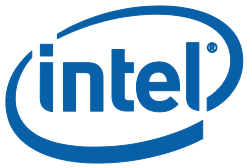

# Intel® 7 Series/C216 Chipset Family

# Intel® Management Engine

# Firmware 8.1 SKU

**1.5MB Readme / Release Notes - NDA**

***January 2013***

***Revision 8.1.30.1350 Maintenance Release (MR)***

**Intel Confidential**

# Contents

# Revision History

| Revision Number | Description | Revision Date |
|---|---|---|
| 8.1.0.1035 | Alpha Release | December 2011 |
| 8.1.0.1143 | Beta Release | March 2012 |
| 8.1.0.1248 | Production Candidate (PC) Release | June 2012 |
| 8.1.0.1248 | Production Version (PV) Release | July 2012 |
| 8.1.2.1318 | Hot Fix 2 (HF2) Release | September 2012 |
| 8.1.3.1325 | Hot Fix 3 (HF3) Release | September 2012 |
| 8.1.10.1286 | Production Version (PV) Release for Intel® Management Engine Firmware 8.1 Intel® C600 Series Express Chipset | August 2012 |
| 8.1.20.1336 | Maintenance Release | November 2012 |
| 8.1.20.1336v2 | Maintenance Release | December 2012 |
| 8.1.30.1350 | Maintenance Release | January 2013 |

§

# 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 |
|---|---|
| BLU-RAY PLAYBACK | Blu-ray™ Playback |
| BIOS | Basic Input Output System |
| CRB | Intel® Customer Reference Board |
| Intel® DAL | Intel® Dynamic Application Loader (Intel® DAL) |
| 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 |
| 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) |
| Intel® PDA | Intel® Platform Debug Analyzer (platform debug tool formerly referred to as MDES or Intel® MEDebug) |
| LAN | Local Area Network |
| LMS | Local Manageability Service |
| MAC | Media Access Control |
| MOF | Managed Object Format |
| ISV | Independent Software Vendor |
| MRC | Memory Reference Code |
| OS | Operating System |
| PCH | Platform Control Hub |
| PKI-CH | Public Key Infrastructure with Certificate Hashing |

| Term | Description |
|---|---|
| SOL | Serial over LAN |
| SBT | Intel Small Business Technology |
| SPI | Serial Peripheral Interface |
| SUT | System Under Test |
| SVN | Security Version Number. Used in Firmware Upgrade / Downgrade capabilities |
| TDT | Theft Deterrence Technology. Previous name for AT-p, which is part of the Intel® Anti-Theft Technology. |
| VCN | Version Control Number. Used in Firmware Upgrade / Downgrade capabilities |
| WMI | Windows Management Instrumentation |
| WSI | Web Services Interoperability Organization |

# 2 Release Kit Summary

This document covers the following Intel® Management Engine Firmware SKUs for the Intel® 7 Series/C216 Chipset Family and Cougar Point platforms:

- Intel® Management Engine Firmware 8.1 Intel® 7 Series Express Chipset
  - Consumer
- Intel® Management Engine Firmware 8.1 Intel® 6 Series Express Chipset
  - Consumer

Kit release information is outlined below:

## 2.1 Release Kit Details

* **Firmware Support**: Intel® Anti-Theft, PAVP, Intel® IPT

* **Release** : Intel® Management Engine Firmware 8.1 Intel® 7 Series Express Chipset MR Release – 8.1.30.1350

  Intel® Management Engine Firmware 8.1 Intel® 6 Series Express Chipset MR Release – 8.1.30.1350

* **Target Platform** : Ivy Bridge or Sandy Bridge & Intel® Series 7/C216 Chipset Family

  Ivy Bridge or Sandy Bridge & Cougar Point Chipset Family

* **.zip name** : ME8_1.5M_8.1.30.1350 .zip

**Contents:**

- Intel® Management Engine Firmware (for Intel® 7 and 6 Series Express Chipset Family / PCH platform)
- GbE PCH SPI components
- Intel Reference System BIOS

## 2.2 Kit Overview

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

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

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

## 2.3 Contents of Downloaded Kit

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

Drivers are included in:

- ME8_1.5M_8.1.30.1350 .zip

### 2.3.1 Intel® SW Components

| Installers | Description |
|---|---|
| ME_SW | • Intel® MEI is the interface between the host and the Intel® Management Engine firmware.<br>• 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.<br>• Intel® MEI driver is installed by running: C:\[skuName_x.x.xxxx]\Installers\ME_SW\Setup.exe<br>• The Intel® MEI driver can also be installed using the 'Have Disk' method in 'Device Manager', as follows:<br>  ○ Right click '**My Computer**' and select **Properties**.<br>  ○ Select the **Hardware** tab and click **Device Manager**.<br>  ○ Scan for hardware changes.<br>  ○ Update the particular device driver by pointing to the INF file: C:\[skuName_x.x.xxxx]\ME_SW\Installers\Drivers\ \MEI\HECI.inf. |

| Installers | Description |
|---|---|
| ME_SW_IS | • The ME_SW_IS installer will install the same components as ME_SW but using an InstallShield wrapper. |

### 2.3.2 Image Components

NVM Images are included in:

- ME8_1.5M_8.1.30.1350.zip

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

| Image | Description |
|---|---|
| BIOS | • Contains Intel Reference System BIOS<br>• Supported devices: Intel® 7 Series/C216 Chipset Family and Cougar Point Chipset PCH Families<br>• 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.<br>• BIOS image components are located in the following directory: C:\ [kit]\Image Component\BIOS\<br>• For latest release information and known issues on the BIOS, please refer to the Intel® ME BIOS Writer's Guide. |
| ME | • The Intel® Management Engine firmware contains code and configuration data for Intel® Management Engine functions.<br>• 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.<br>**NOTES:**<br>• For more details on building the flash image, please refer to **1.5MB FW Bringup Guide.pdf**, included in the downloaded kit.<br>• For more details on the firmware and related issues, please refer to **Important Notes** section, of this document. |
| GbE | • 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.<br>• 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.<br>• The GbE image will be programmed into the SPI flash as part of this integrated image using the Flash Programming Tool.<br>• The GbE folder contains images for C0 PHY silicon. Example: NAHUM5_LEWISVILLE_DESKTOP_13.bin. This image can be used with any of the Intel® Management Engine images. |

### 2.3.3 System Tools

System Tools are included in:

- ME8_1.5M_8.1.30.1350 .zip

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

| Tool | Description |
|---|---|
| Flash Image Tool – fitc.exe | • Provides both a GUI and a command line tool.<br>• OS Support –<br>  • Windows XP SP3, Vista SP1* (32-bit & 64-bit), Windows 7 (32-bit & 64-bit), Windows 8 (32-bit & 64-bit), Windows Server 2003, Windows Server 2008 (32-bit & 64-bit).<br>• 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 | • Provided as DOS and Windows* command line tools.<br>• OS Support –<br>  • MS DOS 6.22 and later, DRMK and FreeDOS.<br>  • The Windows version (fptw.exe) will run in Windows PE, Windows XP SP3, Vista SP1, Windows 7 (32-bit & 64-bit), Windows 8 (32-bit & 64-bit), Server 2003, and 2008 R2 (32-bit & 64-bit).<br>• Used to write the flash image into the SPI flash device. |
| FWUpdate – FWUpdLcl Tools | • Provided as DOS and Windows* command line tools.<br>• OS Support –<br>  • MS DOS 6.22 and later, DRMK and FreeDOS.<br>  • The Windows version will run in Windows PE, Windows XP SP3, Vista SP1, Windows 7 (32-bit & 64-bit), Windows 8 (32-bit & 64-bit), Server 2003, and 2008 R2 (32-bit & 64-bit).<br>• Used to update the Intel® Management Engine's firmware. |
| MEInfo | • Provided as DOS and Windows* command line tools.<br>• OS Support –<br>  • MS-DOS 6.22 and later, DRMK and FreeDOS.<br>  • Windows Command line executable for Windows (Intel® MEInfoWin) is supported on Windows PE, Windows XP SP3, Vista SP1, Windows 7 (32-bit & 64-bit), Windows 8 (32-bit & 64-bit), Server 2003, and 2008 R2 (32-bit & 64-bit).<br>• Verifies that Intel® Management Engine (Intel® ME) firmware is alive and returns data about Intel® ME. |

