder 4. fpTEFI -f <nameofimage>	7.1.0.1005
3551622 / 3551380	Using FPT to read the ME Variables supported is returning Error 522 for "PKI DNS Suffix" and "Remote Configuration Enabled".	Affected Component – SW.Tools.FlashProgrammingTool Impact: FPT returns an error when trying to read the PKI DNS Suffix and Remote Configuration Enabled NVARs. Workaround: provision platform Notes: Reproduction Steps: 1. flash image, setup BIOS, enter DOS 2. run FPT -r "PKI DNS Suffix" or "Remote Configuration Enabled"	7.1.0.1005
3551559	MeInfo returns and 'Invalid Usage' error when the '-fwsts' and '-verbose' commands are used together.	Affected Component – SW.Tools.MeInfo Impact: MeInfo will return an error instead of accepting these two commands together. Workaround: Use fwsts and verbose command separately Notes: Reproduction Steps: 1. meinfo -fwsts -verbose	7.1.0.1005



Issue #	Description	Affected Component/Impact / Workaround/Notes	Fixed in Kit#
3551534	Skipping the erase command when flashing the ME region will cause the platform to hang.	<p>Affected Component – SW.Tools.FlashProgrammingTool</p> <p>Impact: Not erasing the ME region during and ME only region flash will cause platform hang.</p> <p>Workaround:</p> <p>Notes: Do not skip the erase command when doing ME only region flashing.</p> <p>Reproduction Steps:</p> <ol style="list-style-type: none"> 1. HECI driver installed 2. ME disabled from MEBx <p>Flash ME region images using "Region" and "Skip Erase" options</p> <ol style="list-style-type: none"> 1. fpt.exe -erase -me 2. fpt.exe -f me_image.bin -me -e 3. Reboot System/G3 power cycle in automation. 	7.1.0.1005
2753005	FPT tool is able to use the '-erase' and the '-address' option n same command line argument.	<p>Affected Component – SW.Tools.FlashProgrammingTool</p> <p>Impact: Unexpected behavior. FPT does not return and error as expected when these two options are combined.</p> <p>Workaround: Use the -erase and -address option separately</p> <p>Notes:</p> <p>Reproduction Steps:</p> <ol style="list-style-type: none"> 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 	7.1.0.1005



6.4 Closed – Intel® Anti-Theft Technology

Issue #	Description	Affected Component/Impact / Workaround/Notes	Fixed in Kit#
3551888	GpsLocationBeaconNotification messages received after ConfigureGpsLocationBeaconing(enable=false)	<p>Affected Component – FW.TDT</p> <p>Impact: GPSLocationBeaconNotification messages being received.</p> <p>Workaround: none</p> <p>Notes:</p> <p>Steps to Reproduce:</p> <ol style="list-style-type: none"> 1. Flash image on platform with Fitc to set MCTP enable=true, address=0x30. 2. Flash platform, Set BIOS default (AT enabled), boot to OS 3. Provision AT, run Basic-Setup.bat, ConfigureSMS, GetMEIK, SetClientId 4. ConfigureLocationBeaconing(Enable=true, TimeInterval=60, TxCount=6, TriggerMask=0x2), AssertStolen, call GpsLocationBeaconNotification 6 times, DeAssertStolen. 5. ConfigureLocationBeaconing(Enable=false, TimeInterval=60, TxCount=6, TriggerMask=0x2), AssertStolen 6. Call GpsLocationBeaconNotification 6 times. 	7.1.0.1005
3550901	HECI failure observed after clearing CMOS while in Suspend state.	<p>Affected Component – FW.TDT</p> <p>Impact: Getstate will fail to open the HECI client.</p> <p>Workaround: none</p> <p>Notes:</p> <p>Steps to Reproduce:</p> <ol style="list-style-type: none"> 1. Flash FW, Set Default BIOS settings 2. Provision AT-p, GetPublicKey, SetPublicKey, SetCredential 3. GetState, SetSuspendModeRemote, GetState 4. Clear CMOS. Set BIOS default settings. Boot to OS 5. Query Getstate 	7.1.0.1005



