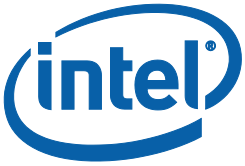

Intel® Management Engine Firmware 10 for Broadwell U/Y

5MB Release Notes - NDA

July 2019

Revision 10.0.60.3000 Hot Fix Release

Intel Confidential

Contents

Revision History

Revision Number	Description	Revision Date
10.0.25.1048	Production Version U/Y E-Stepping	June 2014
10.0.26.1000	Hot Fix Release	July 2014
10.0.27.1006	Hot Fix 2 Release	August 2014
10.0.28.1006 / 10.0.30.1006	Hot Fix 3 Release	September 2014
10.0.29.1000	Hot Fix 4 Release	September 2014
10.0.30.1060	Production Candidate 2 U/Y E and F-Steppings	October 2014
10.0.30.1072	Production Version 2 U/Y E and F-Steppings	October 2014
10.0.33.1012	Hot Fix Release	December 2014
10.0.35.1012	Maintenance Release	December 2014
10.0.37.1000	Hot Fix Release	December 2014
10.0.38.1000	Hot Fix Release	January 2015
10.0.45.1024	Maintenance Release	June 2015
10.0.46.1002	Hot Fix Release	July 2015
10.0.47.1006	Hot Fix Release	August 2015
10.0.50.1004	Maintenance Release	March 2016
10.0.55.3000	Maintenance Release	April 2017
10.0.56.3002	Hot Fix Release	November 2017
10.0.57.3000	Hot Fix Release	March 2018
10.0.60.3000	QSR Release	June 2018
10.0.60.3000v2	Hot Fix Release	July 2019

1 Introduction

1.1 Scope of Document

This document describes the content of this release and the changes since the previous versions.

This document covers the following Intel® Management Engine Firmware SKUs for the Broadwell Mobile U/Y Series platform:

- Intel® Management Engine Firmware Broadwell Mobile U/Y Series Platform.
  - Digital Office Intel® vPro™ (5MB)

1.2 End of Maintenance

Intel® Management Engine 10 firmware reached end of maintenance on September 30, 2018. This product will no longer be supported with functional and security updates.

Intel® Management Engine 11.0.6 software is compatible with Intel® Management Engine 8 firmware, Intel® Management Engine 9 firmware and Intel® Management Engine 10 firmware.

The 11.0 branch of this software release has also reached end of maintenance. This product will no longer be supported with functional and security updates.

Additional information about end of maintenance policy can be found on https://cdrdv2.intel.com/v1/dl/getContent/576893

1.3 Important Notes about This Release

Sections of this document that have been updated since the previous version are highlighted in yellow.

Intel® Management Engine Firmware 10 has been updated to remove certain 3rd party components. Updates include:

- The Intel reference BIOS binary used only on Intel reference platforms, also known as customer reference board (CRB) or reference validation platform (RVP), was removed from this release. No new release is planned for this BIOS binary.
- **This is a firmware-only release**. A hot fix version of Intel® ME 11.0 Software is available on VIP (https://platformsw.intel.com). This version has been updated to remove certain 3rd party components.
- Intel recommends that customers use the latest Intel® ME 11.0 Software (refer to the customer release communication for details of the software kit, including VIP kit number).
  Current release [May 2019] is Intel® ME SW version 11.0.6.1194v3 for Ivy Bridge, Haswell and Broadwell 5MB SKUs [**VIP. Kit 132220**]).

- This release includes bug fixes. For details, see Issues Closed in This Release.
- Intel® Identity Protection Technology (Intel® IPT) POR change: Intel® IPT support expanded to Intel® Pentium® and Intel® Celeron® processors (in addition to Intel® Core™ processors).

  This change is applicable for all generations supporting Intel® IPT (i.e. Sandy Bridge, Ivy Bridge, Haswell and Broadwell processors).

1.4 Best Known Configuration

For the latest Client Based Broadwell U/Y Mobile Platforms Best Known Configuration (BKC), please review Document ID#537047 **[Broadwell] Platform – Client-Based Platform Best Known Configuration for Broadwell Mobile Platform** - http://www.intel.com/cd/edesign/library/asmo-na/eng/539245.htm

2 Kit Details

2.1 Build Details

Kit	Build Details	Changes since previous release	Reasons for changes
Firmware Version	10.0.60.3000	No	N/A
Intel® MEBX Version	10.0.0.0007	No	N/A

2.2 FITC XML Compare

No changes in XML file.