| Tool | Description |
|---|---|
| MEManuf | • Provided as DOS and Windows* command line tools.<br>• Used on the manufacturing line to validate an Intel® Active Management Technology device.<br>• OS Support –<br>  • MS-DOS 6.22 and later, DRMK and FreeDOS,<br>  • Windows PE, Windows XP SP3, Vista SP1, Windows 7, Server 2003, and 2008 R2 (32-bit & 64-bit). |
| UpdParam | • Provided as a DOS command line tool.<br>• OS Support –<br>  • MS-DOS 6.22 and later, DRMK and FreeDOS,<br>• Windows PE, Windows XP SP3, Vista SP1, Windows 7 (32-bit & 64-bit), Windows 8 (32-bit & 64-bit), Server 2003, and 2008 R2 (32-bit & 64-bit).<br>• UpdateParam tool is used to change certain ME firmware parameters (both Intel AMT and Kernel) after the global valid bit is set and descriptor region is locked. |

### 2.3.4 ICC Tools

| Tool | Description |
|---|---|
| Clock Commander Tool (CCT) | • ICC Tool to get ICC registers and settings, see *ICC Tools User Guide* for more information.<br>• OS Support –<br>  • MS-DOS 6.22 and later, DRMK and FreeDOS.<br>  • EFI<br>  • Windows 7 (32-bit & 64-bit) and Windows 8 (32-bit & 64-bit). |

## 2.4 Release Version Numbering Information

Typical release version numbering is as follows,

**8.x.y.z** (for example: 8.1.0.xxxx) where

**'8'** refers to the Intel® Management Engine 8.1 Firmware SKU for the Intel® 7 Series/C216 Chipset Family and Cougar Point based platforms

**'x'** represents point releases such as 8.1 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 Firmware Update Information

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

### 2.5.1 Firmware Update Terminology

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

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

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

**Update rules:**

- If the system is at PV (Production Version) quality firmware that has PV bit set, update to non-PV firmware is not allowed. Only Non-PV to PV is allowed.
    - Example: 8.0.0.1351 PV cannot upgrade to 8.1.0.1035 Beta
- Update to firmware that has lower SVN (Security Version Number) is not allowed.
- Update to firmware that has lower VCN (Version control number) is not allowed.
- Update across major point release is not allowed for example 8.x to 9.x.

- If firmware update setting in Intel® MEBX is password protected, Intel® MEBX password must be supplied during the update.

### 2.5.2 VCN Firmware Upgrade / Downgrade Table

| Intel® ME FW Version | SVN # | VCN # | PV (1 or 0) |
|---|---|---|---|
| **8.1.30.1350 (8.1 MR)** | 1 | 2 | 1 |
| **8.1.20.1336 (8.1 MR)** | 1 | 2 | 1 |
| **8.1.3.1325 (8.1 HF3)** | 1 | 2 | 1 |
| **8.1.2.1318 (8.1 HF2)** | 1 | 2 | 1 |
| **8.1.0.1265 (8.1 PV)** | 1 | 2 | 1 |
| **8.1.0.1265 (8.1 PC2)** | 1 | 2 | 1 |
| **8.1.0.1265 (8.1 PC)** | 1 | 2 | 1 |
| **8.0.13.1502 (MR1 HF3)** | 1 | 2 | 1 |
| **8.0.10.1464 (MR1)** | 1 | 2 | 1 |
| **8.0.4.1441 (HF4)** | 1 | 2 | 1 |
| **8.1.0.1143 (Beta)** | 1 | 2 | 0 |
| **8.0.3.1427 (HF3)** | 1 | 2 | 1 |
| **8.0.2.1410 (HF2)** | 1 | 2 | 1 |
| **8.0.1.1399 (HF1)** | 1 | 2 | 1 |
| **8.0.0.1351 (PV Release)** | 1 | 2 | 1 |

| | | | |
|---|---|---|---|
| **8.1.0.1035 (8.1 Alpha)** | 1 | 0 | 0 |

# 3 Important Notes

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

- Basic Moff Power flows (PP1) – Supported
- Intel® Anti-Theft Technology – Supported
- BLU-RAY PLAYBACK - Supported
- Intel® Insider™ is not supported in this release
- DAL - Supported
- Intel® Identity Protection Technology - Supported

## 3.1 Hardware Configurations

This release supports the following HW configurations:

- CPU: **IVB** D0 (pre-QS), E0, L0, L1 (QS) / **SNB** D2
- PCH: **PPT** C0 (pre-QS), C1 (QS) / **CPT** B1, B3

## 3.2 Important Issues / Notes

- **Issue #197116** - LMSService is potentially vulnerable to unquoted service path vulnerability. This issue was fixed in 8.1.30 MR. Please see customer communication attached with release announcement and CDI / IBP#: 494925.

## 3.3 Software / Tools

- An error may occur when executing FPT –verify after flashing a system with FPT –f. If the flash memory in the GbE NVM region(s) has been modified, FPT will have recalculated the checksum and written the new value to the GbE NVM checksum location. If the checksum value in the original binary file were incorrect, running –verify will result in a data verification error message since the image on the SPI flash part is now different than the contents to the original binary.

- **Issue #195872:** SUT will hang at POST code 0x96 if network cable is not plugged in before running Platform Debug Analyzer (Intel® PDA) tool. For more details please review issue **195872** under section **8.2 Open – Intel® ME Kernel**

## 3.4 Intel® METS

**Intel® METS Intel® ME_PM_19 & Intel® ME_PM_20 Failure**

- If the platform design is set to enable "SUS Well Down Disabled" (System Stays in S4/S5 in normal S4/S5 entry path when system in DC mode) –
    - Customer design PBO to G3 – Intel® METS Intel® ME_PM_19 & Intel® ME_PM_20 is expected to Pass.
        - If System goes to G3 – pass
        - If System goes to S5 – See PCH Sighting Report #3881606
    - Customer design PBO to S5 – Intel® METS Intel® ME_PM_19 & Intel® ME_PM_20 is expected to Fail.
- If the platform design is set to enabled "SUS Well Down Enabled" (System moves to G3 in normal S4/S5 entry Path when system in DC mode) –
    - Customer design PBO to G3 – Intel® METS Intel® ME_PM_19 & Intel® ME_PM_20 is expected to Pass.
        - If System goes to G3 – pass
        - If System goes to S5 – See PCH Sighting Report #3881606
    - Customer design PBO to S5 – Intel® METS Intel® ME_PM_19 & Intel® ME_PM_20 is expected to Fail.

## 3.5 Best Known Configuration

For the latest Client Based Platform Best Known Configuration (BKC), please visit the Best Known Configuration page on Intel® PC Design Center https://teamspace.intel.com/sites/PCDC/BKC/Home.aspx.

## 3.6 Windows 8 Compatibility / Best Known Configuration

This release has been tested with a preliminary version of Windows* 8 (RTM) to ensure compatibility.