6.5 Closed – Intel® Upgrade Service

Issue #	Description	Affected Component/Impact / Workaround/Notes	Fixed in Kit#
3534838	ME RESET is being counted toward PCH MTP Period Boot Count.	<p>Affected Component – FW.CLS</p> <p>Impact: MTP period boot count would expire earlier than expected.</p> <p>Workaround:</p> <p>Notes:</p> <p>Steps to Reproduce:</p> <p>Flow-A</p> <p>=====</p> <ol style="list-style-type: none"> 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 be 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. <p>Flow-B</p> <p>=====</p> <ol style="list-style-type: none"> 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) <p>MTP Permit is De-Activated after 2nd ME Reset, although ME Reset should not have been counted.</p>	7.1.0.1005



6.6 Closed – Not Firmware Issue

Issue #	Description	Affected Component/Impact / Workaround/Notes
3584530	MEBx will present incorrectly extended ASCII text ,when vBios code page is not standard English (437)	Affected Component – ExternalDependency Impact: MEBx AMT User consent text containing letters in the range ASCII 128-255 might be displayed incorrectly. Workaround: Set the user consent language from localized back to English (can be done programmatically or through IMSS). Note: This could also affect the setting of sprite language in the case of switchable GFX. Notes: Reproduction Steps: <ol style="list-style-type: none">1. Install SUT with graphic card containing vbios without standard code page.2. Test user consent in mebx showing message with extended ASCII incorrectly.
3551877	SMS GpsLocationBeaconingNotification fails to detect beacon messages from FW with trigger mask 0x8 (Attack Detected)	Affected Component – FW.TDT Impact: There are no Beacon messages being seen. Workaround: none Notes: Steps to Reproduce: <ol style="list-style-type: none">1. Using Fitc, modify FW to enable MTCP and set MTCP address 0x302. Flash platform, enter BIOS enable AT. Boot to OS, Provision AT, run Basic-Setup.bat3. ConfigureSMS, GetMEIK, SetClientId, ConfigureGpsLocationBeaconing(BeaconEnable=Enabled, TimeInterval=60, TxCount=4, TriggerMask=0x8) enable PBAM after EOP.4. Clear CMOS, boot to OS, GetState(State=Stolen, Theft Trigger=Attack Detected)5. call SmsGpsLocationBeaconingNotification
3550806	Host wake on Magic Packet not waking platform after a G3 exit to S5. It does work with S0 -> S5 power flow.	Affected Component – ExternalDependency Impact: Platform will not respond to Magic Packet. Workaround: none Notes: Reproduction Steps: <ol style="list-style-type: none">1. Setup BIOS, set it to S5 after g3 save and exit2. Boot up to windows S0/M03. Graceful shutdown4. G3 Turn power off5. AC Turn power back on6. Send a magic packet to bring the SUT back to S0/M0



Issue #	Description	Affected Component/Impact / Workaround/Notes
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



6.7 Closed – No Plan to Fix

Issue #	Description	Affected Component/Impact / Workaround/Notes
3551778	AuditLog does not get updated with new record when a firmware update failure occurs.	<p>Affected Component – FW.Kernel.FWUpdate</p> <p>Impact: If firmware update fails there will be no corresponding event record to indicate this.</p> <p>Workaround: none</p> <p>Notes:</p> <p>Deferred to future project</p> <p>Reproduction steps:</p> <ol style="list-style-type: none">1. Make provisioning in ACM mode, set the default.config.xml to enable the audit log.2. Set "Firmware Update failed" event to be enabled by the AMT_AuditPolicyRule.SetAuditPolicy method. Enable – 1 AuditAppID – 19 EventId – 1 Flag – 03. Perform Firmware Update, use an invalid image Use FW update windows tool from: \Tools\System Tools\FWUpdate\Local-Win, and run locally: "fwupdlcl -f [image name] -generic " Image is located on the kit in: Image Components\ME. FW update process should fail.4. Read Audit log's records.
3551045	Setting End of Manufacture using FITC causes more boots on Mobile platform than it does on Desktop platforms.	<p>Affected Component – FW.CLS</p> <p>Impact: Permit attribute of MTP is not active as expected.</p> <p>Workaround: none</p> <p>Notes:</p> <p>Deferred to future project</p> <p>Steps to Reproduce:</p> <ol style="list-style-type: none">1. Use FSTApp to generate PCH MTP binaries with periodtype=1, period=3, Execution time=5 minutes, Expiration time=30 minutes.2. Use FITc to build PCH MTP image with resolution set to Minutes and Globallock set.3. Flash via Dediprog/FPT > G3(unplug power) > Reapply Power > Boot to BIOS > Set following Parameters: 3a. Set SATA Mode = IDE [ADV > CONFIG > SATA CONFIG] 3b. F4 to Save and Exit4. Boot to OS5. Check the permit attributes of PCH MTP.