3 Firmware Update Guidance and Restrictions

3.1 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.

3.1.1 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: 10.0.0.zzzz PV cannot upgrade to 10.1.0.zzzz Beta
- Update to firmware that has lower SVN (Security Version Number) is not allowed.
- Update to firmware that has lower VCN (Version control number) is not allowed.
- Update across major point release is not allowed for example 8.x to 9.x.
- If firmware update setting in Intel® MEBX is password protected, Intel® MEBX password must be supplied during the update.

3.1.2 VCN Firmware Upgrade / Downgrade Table

Intel® ME FW Version	SVN #	VCN #	PV (1 or 0)
10.0.57.3xxx (HF)	1	8	1
10.0.56.3002 (HF)	1	7	1
10.0.55.3000 (MR)	1	6	1
10.0.50.1004 (MR)	1	5	1
10.0.47.1006 (HF)	1	4	1
10.0.46.1002 (HF)	1	3	1
10.0.45.1024 (MR)	1	3	1
10.0.38.1000 (HF)	1	3	1
10.0.37.1000 (HF)	1	3	1
10.0.35.1012 (MR)	1	3	1
10.0.33.1012 (HF)	1	2	1
10.0.30.1072 (PV2 U/Y Series)	1	2	1
10.0.30.1060 (PC2 U/Y Series)	1	2	1
10.0.29.1000 (HF4 U/Y Series)	1	2	1
10.0.28.1006 (HF3 U/Y Series)	1	2	1
10.0.27.1006 (HF2 U/Y Series)	1	2	1

Intel® ME FW Version	SVN #	VCN #	PV (1 or 0)
10.0.26.1000 (HF U/Y Series)	1	2	1
10.0.25.1048 (PV U/Y Series)	1	2	1
10.0.25.1030 (PC U/Y Series)	1	1	1
10.0.20.1156 (Beta U/Y Series)	1	0	0
10.0.0.1042 (Alpha U-Series)	1	0	0
10.0.0.1012 (Alpha Y-Series)	1	0	0

- The VCN value was increased to 'x' with Intel® ME 10.0.57.3xxx HF as a result the fixed FW issues below, preventing downgrades from versions Intel® ME 10.0.57.3xxx and above to versions below Intel® ME 10.0.57.3xxx.

4 Issue Status Definitions

This document provides sightings and bugs report for Intel® Management Engine Firmware 10.0 SKU, Software and Tools for the Broadwell U/Y-Series Platform. Each report contains a snapshot of sightings and critical internal bugs dating to the Friday of the week in which it was released. At the time of a milestone release, this report will be distributed with the Intel® ME Kit and will provide information on new issues and the status of old issues (replacing the Release Notes document).

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

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

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

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

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

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

5 RCRs Added in this Release

RCR #	Description / Background	Build	Sku
N/A	N/A	N/A	N/A

6 Issues Closed in this Release

Issue #	Description	Affected Component/Impact / Workaround/Notes	Fixed in Kit#

6.1 Security bugs fixed

This section describes security bugs fixed in Intel® CSME / Intel® TXE in this Quarterly Security Release (QSR).

QSR	Technical Advisory (TA)	Doc #	Reference Details
Q2’ 18	PSIRT-TA-201805-001	597108	Intel® Converged Security Management Engine (CSME) Q2’2018 Security Release

7 Known Issues

7.1 Open – Intel® AMT

Issue #	Description	Affected Component/Impact / Workaround/Notes	Sku
100186531	Host driver does not connect within a few seconds in passive mode after resuming from Sx, or when enabling the wireless driver or during a restart.	**Affected Component** – WiAMT **Impact:** Redirection stress testing over WLAN may fail. **Workaround:** None. **Notes:** To be fixed in future Intel® PROset drivers kit release.	5MB