For the latest Client Based Platform Best Known Configuration (BKC) for Microsoft Windows 8* (Win8) document, please see document # 481125 on CDI/IBL.

# 4 Kit Details

## 4.1 Build Details

| Kit | Build Details | Changes since previous release (8.1.20.1336v2)? | Reasons for changes |
|---|---|---|---|
| **Firmware Version** | 8.1.30.1350 | Yes | FW and SW changes highlighted below. |
| **CRB BIOS Version** | IVB098.rom | No | N/A |
| **Intel® MEI Driver Version** | 8.1.10.1275<br>Certified for Windows* 7/8 | No | N/A |
| **SOL Driver Version** | 8.1.10.1275<br>Certified for Windows* 7/8 | No | N/A |

## 4.2 FITC XML Compare

| Changes between: | | | | |
|---|---|---|---|---|
| **MR 8.1.20.1336 newfiletmpl.xml** | | **Line** | | **MR 8.1.30.1350 newfiletmpl.xml** |
| 1 | <?xml version="1.0" encoding="utf-8"?> | = | 1 | <?xml version="1.0" encoding="utf-8"?> |
| 2 | <ftoolRoot version="47"> | = | 2 | <ftoolRoot version="47"> |
| 3<br>4<br>5<br>6<br>7<br>8 | | | | <No Change> |

**Note:**

- For information on the values that need to be entered for the setup procedure below, please refer to the **Intel® Series 7/C216 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 Panther Point EDS, **22.2.7.2 VSCC0—Vendor Specific Component Capabilities 0** describes the 32 bit VSCC register value.
- For access to the Intel® Panther 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.

# 5 Intel® ME New Features

## 5.1 RCR Update

| RCR # | Description / Background | Build |
|---|---|---|
| CCG0100010197 | **Description:**<br>Expand Intel® IPT to all Intel® Core™ and Xeon™ based platforms (including mobile and AIO).<br>**Background:**<br>Current implementation of Intel® IPT on Intel® ME 8.1 allows running Intel® IPT applets on Ultrabook™ or Intel® vPro™ or Intel® Core™ Desktop, but not on mobile or AIP (All-In-One Innovation Program) mobile systems. | 8.1.30.1350 |
| CCG100010162 | **Description:**<br>Intel® ME FW support for the UM77 PCH / i3-2365M and i3-2375M Core processors combination.<br>**Background:**<br>Amendment to CCG0100010084 RCR. | 8.1.3.1325 |
| CCG0100010084 | **Description:**<br>Intel® ME FW support for the UM77 PCH / Intel® Y Series 3rd Generation Core® Processors combination.<br>**Background:**<br>A new ULX processor for low TDP designs and has been added to the Intel® 3rd Generation Core® Processor product roadmap. | 8.1.2.1318 |
| CCG0100009956 | **Description:**<br>Add Microsoft* Windows 8 uEFI native boot mode support for Intel® ME MEInfowin and MEManufwin manufacturing tools.<br>**Background:**<br>Intel® ME 8 Tools PRD did not specifically include Windows 8 uEFI native boot mode support for MEInfowin and MEManuf. This is needed for Microsoft's Logo requirement with Windows 8 Secure Boot. | 8.1.0.1248 |

| RCR # | Description / Background | Build |
|---|---|---|
| CCG0100190265 | **Description:**<br>Change IFR service to automatically start during IFR flow.<br>**Background:**<br>Improves the user experience of IFR by reducing the delay while an IFR is in progress. | 8.1.0.1248 |
| CCG0100009844 | **Description:**<br>Intel is changing the implementation of Code 10 violation of the Ethernet controller after G3->S5->WoL bug fix.<br>• ME FW automatically detects impacted platforms<br>• On impacted platforms, FW adds a 50ms delay in FW<br>• Impacted platforms include those that:<br>  ○ Do not support ME operation in M3 (APWROK and PCH_PWROK are tied together)<br>  ○ Using Intel LAN<br>• LAN MAC Delay Timer (ME soft strap 10 bit 26) configuration option has been removed from FITC<br>**Background:**<br>This implementation change was made in Intel® ME FW 8.0.10.1464 MR and carries over to 8.1.0.1248. Intel had observed a Code 10 violation of the Ethernet controller on ME 8.0 platforms during the G3-S5 state followed by WOL. Symptom is no LAN connectivity during WOL (inoperable LAN connection) operation. | 8.1.0.1248 |
| CCG0100009815 | **Description:**<br>Add CPU model Intel® Core™i3-2377M processor to Intel® microarchitecture code name Sandy Bridge Ultrabook™ CPU list to allow Intel® IPT availability with this model.<br>**Background:**<br>CPU model did not have Intel® IPT support; a requirement for Ultrabook™. | 8.1.0.1248 |
| CCG0100009823 | **Description:**<br>MEManuf EOL support for systems with Intel® Integrated LAN disabled.<br>**Background:**<br>Add a check to MEManuf –EOL in cases where Intel® Integrated LAN Enable is set to False in FITC. | 8.1.0.1248 |

| RCR # | Description / Background | Build |
|---|---|---|
| CCG0100009760 | **Description:**<br>Updates the FPT tool to retain MAC/SSID/SVID when flashing image.<br>**Background:**<br>FPT failure to recognize the correct MAC/SSID/SVID and overwriting them. | 8.1.0.1143 |
| CCG0100009719 | **Description:**<br>Implement Recovery Mode check in MEManuf.<br>**Background:**<br>MEManuf passed while system is in recovery mode and ME not fully functioning. | 8.1.0.1143 |
| 1024025 | **Description:**<br>Add current version of Microsoft Visual Studio VC++ redistributables to ME_SW Installer.<br>**Background:**<br>Installer does not complete the installation of all ME SW components when trying to install newer version of Microsoft Visual Studio VC++ redistributables than exists on system. | 8.1.0.1143 |
| CCG0100125704 | **Description:**<br>FW BIST Integrated in the ME early boot<br>**Background:**<br>In the manufacturing line, the BIST result is not available until software tool requests FW to run the BIST. In order to perform BIST, OEM has to (a) boot to OS (b) run MEMANUF test (c) incur power cycle reset (d) boot to OS after Power cycle reset (e) run MEMANUF again to retrieve results.<br>If ME were to automate the BIST process itself then in the aforementioned sequence, steps a) and b) can be avoided saving many seconds in the flow. | 8.1.0.1035 |
| CCG0100009277 | **Description:**<br>ME FW mechanism to check MFS status<br>**Background:**<br>Improve robustness of MFS and ME stability so that ME doesn't get into a bad state and if it does, identify cause for customers. | 8.1.0.1035 |

| RCR # | Description / Background | Build |
|---|---|---|
| CCG0100115620 | **Description:**<br>OEM option to OPT-OUT from IFR Updates<br>**Background:**<br>Having hard OPT OUT option from IFR will allow customers to validate and expedite critical FW updates instead of utilizing Intel's Firmware Recovery. | 8.1.0.1035 |
| CCG0100134301 | **Description:**<br>Request for an Anti-Theft option to prevent PBA Logon Timer restart on warm reset<br>**Background:**<br>Client systems using Self Encrypted Drives (SEDs) shutdown unless a command is sent to stop PBALogon timer after the disk is unlocked and the data partition is revealed. | 8.1.0.1035 |
| CCG0100128347 | **Description:**<br>FITC VSCC cleanup.<br>**Background:**<br>VSCC cleanup – Removal of parts no longer used in current generation platforms (i.e. AT26DF321), and simplifying the VSCC register value to one universal value for all SPI parts (0x20052005). | 8.1.0.1035 |
| CCG0100129713 | **Description:**<br>Support diagnostic PET over PLDM<br>**Background:**<br>Ability for ME to translate platform monitoring events sent from EC/SIO to WSMan Events and send them to the management station. | 8.1.0.1035 |
| CCG0100103738 | **Description:**<br>Support for SIGMA spec 0.88<br>**Background:**<br>Adds SIGMA support for multiple clients e.g. CLS, JOM, PAVP and others. | 8.1.0.1035 |
| CCG0100009226 | **Description:**<br>Certification for Platform Embedded Asymmetric Token (PEAT)<br>**Background:**<br>The purpose of Platform Embedded Asymmetric Token is to enable embedded asymmetric key (private key) based tokens within the secure processing element of Intel platforms. | 8.1.0.1035 |