6.8 Closed – Documentation Change

Issue #	Description	Affected Component/Impact / Workaround/Notes
3792059	Update Patsburg SPI Programming Guide FITC PCH Strap 16 -> Bit 14 & 18 for Patsburg are Disable & Changeable.	<p>Affected Component – Documentation.SPIFlashProgramming Guide</p> <p>Impact: SPI Programming Guide does not have guidance for FITC setting.</p> <p>Workaround: N/A</p> <p>Notes: PCH Softstrap 16 bits 14 and 18 have been documented as Reserved and default setting as "1" in Patsburg_SPI_Programming_Guide_454672_rev_1.63.pdf.</p>
3534716 / 3534717 / 3535281	Executing FPT with the '-c' command line parameter results in 'error 27' being returned.	<p>Affected Component – Documentation.SystemToolsUserGuide4MB</p> <p>Impact: FPT returns an error 27 Host CPU does not have erase access to target flash area.</p> <p>Workaround: Either limit the area to the area available using the -length command *or* create a 2 SPI component image.</p> <p>You know it will error out when you receive the message in FPT:</p> <p>"Warning: There are some addresses that are not defined in any regions. Read/Write/Erase operations are not possible on those addresses"</p> <p>Notes:</p> <p>Reproduction Steps:</p> <ol style="list-style-type: none"> 1. From dos command line in FPT-Win...FPT.exe -c



7 Known Issues

7.1 Open – Intel® ME Kernel

Issue #	Description	Affected Component/Impact / Workaround/Notes

7.2 Open – Integrated Clock Control (ICC)

Issue #	Description	Affected Component/Impact / Workaround/Notes
BUP000001	<p>27-MHz FLEX Clock (for switchable graphics) has unexpected output value, unless Display PLL ownership is transferred to Intel® ME.</p> <p>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.</p>	<p>Affected Component: FW.ICC</p> <p>Impact:</p> <p>Workaround: The following bits need to be edited as specified to utilize on-board graphics down devices that use 27-MHz FLEX clock from Cougar Point:</p> <ul style="list-style-type: none">• PLEN bit 9 = 1b (Enable ME Ownership)• DPLLBC bit 30 = 1b (Enable DPLLB) <p>Optional steps 3 and 4 If 27-MHz SSC clock is needed from CPT:</p> <ul style="list-style-type: none">• DPLLAC bit 30 = 1b (Enable DPLLA)• DPLLAC bits 26:24 = 011b (Enable 27M spread on DPLLA) <p>This editing can be done in one of two ways:</p> <ul style="list-style-type: none">• 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. <p>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.</p>



7.3 Open – Software / Tools

Issue #	Description	Affected Component/Workaround/Notes
3551432	When installing the MEI-Only Installer the 'Readme File Information' windows shown to the user is empty.	Affected Component – Build Impact: Readme information section blank in installer. Workaround: none Notes: Reproduction Steps: 1. Open the Installers folder start MEI-Only installation

7.4 Open – Intel® Anti-Theft Technology

Issue #	Description	Affected Component/Impact / Workaround/Notes

7.5 Open – Intel® Identity Protection Technology

Issue #	Description	Affected Component/Impact / Workaround/Notes

7.6 Open – Intel® Upgrade Service

Issue #	Description	Affected Component/Impact / Workaround/Notes

7.7 Open – Not Firmware Issue

Issue #	Description	Affected Component/Impact / Workaround/Notes
4027368	AT7.1.20 Power: When using SATA port 4 Platform fails to load SuSE Linux OS (~10% of time for DT and ~5% for MBL)	Affected Component: BIOS Impact: Some failures with SATA ports loading Linux Workaround: none Notes: Reproduction Steps: 1. Burn Image 2. Load SuSE Linux OS. 3. Move to S5. 4. Repeat steps 2-3 until reproduced (should happens within a few flows).



7.8 Open - Documentation Change

Issue #	Description	Affected Component/Impact / Workaround/Notes
3792037	Patsburg SPI Programming Guide doesn't explain bits PCH Strap 16 Bits 27:24	Affected Component – SW.AMT.Docs Impact: Document lacks details for configuration. Workaround: N/A Notes:

§