8 Archive – Fixes in Previous Releases

8.1 Closed – Intel® AMT (5MB)

Issue #	Description	Affected Component/Impact / Workaround/Notes	Fixed in Kit#
CVE-2017-5711	Mitigated security vulnerability documented in CVE-2017-5711 (http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=2017-5711)	**Affected Component:** FW.AMT **Impact:** CVSS 6.7 Medium AV:L/AC:L/PR:H/UI:N/S:U/C:H/I:H/A:H	10.0.56.3002
CVE-2017-5712	Mitigated security vulnerability documented in CVE-2017-5712 (http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=2017-5712)	**Affected Component:** FW.AMT **Impact:** CVSS 7.2 High AV:N/AC:L/PR:H/UI:N/S:U/C:H/I:H/A:H	10.0.56.3002
CVE-2017-13077	Mitigated security vulnerability documented in CVE-2017-13077 (http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=2017-13077) Wi-Fi Protected Access (WPA and WPA2) allows reinstallation of the Pairwise Transient Key (PTK) Temporal Key (TK) during the four-way handshake, allowing an attacker within radio range to replay, decrypt, or spoof frames.	**Affected Component**: FW.WiAMT **Impact:** CVSS 8.3 High AV:A/AC:H/PR:N/UI:N/S:C/C:H/I:H/A:H	10.0.56.3002
CVE-2017-13078	Mitigated security vulnerability documented in CVE-2017-13078 (http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=2017-13078) Wi-Fi Protected Access (WPA and WPA2) allows reinstallation of the Group Temporal Key (GTK) during the four-way handshake, allowing an attacker within radio range to replay frames from access points to clients.	**Affected Component**: FW.WiAMT **Impact:** CVSS 8.3 High AV:A/AC:H/PR:N/UI:N/S:C/C:H/I:H/A:H	10.0.56.3002

Issue #	Description	Affected Component/Impact / Workaround/Notes	Fixed in Kit#
CVE-2017-13080	Mitigated security vulnerability documented in CVE-2017-13080 (http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=2017-13080) Wi-Fi Protected Access (WPA and WPA2) allows reinstallation of the Group Temporal Key (GTK) during the group key handshake, allowing an attacker within radio range to replay frames from access points to clients.	**Affected Component**: FW.WiAMT **Impact:** CVSS 4.7 Medium AV:A/AC:L/PR:N/UI:N/S:C/C:N/I:N/A:L	10.0.56.3002
321450/ 1304846562	Some Intel® AMT features are not accessible when using domain local group.	**Affected Component:** FW.Network_Service.Kerberos	10.0.55.3000
321432	Security issue: Intel® AMT may crash during Kerberos authentication flow when processing a malformed Kerberos token.	**Affected Component:** FW.AMT.Kerberos **Impact:** Intel® AMT may crash. **CVSS:** 3.0/AV:N/AC:H/PR:N/UI:N/S:U/C:N/I:N/A:H	10.0.55.3000
1304881355	Security issue: Intel® ME enters recovery state after running PETS AMT_072 test.	**Affected Component:** FW.AMT.3PDS **Impact:** Recovery by reflashing image is required. CVSS score: Medium (4.4) (AV:L/AC:L/Au:S/C:N/I:N/A:C)	10.0.55.3000
	Fixed security vulnerability	Documented in CVE-2017-5689	10.0.55.3000
321360	When a platform wakes via Intel® AMT Alarm Clock, description displays "Unspecified event" instead of a general message regarding woken by alarm clock.	**Affected Component** – FW.AMT.AlarmClock **Impact:** Intel® AMT Alarm clock displays wrong wake message. **Workaround:** **Notes:** Reproduction Steps: 1. Add alarm. 2. Move platform to S5. 3. Let alarm wake the platform. 4. Verify event via Intel® WebUI. Data shows "Unspecified Event"	10.0.50.1004

Issue #	Description	Affected Component/Impact / Workaround/Notes	Fixed in Kit#
321416	Security issue: Insufficient Clickjacking Protection in Intel® AMT WEB UI	**Affected Component** – FW.AMT **Impact:** An attacker may be able to extract sensitive information from the platform **CVSS:** Medium	10.0.50.1004
321415	HostName, DomainName are cleared instead of returning to factory defaults, after unprovision / ME unconfiguration, after EOM	**Affected Component** –FW.AMT.Provisioning **Impact:** **Reproduction steps:** 1. Change the host and domain name through MEBX 2. Perform: FPTW64.exe -closemnf 3. Perform CCM/ACM Provisioning 4. Perform Full Unprovision / ME Unconfiguration	10.0.50.1004
321423	Possible corrupted playback of PAVP 2.0 or 3.0	**Affected Component** – FW.Apps.PAVP **Impact:** Due to a coding bug in Intel® ME firmware, legacy player programs that use Intel® ME's PAVP 2.0 or 3.0 may encounter corrupted playback.	10.0.50.1004
3327996	Sending a malformed packet to the Intel® Management Engine network stack could trigger a Denial of Service	**Affected Component** – FW.AMT.TCPIP **Impact:** Intel® ME manageability functionality (in Intel® AMT and Intel® Standard Manageability) and OEM-specific features that use the Intel® Management Engine network stack would stop working until G3 or Sx/Moff exit For further details see the security communication attached to the customer release announcement **CVSS v2 Rating:** 8.6 (High) < AV:N/AC:L/Au:N/C:N/I:P/A:C >.	10.0.45.1024
320931	After DAD failure, AMT does not reconfigure its DHCPv6 IP address	**Affected Component** – FW.AMT.NETP **Impact:** AMT remains without DHCPv6 IP Address **Recovery:** Disable/Enable IPv6	10.0.45.1024
320922	After S4->S0 with disconnected cable, the PHY is not in Ultra Low Power ULP (ME in PP2)	**Affected Component** – FW.AMT.Link Manager **Impact**:	10.0.45.1024