| RCR # | Description / Background | Build |
|---|---|---|
| CCG0100009168 | **Description:**<br>ME 8.0 support for XP on workstation and client platforms<br>**Background:**<br>Adds full feature support for Windows* XP SP3 workstation and client platforms with exception of USB3 and wireless display features. | 8.1.0.1035 |
| CCG0100008852 | **Description:**<br>FOV support to configure ODM ID and System integrator ID NVARs during manufacturing (post image flash) and addition to MEInfo to present these NVARs.<br>**Background:**<br>In order to address OEM request (HP) to be able to configure ODM ID (used by Intel Services) in manufacturing and verify by MEInfo | 8.1.0.1035 |

# 6 Issue Status Definitions

This document provides sightings and bugs report for Intel® Management Engine Firmware 8.0 SKU, Software and Tools for Intel® AMT on the Intel® 7 Series/C216 Chipset Family and Cougar Point Family / PCH platforms. Each report contains a snapshot of sightings and critical internal bugs dating to the Friday of the week in which it was released. At the time of a milestone release, this report will be distributed with the Intel® ME Kit and will provide information on new issues and the status of old issues (replacing the Release Notes document).

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

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

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

**Open Issues**: New sightings and bugs will be classified as "Open" issues until the fix is verified with the appropriate firmware version. Open issues are separated into 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 Intel® 7 Series/C216 Chipset Family CRB SKU's unless otherwise noted either in this document or in the sightings tracking systems.**

# 7 Closed Issues

## 7.1 Closed - Intel® ME Kernel

| Issue # | Description | Affected Component/Impact / Workaround/Notes | Fixed in Kit# |
|---|---|---|---|
| 197134 / 3708793 | Integrated graphic adapter VGA/HDMI/DVI cannot display and system may not boot under temperature sensitive conditions. | **Affected Component** – FW.Bringup<br>**Impact:** No display from integrated graphics adapter and system may not boot.<br>**Notes:** Affects Intel® 6 Series and Intel® C200 Series Chipset and Intel® 7 Series and Intel® C206 Series Chipset platforms using Intel® ME8 FW. | 8.1.30.1350 |
| 196979 | Rare ME File System Corruption Issue. | **Affected Component:** FW.Kernel.StorageMgr<br>**Impact:** Under rare corner case conditions involving power loss during manufacturing or ME un-configuration (via BIOS or CMOS clear), ME file system may be corrupted.<br>**Workaround:** Re-flash<br>**Notes:**<br>• 5 MB firmware in both flows – configured and un-configured.<br>• 1.5 MB firmware in Intel® ME un-configuration flow only | 8.1.20.1336 |
| 197044/ 197046 | Integrated VGA does not display after AC-Power/CLR CMOS jumper operations. | **Affected Component** – FW.Bringup<br>**Impact:** No display from integrated graphics adapter.<br>**Workaround:** Reflash firmware.<br>**Notes:**<br>Reproduction Steps:<br>1. Disconnect AC power (G3).<br>2. Short CLR_CMOS jumper.<br>3. Re-connect AC power (leave CLR_CMOS shorted).<br>4. Remove CLR CMOS jumper<br>5. Press PWR button.<br>6. Do G3 again then PWR on SUT.<br>7. PWR on. SUT halts at 0xD6 without VGA output. | 8.1.2.1318 |

| Issue # | Description | Affected Component/Impact / Workaround/Notes | Fixed in Kit# |
|---|---|---|---|
| 196990 | Under rare corner case conditions involving power loss during manufacturing or Intel® ME un-configuration (via BIOS or CMOS clear), ME file system may become corrupted. | **Affected Component** – FW.Kernel.StorageMgr<br>**Impact:** Intel® ME halts and is unresponsive.<br>**Notes:** Recovery via re-flashing firmware.<br>This affects:<br>• 5 MB firmware in both flows – configured and un-configured.<br>• 1.5 MB firmware in Intel® ME un-configuration flow only<br>• The defect exists in all ME 8.x releases prior to 8.1.2.<br>  • OEM customers are reminded to ensure that no unplanned power loss occurs during manufacturing or during Intel® ME un-configuration. | 8.1.2.1318 |
| 196833 | Sporadically after system moves to S3, it moves to 'S0-lite' and becomes stuck instead to moving to a S4 state. | **Affected Component:** FW.Kernel.FFS<br>**Impact:** System hangs in S0-lite state fails to move to S4.<br>**Workaround:** None.<br>**Notes:**<br>Reproduction Steps:<br>1. Configure system to FFS.<br>2. Power system up to S0/H0 state and add a valid Intel® ME profile.<br>3. Move system to S3.<br>4. Observe system becomes stuck in 'S0-lite' state instead of moving to S4. | 8.1.0.1248 |

| Issue # | Description | Affected Component/Impact / Workaround/Notes | Fixed in Kit# |
|---|---|---|---|
| 196595 | During a partial FW Update in Windows and starting S3 stress testing, system displays "System unexpectedly restarts during standby/resume" error after the first S0->S3->S0 resume. | **Affected Component** – FW.Kernel.FWUpdate<br>**Impact:** During a partial FW Update process, ICV may not get updated properly triggering Intel® ME to reset.<br>**Workaround:** N/A<br>**Notes:**<br>Reproduction Steps:<br>1. Flash a FW image with a WCOD partition mismatching the WLAN NIC in the system.<br>2. Provision Intel® AMT and set idle timeout to 1.<br>3. Boot to Windows and perform a Partial FW Update.<br>4. Put system in S0->S3->S0 cycling.<br>5. Disconnect wired LAN to ensure system moves from Moff -> M3 after 1 minute.<br>6. Connect wired LAN to wake the Intel® ME.<br>Global reset occurs. | 8.1.0.1248 |
| 196397 | Intel® ME is not accessible after soft reboot cycles in Windows* 7. | **Affected Component** – FW.Kernel<br>**Impact:** Loss of Intel® ME until system is rebooted.<br>**Workaround:** N/A<br>**Notes:**<br>Issue typically seen after 3000 cycles. Issue does not occur when booting from DOS.<br>**Reproduction Steps:**<br>1. Install Windows* 7 64-bit.<br>Perform continuous warm reboot cycling until Intel® ME is not accessible (may exceed 3000 cycles). | 8.1.0.1248 |
| 196555 | FW returns error code 5 when RW configuration is sent after multiple iterations of S0->S4->S0 stress testing. | **Affected Component:** FW.mDNSProxy<br>**Impact:** Customers may not be able to activate UDP – Remote Wake.<br>**Workaround:** none.<br>**Notes:**<br>Reproduction Steps:<br>1. Send RW configuration.<br>2. Move SUT from S0 to S4.<br>3. Verify the UDP packets were sent.<br>4. Wake SUT with Magic Packet. | 8.1.0.1248 |