Issue #	Description	Affected Component/Impact / Workaround/Notes	Fixed in Kit#
MWG100228334	Unexpected shut down during S3 stress test with active AMT and WLAN profile added	**Affected Component:** iAMT **Impact:** Unexpected shut down.	10.0.45.1024
100225145	When running S3->S0 stress test, after a few hundreds iterations the platform may go to S5 because of a CLINK hang	**Affected Component** – WiAMT **Impact:** Any work on user desktop will not be saved when moving from S3->S5 **Workaround:** The issue has been dealt with via the following workaround: Limiting bus capabilities to minimal to avoid CLINK hang. Once the problematic scenario appears, interrupts and master accesses of the NIC are disabled.	10.0.38.1000
100225145	When running S3->S0 stress test, after a few hundreds iterations the platform may go to S5 because of a CLINK hang	**Affected Component** – WiAMT **Impact:** Any work on user desktop will not be saved when moving from S3->S5 **Workaround:** Limit bus capabilities to minimal to avoid CLINK hang. Once the problematic scenario appears, interrupts and master accesses of the NIC are being disabled. **Notes:** The issue is fixed with a workaround	10.0.37.1000
320876	On an image with NFC enabled, after disabling NFC in BIOS and performing a clear CMOS,BIOS menu shows NFC support as disabled and NFC Feature State as enabled, MEManuf test fails, and yellow bang is shown on the NFC device	**Affected Component** – FW.NFC **Impact**: After disabling NFC in BIOS and performing a clear CMOS, the NFC is shown as disabled in the BIOS (expected behavior is to show as enabled). MEManuf test fails and the NFC device appears with a yellow bang **Recovery:** A warm reset in 1.5 MB SKU or a cold reset in 5MB SKU	10.0.35.1012
100219909	When WLAN is enabled, after a few local restarts a Global reset occurs.	**Affected Component** – WiAMT **Impact**: A Global reset occurs instead of a local restart when performing a few local restarts.	10.0.35.1012

Issue #	Description	Affected Component/Impact / Workaround/Notes	Fixed in Kit#
320684	While executing extended stress testing with Connected Standby cycles on SUT, system may enter S5 state.	**Affected Component** – FW.LAN.Driver **Impact:** System may reset/shutdown during Connected Standby state. **Workaround:** None. **Notes:** Reproduction Steps: 1. Boot to OS and install all mandatory drivers. 2. Ensure no yellow bang and clear event log error before doing cycling. 3. Ensure all CS BIOS settings are followed. 4. Run CS cycle stress testing and observe SUT enter S5 state instead of returning to CS state.	10.0.30.1060
100216830	During a full BIOS/FW update, WLAN micro code does not get updated.	**Affected Component –** WiAMT **Impact**: May not be able to validate FW update. **Workaround**: None.	10.0.30.1060
320871	Physical LAN disconnect stress tests cause Intel® ME to go through system discrepancies.	**Affected Component –** FW.AMT.Link Manager **Impact**: PG flow/network connectivity dysfunctional, system may shutdown. **Workaround**: None. **Notes:** Reproduction Steps: 1. In S0 disconenct LAN. Verify PG entry. 2. Move to Microsoft* InstantGo by Power Button. 3. Move back to S0 by power button. 4. Connect LAN cable verify connectivity to OS.	10.0.30.1048
320824	When OS LAN driver is enabled (from D3 to D0) Intel® ME loses its PG functionaility.	**Affected Component** – FW.AMT.Link Manager **Impact:** PG flow disabled. **Workaround:** None. **Notes:** Reproduction Steps: 1. Configure Mircosoft* InstantGo enabled. 2. Remove LAN cable. 3. Restart to OS. 4. Verify Intel® ME PG. 5. Disable LAN driver. 6. Verify PG entry stable. 7. Run Intel® MEInfo to exit PG state. 8. Enable LAN driver.	10.0.30.1048