***Closed Issues***

| Issue # | Description | Affected Component/Impact / Workaround/Notes | Fixed in Kit# |
|---|---|---|---|
| 196442 | Intel® ME is stuck in an initialization phase during power cycling after Memory Protection Range (MPR) violations. | **Affected Component:** FW.Kernel<br>**Impact:** Loss of Intel® ME functionality and MEInfo –fwsts will display an ME debug error.<br>**Workaround:** Recovery via G3<br>**Notes:** Occurs sporadically during power cycle stress testing. | 8.1.0.1143 |
| 196471 | System hangs in host OS after S3 resume. | **Affected Component:** FW.Kernel.PowerManagement<br>**Impact:** The system could hang when Intel® ME is initializing after a MPR violation or multiple Intel® ME exceptions.<br>**Workaround:** Recovery via G3<br>**Notes:** | 8.1.0.1143 |
| 196459 | Intel® ME enters recovery mode when running warm reset cycles. | **Affected Component:** FW.Kernel<br>**Impact:** Sporadic loss of Intel® ME functionality during warm reset cycling.<br>**Workaround:** Recovery via G3<br>**Notes:** | 8.1.0.1143 |
| 196387 | SkuMgr sets the Platform type for River City Workstation as Desktop. | **Affected Component:** FW.Kernel.Sku Mgr<br>**Impact:** Incorrect image configuration.<br>**Workaround:** Recovery via G3<br>**Notes:**<br>Reproduction Steps:<br>1. Boot River City workstation CRB with Intel® ME 8.1 firmware.<br>2. Check SkuMgr platform rule. | 8.1.0.1143 |
| 195545 | MFS Corruption Not Sent to BIOS on M3 Flows | **Affected Component** – FW.Kernel.StorageMgr<br>**Impact:** MFS corruption data is not being sent correctly to BIOS during M3 flows when the MFS corruption doesn't include ME resets.<br>**Workaround:** none<br>**Notes:** | 8.1.0.1143 |
| 195201 | Platform halts when performing full FW update after clearing CMOS while FW was in recovery state. | **Affected Component** – FW.Kernel<br>**Impact:** SUT halts after performing full FW update if CMOS was cleared while FW was in recovery state.<br>**Workaround:** none<br>**Notes:** | 8.1.0.1143 |
| 195164 | ME enters FW Recovery mode when HDA_SDO (hot key sequence) is performed when AT is Enrolled | **Affected Component** – FW.MCTP<br>**Impact:** SUT goes into FW Recovery mode when enrolling AT.<br>**Workaround:** none<br>**Notes:** None. | 8.1.0.1143 |

| Issue # | Description | Affected Component/Impact / Workaround/Notes | Fixed in Kit# |
|---|---|---|---|
| N/A | Deep S3 disabled platforms attempt to enter Deep SX instead of S3 (FW incorrectly interprets RCBA value) | **Affected Component** – FW.Kernel<br>**Impact:** SUT goes into S5 instead of S3.<br>**Workaround:** none<br>**Notes:** | 8.1.0.1143 |
| 196069 | Due to lack of validity check in Intel® ME against parameters passed in by the host, malformed FW update messages sent to ME through Intel® MEI may result in ungraceful FW reset. | **Affected Component:** FW.Kernel.FWUpdate<br>**Impact:** Malware that has administrator privilege can send malformed FW update Intel® MEI messages to ME and triggers ungraceful ME reset. Three consecutive ME reset within 60 seconds result in ME halt.<br>CVSS: 4.7<br>(AV:L/AC:L/Au:N/C:N/I:N/A:C/E:F/RL:ND/RC:ND)<br>**Workaround:** N/A<br>**Note:** Exploitable by local malware that has administrator privilege. Not exploitable over network. | 8.1.0.1143 |
| 193490 | SMS GpsLocationBeaconingNotification fails to detect beacon messages from FW after resume from ME RESET with trigger mask 0xF. | **Affected Component** – FW.MCTP<br>**Impact:** FW unable to send beaconing message after ME Reset.<br>**Workaround:** Warm reset.<br>**Notes:** | 8.0.0.1221 eng drop |

## 7.2 Closed – Integrated Clock Control (ICC)

| Issue # | Description | Affected Component/Impact / Workaround/Notes | Fixed in Kit# |
|---|---|---|---|
| | | **Affected Component:**<br>**Impact:**<br>**Workaround:**<br>**Notes:**<br>Reproduction Steps: | |

## 7.3 Closed – Software / Tools

| Issue # | Description | Affected Component/Impact / Workaround/Notes | Fixed in Kit# |
|---|---|---|---|
| 197110 | MEManuf displays "Error 9271: Flash ID 0xC22017 Intel(R) ME VSCC value mismatch." | **Affected Component** – SW.Tools.MeManuf<br>**Impact:** MEManu failure.<br>**Workaround:** Use MEManuf in 8.1.3.1325.<br>**Notes:** Affects customer BIOS not following the PREOP/OPMENU configuration used in the Intel CRB BIOS and MEManuf in 8.1.20.1318 MR kit.<br>MEManuf in this release will use HW Sequencing to fix above scenario.<br>Reproduction Steps:<br>1. Create SPI image with the following BIOS modifications.<br>a. OPMENU (SPIBAR + 98h) to 05 01 03 02 D8 20 9F FF.<br>b. PREOP (SPIBAR + 96h) to 0x0FE4<br>c. Set HSFS.FLOCKDN (SPIBAR + 04h bit14) to 1<br>2. Run MEManuf 0s0 –verbose<br>3. Error 9271: Flash ID 0xC22017 Intel(R) ME VSCC value mismatch." | 8.1.30.1350 |

| Issue # | Description | Affected Component/Impact / Workaround/Notes | Fixed in Kit# |
|---|---|---|---|
| 197086 | FWUpdLcl tool fails when performing a full firmware update on non-English Microsoft* Windows 8 with Taylor Peak WLAN card. | **Affected Component** – SW.Tools.FwUpdLcl<br>**Impact:** Tool does not perform firmware update on non-English Microsoft* Windows 8 system and exits.<br>**Workaround:** Set language to English in IMSS before running tool. Note that after the failure has occurred, the system should be restarted before changing the language to English. The language can be set back to the prior setting after the firmware update process is completed.<br>**Notes:**<br>Reproduction Steps:<br>1. Install Taylor Peak WLAN card.<br>2. Install non-English version of Microsoft* Windows 8 RTM 64-bit (Pro or Standard edition).<br>3. Install PCH and ME drivers (w/ IMSS).<br>4. Ensure that IMSS language is set to Japanese or Windows OS [Japanese].<br>5. Run FWUpdLcl tool.<br>Tool exits without updating firmware. | 8.1.20.1336 |
| 196604 | 'MEinfowin32/64.exe –EOL' and 'MEinfowin32/64.exe' stop running on Win8x64 UEFI native boot OS environment. | **Affected Component** – SW.Tools.MeManuf<br>**Impact:** MEInfo and MEManuf –EOL doesn't work on EFI native boot OS environment.<br>**Workaround:** Tools functional in UEFI native mode<br>**Notes:** This issue was fixed in the 8.1.0.1265 PC release but was not documented as having been closed. See RCR CCG0100009956 above for more details. | 8.1.0.1248 |
| 196896 | MEInfoWin and MEManufWin error: "Entry Point Not Found The procedure entry point GetSystemFirmwareTable could not be located in the dynamic link library KERNEL32.dll". | **Affected Component:** SW.Tools.MEInfo<br>**Impact:** API is missing in KERNEL32.dll on Microsoft* Windows XP 32-bit systems causing Windows version of MEInfo to crash.<br>**Workaround:** None.<br>**Notes:** Error does not occur with 64-bit version of Windows XP. | 8.1.0.1248 |