8.2 Closed – Intel® ME Kernel

Issue #	Description	Affected Component/Impact / Workaround/Notes	Fixed in Kit#
321354	PlayReady 3 playback is corrupted when an external monitor is connected and HDCP is not enabled	**Affected Component –** FW.Apps.PAVP **Impact:** Playback corrupted **Reproduction steps:** 1. Start playback. 2. Plug in an external monitor. Instead of just providing an error code, playback is corrupted.	10.0.47.1006
321323	There was an arithmetic bug in the implementation of the PlayReady 3.0 license acquisition. As a result, approximately 1.4% of license acquisitions may fail, preventing movie playback.	**Affected Component –** FW.Apps.PAVP **Impact:** Approximately 1.4% of license acquisitions may fail, preventing movie playback	10.0.46.1002
321315	Intel® PTT remains enabled even though the Shipping State has been set to Disabled (bit 29 in featureShipState.)	**Affected Component** – FW.Kernel.SkuMgr	10.0.46.1002
321305	NFF is supported in firmware even though Intel® TA is no longer POR	**Affected Component –** FW.Kernel.SkuMgr	10.0.45.1024
320858	Intel® ME FW dictates a CPU replacement message after a G3 flow with Intel® ME disabled.	**Affected Component** – FW.Bringup **Impact:** May be unable to perform BIOS updates on WiAMT enabled platforms. **Workaround:** None	10.0.30.1048
320813	During extended stress testing on systems where Microsoft* InstantGo is enabled (Intel® ME Power Gating is active), the Intel® ME may experience file system corruption.	**Affected Component** – FW.Kernel.PowerManagment **Impact:** May cause system shutdowns or Intel® MEI yellow bang in Windows* device manager. **Workaround:** None	10.0.28.1006
320629	After Intel® ME BIOS Payload message, HECI may indicate it is ready to receive messages before it is able to receive.	**Affected Component** – FW.Kernel.HECI **Impact:** May cause HECI message sent after MBP to be incomplete to Intel® ME. **Workaround:** None	10.0.25.1048
320487	Intel® ME exits Intel® ME PG state immediately.	**Affected Component** – FW.Kernel.TCPIP **Impact:** May prevent power saving. **Workaround:** Allow SUT to move to Power Gating (PG) after 30 minutes. **Notes:** Occurs after configuring system with Connected Standby, booting to OS and removing LAN cable when system is idle.	10.0.25.1048

Issue #	Description	Affected Component/Impact / Workaround/Notes	Fixed in Kit#
320287	Intel® ME returns KA Timeout as wake reason for valid Remote Wake.	**Affected Component** – FW.Kernel **Impact:** Wake reason can be overwritten if the server send wake packet followed by disconnect packet. **Workaround:** None	10.0.25.1048

8.3 Closed – Intel® Dynamic Application Loader (DAL)

Issue #	Description	Affected Component/Impact / Workaround/Notes	Fixed in Kit#
321102	On systems where EOP precedes the loading of Intel® DAL (when EOP is sent after less than 1 second after the BIOS has loaded), Intel® DAL does not get initialized (because it is waiting for the EOP message, which already occurred).	**Affected Component** – FW.JoM.JVM **Impact:** Breaks Intel® DAL functionality and Intel® IPT (Identity Protection Technology), Intel® YAP (You are the Password), Intel® SA (Security Assist) and Intel® MFA (Multi Factor Authentication). **Workaround:** None.	10.0.38.1000

8.4 Closed – Intel® Device Protection Technology with Boot Guard / Intel® PTT

Issue #	Description	Affected Component/Impact / Workaround/Notes	Fixed in Kit#
321438	Some NV data could still be read after the NV index has been deleted.	**Affected Component** – FW.PTT.Main **CVSS:** (AV:L/AC:L/Au:S/C:C/I:C/A:C)	**10.0.55.3000**
321359	Intel® PTT security issue. See attached communication for details.	**Affected Component –** FW.PTT.Main	10.0.47.1006
321325	Intel® PTT returns TPM_RC_NV_SPACE response code when trying to define an NV Index with data size less than 0x360 bytes in Windows 10.	**Affected Component –** FW.PTT.Main	10.0.47. 1006
321345	Policy fails with RC_Expired message even though expiration value is legal	**Affected Component –** FW.PTT.Main	10.0.47.1006
320721	Decrypting a buffer that was encrypted from a buffer smaller that the key size, returns the decrypted/original buffer plus additional data from the end of the original buffer.	**Affected Component –** FW.PTT.Main	10.0.47.1006

Issue #	Description	Affected Component/Impact / Workaround/Notes	Fixed in Kit#
321347	TPM2_GetCapability returns moreData = 0 (instead of 1) when requesting 0 persistent handles even though there are persistent handles present in PTT	**Affected Component –** FW.PTT.Main	10.0.47.1006
321155	PTT: It is possible to load session context after it was flushed	**Affected Component** – FW.PTT.Main **Impact:** Enables reuse of authorization session. CVSS score: Low (OA:N/PP:N/AV:L/AC:L/AU:N/CI:P/II:P/AI:N/SU:RPh)	10.0.45.1024
321197	PTT enters failure mode after TPM2_HMAC command when keys alg and hashAlg are null	**Affected Component** – FW.PTT.Main **Details:** Instead of returning TPM_RC_VALUE, PTT returns RC_FAILURE and enters failure mode	10.0.45.1024
321266	PTT: RSA Sign operation takes longer than required	**Affected Component** – FW.PTT.Main **Details:** RSA Sign operation takes approx. 1300ms instead of completing within 500ms	10.0.45.1024
321289	RSA key-cache does not refill when empty	**Affected Component –** FW.PTT.Main	10.0.45.1024
\320951	Some NV data could still be read after the NV index has been deleted.	**Affected Component** – FW.PTT.Main **Impact:** NV data could still be read even though it was deleted. **CVSS Score:** 4.9 (Medium) (AV:L/AC:L/Au:N/C:C/I:N/A:N).	10.0.35.1012
320927	In some cases, it is possible to set the TPM clock to an older clock.	**Affected Component** – FW.PTT.Main **Impact:** Use cases relying on TPM clock (e.g. remote attestation) could be impacted **CVSS Score:** 4.9 (Medium) (AV:L/AC:L/Au:N/C:N/I:C/A:N).	10.0.35.1012
320929	TPM yellow bang displays in Windows* Device Manager and is unrecoverable.	**Affected Component** – FW.PTT.Main **Impact:** TPM not functional. **Workaround:** None - reset/G3/CLR CMOS/Reflash will not clear or recover once TPM experiences a yellow bang.	10.0.30.1072
320708	System hang during S3/S4 stress testing. System does not resume from S3/S4 and system may hang with POST Code 0x00AD or 0x0096.	**Affected Component** – FW.PTT.Main **Impact:** Intel® PTT may cause a BDW 2+2 SUT from resuming after strenuous Sx cycle testing. **Workaround:** None.	10.0.26.1000

8.5 Closed – Software / Tools

Issue #	Description	Affected Component/Impact / Workaround/Notes	Fixed in Kit#
320894	Intel® ME reset occurs after many iterations of Intel® MEI disable/enable stress testing.	**Affected Component –** SW.HECI Driver **Impact**: Intel® ME may reset **Workaround**: None. **Notes:** Reproduction Steps: 1. Setup SUT with latest FW and Intel® ME SW version 10.0.28.1000. 2. Run Intel® MEI disable/enable stress testing and monitor the Windows Device Manager or Event Viewer for a yellow bang error for the Intel® MEI driver.	10.0.30.1060
320784	Intel® MEI reset after sleep cycle stress testing.	**Affected Component** – SW.HECI Driver **Impact:** Intel® MEI may reset. **Notes:** Reproduction Steps: 1. Boot to OS. 2. Run automated S0-S3 cycling. 3. Open event viewer.	10.0.30.1060
320673	Intel® Management Security Status shows "Information unavailable" for the IPv6 address.	**Affected Component** – SW.AMT.Icon **Impact:** IPv6 address doesn't appear in Intel® IMSS. **Workaround:** None. **Notes:** Reproduction Steps: 1. Enable IPv6 via Intel® AMT WEBUI. 2. Check IPv6 address of the LAN via Intel® MSS. 3. WLAN address appears in LAN interface.	10.0.30.1018
320639	Intel® Management Security Status requests system to reboot even though SOL is activated successfully.	**Affected Component** – SW.AMT.Services **Impact:** OS needs reboot even when SOL is active. **Workaround:** None. **Notes:** Reproduction Steps: 1. Flash new image to board. 2. Provision via Intel® MEBX. 3. Boot to OS. 4. Install appropriate SWs 5. Open device manager and confirm that SOL is activated successfully. 6. Intel® Management Security Status requests user to reboot sytem.	10.0.28.1006