| Issue # | Description | Affected Component/Impact / Workaround/Notes | Fixed in Kit# |
|---|---|---|---|
| 196851 | MEManuf tool has been updated to provide a check for firmware incorrectly reporting EPID Group IDs | **Affected Component:** SW.Tools.MEManuf<br>**Impact:** Enables check for firmware incorrectly reporting EPID Group IDs.<br>**Workaround:** None.<br>**Notes:** Refer to the Customer Communication provided separately with this release. | 8.1.0.1248 |
| 196117 | Intel® ME FW Recovery Agent reports IFR update failed after the update was interrupted but still finished successfully | **Affected Component:** SW.IFR.TCAgent<br>**Impact:** IFR update incorrectly reports "Failed" when an interrupted IFR Update process successfully rolls back the update.<br>**Workaround:** None.<br>**Notes:**<br>Reproduction Steps:<br>1. Enable IFR Update in the Intel® ME.<br>2. Install Intel® FW Recovery Agent.<br>3. Check for and start an IFR update.<br>4. Interrupt IFR update (e.g. power loss in FW update step).<br>5. Continue the update or perform second power loss to initiate rollback operation.<br>6. Open the Intel® ME FW Recovery Agent window.<br>7. View the Intel® FW Recovery Agent log. Failed is reported instead of update successful or update failed and rollback completed successfully. | 8.1.0.1248 |
| 196670 | IFR update fails with "Error 8787: Verify that Intel® ME Service is installed and running" due to a delay during startup of IntelMEFWService. | **Affected Component:** SW.IFR.Windowservice<br>**Impact:** IFR update failure.<br>**Workaround:** Manually start IntelMEFWService after every phase of IFR reboots.<br>**Notes:** Fixed in 8.0.10.1464v2<br>Reproduction Steps:<br>1. Flash SPI image with IFR Enabled.<br>2. Boot to host OS.<br>3. Start IntelMeFwService.exe<br>4. Reboot system.<br>**5.** Run the following command: "*IntelMeFwService.exe –query*". | 8.1.0.1248 |

| Issue # | Description | Affected Component/Impact / Workaround/Notes | Fixed in Kit# |
|---|---|---|---|
| 196540 | "Intel® ME Service" is shown to be "unknown" in System configuration. | **Affected Component:** SW.IFR.Windowservice<br>**Impact:** After installing the driver, the "ME Service" in the Windows* System Configuration utility is displayed as "unknown" in the "Manufacturer" field.<br>**Workaround:** None.<br>**Notes:** Fixed in 8.0.10.1464v2<br>Reproduction Steps: | 8.1.0.1248 |
| 196502 | SKU manager in all FPTW tool commands fail on HM67, QS67 and UM67 SKUs. | **Affected Component:** SW.Tools.FlashProgrammingTool<br>**Impact:** Support for QS67, HM67, and UM67 had been incorrectly removed.<br>**Workaround:** N/A<br>**Notes:** | 8.1.0.1248 |
| 196495 | MAC address becomes corrupt after updating SPI using FPT –savemac command. | **Affected Component:** SW.Tools.FlashProgrammingTool<br>**Impact:** Invalid MAC address (all 00) after update SPI by using FPT –savemac command.<br>**Workaround:** N/A<br>**Notes:** Fixed in 8.0.10.1464v2<br>Reproduction Steps:<br>1. Set MAC address to 001122334455.<br>2. Perform Global Reset.<br>3. Flash SPI image with -savemac parameter.<br>4. Perform Global Reset.<br>5. Check current MAC address setting (may display as 0x00000000). | 8.1.0.1248 |
| 196454 | System cannot execute FwUpdLcl.efi under EFI shell in x64 environment. | **Affected Component:** SW.Tools.FwUpdLcl<br>**Impact:** FwUpdLcl.efi tool execution failure.<br>**Workaround:** N/A<br>**Notes:** Fixed in 8.0.10.1464v2<br>Reproduction Steps:<br>**1.** Boot to EFI shell.<br>**2.** Execute Fwupdlcl.efi -f ME.bin<br>**3.** FwUpdLcl.efi returns "Failed: file "\..\Common\Port\Efi64\Efiwrap.c, line93". | 8.1.0.1248 |

| Issue # | Description | Affected Component/Impact / Workaround/Notes | Fixed in Kit# |
|---|---|---|---|
| 196415 | FPT from Intel® ME 8.0.3.1427 release fails to complete SPI flash operation if the image does not contain a GbE region. | **Affected Component:** Installer<br>**Impact:** FPT cannot update full SPI flash image when SPI image does not contain a GbE region.<br>**Workaround:** N/A<br>**Notes:** Fixed in 8.0.10.1464v2<br>Issue occurs with all OS versions of FPT in HF3.<br>Reproduction Steps:<br>1. Flash SPI image which does not contain a GbE region using FPT from earlier kit.<br>2. Perform a global reset.<br>3. Flash a new SPI image with FPT from Intel® ME8 HF3.<br>4. FPT will display "GbE Region does not exist.". Windows version of FPT will display an Intel® Flash Programming Tool error message that FPT has stopped working and a prompt to Check online or Close the program. | 8.1.0.1248 |
| 196056 | FWUpdLcl does not display warning message "*Warning: Do not exit the process or power off the machine before the firmware update process ends*". | **Affected Component** – SW.Tools.FWUpdLcl<br>**Impact:** When performing FW update, FW update tool does not display warning message "*Warning: Do not exit the process or power off the machine before the firmware update process ends*"<br>**Workaround:** N/A<br>**Notes:** | 8.1.0.1248 |

| Issue # | Description | Affected Component/Impact / Workaround/Notes | Fixed in Kit# |
|---|---|---|---|
| 196415 | FPT fails to complete SPI flash operation if the image does not contain a GbE region. | **Affected Component:** Installer<br>**Impact:** FPT cannot update full SPI flash image when SPI image does not contain a GbE region.<br>**Workaround:** Use FPT from Intel® ME 8.0.2.1410 HF2 as a temporary solution. **Note:** Intel's normal guidance is to use the version from the kit release.<br>**Notes:** Issue occurs with all OS versions of FPT in HF3 and has been fixed in a future release.<br>Reproduction Steps:<br>1. Flash SPI image which does not contain a GbE region using FPT from earlier kit.<br>2. Perform a global reset.<br>3. Flash a new SPI image with FPT from Intel® ME8 HF3.<br>4. FPT will display "GbE Region does not exist.". Windows versions of FPT will display an Intel® Flash Programming Tool error message that FPT has stopped working and a prompt to Check online or Close the program. | 8.1.0.1248 |
| 196394 | FITC build error with Flash Part: PM25LQ032C is added to VSCC table | **Affected Component** – SW.Tools.FlashProgrammingTool<br>**Impact:** The image cannot build successfully.<br>**Workaround:** None.<br>**Notes:** | 8.1.0.1248 |
| 196048 | Management Engine Interface (Intel® MEI) driver installation fails. | **Affected Component** – Installer<br>**Impact:** Unsuccessful Intel® MEI driver installation installation<br>**Workaround:** Install using –novc switch.<br>**Notes:** When re-installing Intel® MEI driver using swsetup.exe from Intel® MEFW 8.0.0.1351 kit, installation process gets to vcredist_x86.exe when an error message appears "The program failed to start...will exit". | 8.1.0.1248 |
| 195788 | FW Update tool does not decode UPDATE_IMAGE_BLACKLISTED status returned from the FW | **Affected Component** – SW.Tools.FwUpdLcl<br>**Impact:** Tool displays error message when attempting to downgrade firmware instead of expected message that downgrade to blacklisted FW is not supported.<br>**Notes:** | 8.1.0.1248 |