Issue #	Description	Affected Component/Impact / Workaround/Notes	Fixed in Kit#
320755	The handle count of the system process keeps increasing at every S4/S3 cycle.	**Affected Component** – SW.AMT.Services **Impact:** Old notification handle does not close after resume. **Workaround:** None.	10.0.28.1006
320570	Intel® Management Engine Interface yellow bang issue when run warm boot or Sx stress testing.	**Affected Component** – SW.HECI Driver **Impact:** Intel® MEI driver may display a yellow bang after extensive warm reboot stress testing. **Workaround:** Shutdown and restart SUT Intel® MEI driver will no longer be in yellow bang state and will function as expected.	10.0.27.1006

8.6 Closed – Not a Firmware or Software Bug

Issue #	Description	Affected Component/Impact / Workaround/Notes
100203825	When resuming from S3 with an active IDER session, the session gets closed.	**Affected Component** – WiAMT **Impact:** May lose IDER session over wireless. **Workaround:** Reattempt IDER session. **Notes:** Not a FW issue. Debugging wireless driver.
100209192	In a Connected Standby state, the host sends DHCP Requests in ~20 second intervals regardless of the DHCP Lease Time.	**Affected Component** – WiAMT **Impact:** Connectivity loss and impacts CS related compliance testing. **Workaround:** None. **Notes:** Not a FW issue.
320538	SUT hangs are postcode "0xEC02" after resuming from G3 to S5-Moff DC only to S0-M0 via power button press.	**Affected Component** –Embedded Controller **Impact:** **Workaround:** Issue can be avoided by hitting the power button before 10 seconds are up. **Notes:** Doesn't occur when State after G3 in BIOS is set to S0. Only occurs on DC power after G3. Doesn't happen when state after G3 is AC/DC or AC.
320501	Intel® AMT WEBUI may not be able to reconnect within the expected amount of time when running S4 wake by RCO stress testing.	**Affected Component** – FW.AMT.WEB UI **Impact:** Unable to reconnect WEBUI session without delay. **Workaround:** Issue can be avoided by hitting the power button before 10 seconds are up. **Notes:** No longer able to reproduce with latest firmware. May have been a test tool issue.

Issue #	Description	Affected Component/Impact / Workaround/Notes
320510	After running "fpt -closemnf" to fuse the part followed by G3 and CMOS clear, "PTT Lockout Override Counter" does not increment as expected in DOS and EFI.	**Affected Component** – FW.PTT.HCI **Impact:** Counter does not increment when executing "PTT Lockout Override Counter" in DOS/EFI versions of FPT however Windows* version works as expected. **Workaround:** Perform operation in Windows* version. **Notes:** Not a bug. DOS/EFI cannot take ownership of TPM and must test after booting at least once to Windows* after flashing FW.
215843	Error 7: Hardware sequencing failed when flashing image on SUT.	**Affected Component** – SW.Tools.FlashProgrammingTool **Impact:** Potential Hardware Sequencing failure when flashing image. **Workaround:** None **Notes:** Not POR and therefore not a bug. Reproduction Steps: 1. Flash Full_Image to board 2. Boot to OS 3. Run "FPT.exe -f image.bin" 4. or 5. Flash Full_Image to board 6. Boot to OS 7. Run "FPT.exe -d InitBios.bin -bios" 8. Reboot SUT 9. Run "FPT.exe -f InitBios.bin -bios". 10. Error 7: Hardware sequencing failed. (while trying to erase)

8.7 Closed – No Plan to Fix

Issue #	Description	Affected Component/Impact / Workaround/Notes
320984	When establishing a KVM session, the connection fails since User Consent does not show up	**Affected Component** – FW.AMT.UserConsent **Impact:** When a system is trying to display a User Consent sprite to the local-user for connection authorization before establishing a KVM session, a message "Error: 0x80862400 Sprite failure." Will appear and the KVM connection will fail. **Notes:** This issue happens with the combination of PV1 FW and PV2 SW. Intel recommends to upgrade the firmware and software to align to Intel® ME PV2 or later to avoid this issue. Issue is relevant only when using localization languages on systems with IMSS
320505	Updating FOV "FeatureShipState" on Bit29 PTT feature does not take effect after global reset.	**Affected Component** – FW.Kernel.SkuMgr **Impact:** Updating FOVs may not update the Intel® PTT enable bit. **Workaround:** None