***Closed Issues***

| Issue # | Description | Affected Component/Impact / Workaround/Notes | Fixed in Kit# |
|---|---|---|---|
| 195596 | UNS creates excessive number of empty folders in registry on Windows XP systems. | **Affected Component** – SW.AMT.Services<br>**Impact:** Unnecessary empty folders are created in Windows XP registry for each USB insert or WS-MAN operation**.**<br>**Notes:**<br>Reproduction Steps | 8.1.0.1143 |
| 195532 | IMSS in Windows 8 presents the LAN and WLAN drivers as disabled. | **Affected Component** – SW.AMT.Icon<br>**Impact:** LAN and WLAN driver information is not displayed in IMSS Extended System Details.<br>**Notes:**<br>Reproduction Steps | 8.1.0.1143 |
| 195020 | START and EXIT buttons are not shown in IFR GUI when using low resolution screen (800x600/1024x768) | **Affected Component** – SW.IFR.FWupdate<br>**Impact:** When using resolutions lower than 1280x960 , "START" and "EXIT" buttons will not be shown in IFR GUI<br>**Workaround:** Change screen resolution to a higher value.<br>**Notes:** Fixed in future merge.<br>Reproduction Steps: | 8.1.0.1143 |
| 194995 | UNS service hangs after performing partial FWUpdate and immediately exiting IMSS. | **Affected Component** – SW.AMT.Services<br>**Impact:** UNS process hangs; IMSS will not open after performing Partial FW Update and immediately exiting IMSS.<br>**Notes:** Fixed in future merge.<br>Reproduction Steps: | 8.1.0.1143 |
| 193241 / 195818 | If the computer name contains non-Latin symbols (e.g. Cyrillic), then all UNS's local WS-MAN calls fail.<br><br>WebUI and VisualCIM over local are working. | **Affected Component** – SW.AMT.Services<br>**Impact:** Privacy issue. User will not be able to cancel redirection sessions.<br>**Workaround:** N/A<br>**Notes:**<br>Reproduction Steps: N/A | 8.1.0.1143 |

| Issue # | Description | Affected Component/Impact / Workaround/Notes | Fixed in Kit# |
|---|---|---|---|
| 193805 | KVM session closes with Protocol Violation during reset from Windows to DOS. | **Affected Component** – SW.AMT.SDK.KVM.RealVNC<br>**Impact:** Intel KVM Viewer disconnects session due to error.<br>**Workaround:** Does not occur with KVMTray or UltraVNC.<br>**Notes:**<br>Reproduction Steps:<br>1. Boot system to Windows.<br>2. Open KVM session.<br>3. Reset remote system through RCO or local reset to moved system to ODS mode (need to run chkdsk or create BSOD).<br>4. KVM session should remain connected however closes session with "Connection to remote machine stopped. Reason: Error: 0x80862602: KVM protocol violation" | 8.1.0.1143 |
| 193820 / 193950 | IMSS hung when pressing extended system details immediately after loading the application on Windows 8. | **Affected Component** – SW.AMT.Icon<br>**Impact:** IMSS application is unresponsive.<br>**Workaround:** Recovery by killing process.<br>**Notes:** Only seen on Windows 8 32-bit.<br>**Reproduction Steps:**<br>1. Burn image.<br>2. Do not provision Windows 8 system.<br>3. Start IMSS (If already started, open icon and select Exit and restart IMSS again).<br>4. Go to the advanced tab in IMSS. Press Extended System Details.<br>5. Application hangs. | 8.1.0.1143 |
| 194631 / 194715 | EFI and Windows 64-bit versions of FPT fail to consume values for MEIdleTimeout FOV | **Affected Component** – SW.Tools.FlashProgrammingTool<br>**Impact:**<br>**Workaround:** Reopen application reset the strings changes and the strings return to the localized language.<br>**Notes:** | 8.0.0.1240 eng drop |

| Issue # | Description | Affected Component/Impact / Workaround/Notes | Fixed in Kit# |
|---|---|---|---|
| 193704 | IFR Update Agent will not install on Windows XP 32-bit or Windows XP 64-bit system | **Affected Component** – Installer<br>**Impact:** Unable to install IFR Update Agent on Windows XP 32 and 64 bit systems.<br>**Workaround:** N/A<br>**Notes:** | 8.0.0.1240 eng drop |
| 193488 | After flashing image, FWUPDLCL returns "Error 8769: Polling for FW Update Failed." And "Error 8707: Firmware update failed due to an internal error." | **Affected Component** – SW.Tools.FwUpdLcl<br>**Impact:** Intermittent failures to upgrade FW images using FWUpdLcl.<br>**Workaround:** N/A<br>**Notes:** | 8.0.0.1240 eng drop |

## 7.4 Closed – Intel® Upgrade Service

| Issue # | Description | Affected Component/Impact / Workaround/Notes | Fixed in Kit# |
|---|---|---|---|
| | | **Affected Component** –<br>**Impact:**<br>**Workaround:**<br>**Notes:**<br>Reproduction Steps: | |

## 7.5 Closed – Not Firmware Issue

| Issue # | Description | Affected Component/Impact / Workaround/Notes |
|---|---|---|
| 196554 | HECI failures with Microsoft* Windows 8 Build 8250. | **Affected Component** –SW.HECI Driver<br>**Impact:** Unable to use tools dependent on HECI such as MEINFO with Windows 8 Build 8250.<br>**Workaround:** N/A<br>**Notes:** Expected behavior in Microsoft* Windows. Error does not occur when installation while logged in as "Administrator" user account or by invoking "Run as Administrator" when launching MEInfo utility.<br>Reproduction Steps:<br>1. Run MEInfo<br>2. Instead of displaying information requested, the following error occurs: MeInfowin Error: 9470: 'Fail to load driver <PCI access for windows>'. |
| 194427 | Alarm Clock fails to wake the system from S3. | **Affected Component** – FW.Kernel.AlarmClock<br>**Impact:** System may not wake from S3 by Alarm Clock.<br>**Workaround:** none<br>**Notes:**<br>Reproduction Steps:<br>1. Flash image on system under test.<br>2. Provision SUT.<br>3. Add Alarm for >4 minutes.<br>4. Move SUT to S3.<br>5. Wait approximately 6 minutes.<br>6. SUT should wake to S0 but remains in S3 6 of 10 tests. |

***Closed Issues***

| Issue # | Description | Affected Component/Impact / Workaround/Notes |
|---|---|---|
| 191570 | FPTW.exe -ERASE fails at 69% if system has been previously resumed from S3. | **Affected Component** – ClientBIOS<br>**Impact:**<br>**Workaround:** DOS version (FPT.exe) is not affected and can be used.<br>**Notes:**<br>Reproduction Steps:<br>1. Boot system to Windows<br>2. Place system in S3<br>3. Resume system from S3<br>4. Run FPTW.exe –ERASE from a Windows command line<br>Command should successfully complete however, will fail with following message<br>-Erasing Flash Block [0x580000] - 69% complete.<br>Error 8: Software sequencing failed. Make sure that you have access to target flash area! |
| 194722 | Machine restart and stuck in 009A code when try to wake ME after the first time entered to Moff with current NIC | **Affected Component** – ClientBIOS<br>**Impact:** When trying to wake ME from Moff after the first time, SUT reset and stuck in post code 009A<br>**Workaround:** Recovery by G3<br>**Notes:**<br>Reproduction Steps:<br>1. Boot SUT with different network adapter.<br>2. Add a valid profile to ME store<br>3. Move SUT to Sx and ensure WiAMT connectivity.<br>4. Wait for ME to enter Moff state (idle timeout =1).<br>5. When ME is in Moff, wake ME vy ARP, NDP, ping etc.<br>6. ME should move to M3 in Sx state but instead SUT resets and hangs at 009A code. |
| 194680 | "AMT on Wireless" is not available in Level 3 Upgrade. | **Affected Component** – ClientBIOS<br>**Impact:** After making Level 3 Upgrade on B75 machine and provisioning, the Wireless submenu is missing from WebUI. The user cannot create a new wireless profile.<br>**Workaround:** none<br>**Notes:** |

| Issue # | Description | Affected Component/Impact / Workaround/Notes |
|---|---|---|
| 194001 | FWUPDLCL failed to update using restore point bin file after flashing previous_oem_image | **Affected Component** – FW.Kernel.FwUpdLcl<br>**Impact:** MEFW Updates using restore points fail.<br>**Workaround:** N/A<br>**Notes:**<br>Reproduction Steps:<br>1. Flash image.<br>2. Execute fwupdlcl.exe -save store.bin<br>3. Flash previous kit image.<br>4. Execute fwupdlcl.exe –f store.bin –forcereset<br>5. System displays Error 8741: FW Update Failed and Error 8707: Firmware update failed due to an internal error. |

## 7.6 Closed - No Plans to Fix

| Issue # | Description | Affected Component/Impact / Workaround/Notes | Fixed in Kit# |
|---|---|---|---|
| 193574 | During Intel Firmware Recovery (IFR) at **Stage 2 of 2**, if system is allowed to go to S3/S4, upon system resume, the Firmware Update (FWU) tool displays error "A general FW issue has occurred. Please try reinstalling the Intel ME FW Tool". | **Affected Component** – SW.Tools.FwUpdLcl<br>**Impact:** IFR firmware update is unsuccessful if system is allowed to go to S3/S4 state during update.<br>**Workaround:** N/A<br>**Notes:**<br>Reproduction Steps:<br>1. Run MEFWR.exe and then when process gets to **Stage 2 of 2**, put the system to S3 or S4.<br>2. Resume system<br>3. An error will be displayed "A general FW issue has occurred. Please try reinstalling the Intel ME FW Tool". | Not a current requirement |

| Issue # | Description | Affected Component/Impact / Workaround/Notes | Fixed in Kit# |
|---|---|---|---|
| 193573 | During Intel Firmware Recovery (IFR) at **Stage 1 of 2**, if system is allowed to go to S3/S4, upon system resume, the Firmware Update (FWU) tool displays error "A general FW issue has occurred. Please try reinstalling the Intel ME FW Tool". | **ffected Component** – SW.Tools.FwUpdLcl<br>**Impact:** IFR firmware update is unsuccessful if system is allowed to go to S3/S4 state during update.<br>**Workaround:** N/A<br>**Notes:**<br>Reproduction Steps:<br>1. Run MEFWR.exe and then when process gets to **Stage 1 of 2**, put the system to S3 or S4.<br>2. Resume system<br>3. An error will be displayed "A general FW issue has occurred. Please try reinstalling the Intel ME FW Tool". | Not a current requirement |
| 191185 | When running client application (e.g. MEInfo) over MEI and then aborting it after connection has been established, the MEI driver resets. | **Affected Component** – SW.HECI Driver<br>**Impact:** May affect operation of other software including customer's which makes calls to MEI driver and suddenly stop the application.<br>**Workaround:** N/A<br>**Notes:**<br>Reproduction Steps: N/A | N/A |
| 193914 | ME Debug viewer displays [EVT_GRP_CHECKPOINT] & [EVT_GRP_PWRMGMT] error messages while running Intel® ME Test Suite, ME_PM_20.1, 20.4, 20.5, 20.6 and 20.7. | **Affected Component** – SW.Tools.MEDebug<br>**Impact:**<br>**Workaround:** N/A<br>**Notes:**<br>Reproduction Steps:<br>1. Boot system and activate AMT.<br>2. Boot to OS.<br>3. Configure ME Debug viewer to collect log information from SUT.<br>4. Run Intel® ME Test Suite and choose Package->open->PPT->5MB_Firmware->Mobile->Wireless->Compliance_Power_G3-S5.xml<br>5. Select ME_PM_20.6 (or one of the others listed) and run it.<br>6. ME Debug Viewer displays the following:<br>"Power Button pressed for 5sec - transitions to S4->S5" to "Wait until the machine transitions to S5". | Deferred to Future Projects |

## 7.7 Closed – Documentation Change

| Issue # | Description | Affected Component/Impact / Workaround/Notes | Fixed in Kit# |
|---|---|---|---|
| 196736 | Incorrect VSCC values for SST and Chingis SPI parts in vsccommn.bin. | **Affected Component** – Documentation.SPIFlashProgrammingGuide<br>**Impact:** System will fail to boot.<br>**Workaround:**<br>**Notes:** vsccommn.bin file rev 2.7 was updated with the following changes:<br><br>Updated vscc value with 0x2009 and 0x2005 in vsccommn.bin for SST25VF016B, SST25VF032B, SST25VF040B, SST25F080B.<br>and<br>Updated Chingis device ID with 7F44h, 7F45h, 7F46h in vsccommn.bin for PM25LQ080C, PM25LQ016C, and PM25LQ032C | 8.1.0.1248 |

# 8 Known Issues

## 8.1 Open – ME Kernel

| Issue # | Description | Affected Component/Impact / Workaround/Notes |
|---|---|---|
| | | **Affected Component** –<br>**Impact:**<br>**Workaround:**<br>**Notes:**<br>Reproduction Steps: |

## 8.2 Open - Integrated Clock Control (ICC)

| | | |
|---|---|---|
| | | **Affected Component** –<br>**Impact:**<br>**Workaround:**<br>**Notes:**<br>Reproduction Steps: |

## 8.3 Open – Software / Tools

| Issue # | Description | Affected Component/Impact / Workaround/Notes |
|---|---|---|
| 196904 | 'MEinfowin32/64.exe –EOL' and 'MEinfowin32/64.exe' stop running on Win8x64 UEFI native boot OS environment. | **Affected Component** –SW.Tools.MeManuf<br>**Impact:** MEInfo and MEManuf –EOL doesn't work on EFI native boot OS environment.<br>**Workaround:** N/A<br>**Notes:**<br>Reproduction Steps: |
| 195872 | SUT will hang at POST code 0x96 if network cable is not plugged in before running Platform Debug Analyzer (Intel® PDA) tool. | **Affected Component** – FW.Kernel.MDES<br>**Impact:** Only occurs with a MDES enabled image and when the network cable is not connected.<br>**Notes:** |

## 8.4 Open – Intel® Identity Protection Technology

| Issue # | Description | Affected Component/Impact / Workaround/Notes |
|---|---|---|
| | | **Affected Component** –<br>**Impact:**<br>**Workaround:**<br>**Notes:**<br>Reproduction Steps |

## 8.5 Open – Intel® Upgrade Service

| Issue # | Description | Affected Component/Impact / Workaround/Notes |
|---|---|---|
| | | **Affected Component** –<br>**Impact:**<br>**Workaround:**<br>**Notes:**<br>Reproduction Steps |

## 8.6 Open – Not Firmware Related

| Issue # | Description | Affected Component/Impact / Workaround/Notes |
|---|---|---|
| | | **Affected Component** –<br>**Impact:**<br>**Workaround:**<br>**Notes:**<br>Reproduction Steps |

## 8.7 Open – Documentation

| Issue # | Description | Affected Component/Impact / Workaround/Notes |
|---|---|---|
| | | **Affected Component** –<br>**Impact:**<br>**Workaround:**<br>**Notes:**<br>Reproduction Steps |