Issue #	Description	Affected Component/Impact / Workaround/Notes
214984	Intel® ME does not wake to M3 by ping from Moff after idle timeout if MDES LAN is enabled.	**Affected Component** – FW.Kernel **Impact:** Once Intel® ME transits to OFF status in S3/4/5, Intel® ME can not be woken up by pinging from LAN or WLAN. **Workaround:** None
215804	"Fast Call for Help" button become available when WiAMT is enabled and LAN or WLAN device is disabled in device manager	**Affected Component** – SW.AMT.Icon **Impact:** "Fast Call for Help" button become available when WiAMT is enabled and LAN or WLAN device is disabled in device manager **Workaround:** When issue occurs, click the "Disconnect" button and then the button status will be correct **Notes:** Reproduction Steps: 1. Flash bios and provision Intel® ME 2. Setup Intel® ME to connect to Wireless profile via WebUI 3. Boot to OS and confirm the Intel® ME has been connected to wireless accordingly. 4. Disable wireless or LAN device in OS device manager 5. Check IMSS "Fast Call for Help" button. ---> (if status still normal in step 5, go to next step.) 6. Set System to enter S3. 7. Resume from S3. 8. Check IMSS "Fast Call for Help" button. ----> (button will become available and show up "Get Technical Help") 9. Click on "Get Technical Help" button. 10. IMSS will pop-up warning message for failing to reach your support organization. 11. Click on OK button to close warning message. Check on "Fast Call for Help" button become available and show up "Disconnect".
215998	"FPT -r NfcGpioIrq" shows wrong FOV value "00" after the value is set to "01.	**Affected Component** – FW.NFC **Impact:** Affects GPIO NFC IRQ pin assignment. **Workaround:** Enable NFC before configuring it. **Notes:** Deferred to Intel® ME 11 platform. Occurs when setting GPIO73 for NFC IRQ pin e.g.# FPT -u -n nfcgpioirq -v 01. Reproduction Steps: 1. On CRB run "FPT -u -n nfcgpioirq -v 01" to set GPIO73 for NFC IRQ pin. 2. Run "FPT -r nfcgpioirq" to check the update of FOV value. 3. #2 result is "Value: GPIO26 / 00" instead of expected "Value: GPIO73 / 01".

8.8 Closed – External Dependency

Issue #	Description	Affected Component/Impact / Workaround/Notes
319851	Intel® MEI driver does not release LMS Service from Intel® SBA service for Intel® ME SW Update and an error message "Windows could not start Intel SBA service on local computer. Error 1075: the dependency service does not exist or has been marked for deletion." is displayed.	**Affected Component** – External Dependency - SBA **Impact:** Intel® SBA loses functionality after reinstalling the Intel® MEI driver.
5528387 / 3527697	During KVM session, a delay is seen upon mouse movement resulting in a difficult remote session for the user.	**Affected Component** – Graphics Driver **Impact:** Difficult operation of remote KVM. **Workaround:** None **Notes:** Graphics hardware related issue.
100210521 / 320610	When attempting to open a KVM session, KVM closes immediately but the border frame UI remains on screen, indication that the KVM session may still be active.	**Affected Component** – WiAMT **Impact:** May be unable to establish KVM session over LANless SUT; loss of redirection sessions. **Workaround:** None **Notes:** Test environment misconfiguration, retested without error, confirmed not a bug.
320538	SUT hangs are postcode "0xEC02" after resuming from G3 to S5-Moff DC only to S0-M0 via power button press.	**Affected Component** –Embedded Controller **Impact:** **Workaround:** Issue can be avoided by hitting the power button before 10 seconds are up. **Notes:** Doesn't occur when State after G3 in BIOS is set to S0. Only occurs on DC power after G3. Doesn't happen when state after G3 is AC/DC or AC.
319776	SUT is unable to ping or access Intel® AMT while in any Sx state.	**Affected Component** – External Dependency – LAN Drivers **Impact:** Ping requests time out and operator is unable to access remote Intel® AMT in Sx mode. **Workaround:** Recovery via G3. **Notes:** Trending as a LAN driver issue.
5316933 / 320362	When CSM is disabled in the BIOS - IDER UEFI floppy device is ignored.	**Affected Component** – External Dependency - BIOS **Impact:** IDER UEFI floppy device fails, but IDER UEFI CD is working. **Workaround:** None. **Notes:** Not a requirement
320649	When secure boot is enabled in BIOS, booting to an IDER device while a SOL session is open causes a black screen.	**Affected Component** – External Dependency - BIOS **Impact:** Remote operation hangs with black screen and must reset to recover. **Workaround:** Recovery via RCO reset.

8.9 Closed- Security Issues

Issue #	Description	Affected Component/Impact / Workaround/Notes	Fixed in Kit#
1305593301	Mitigated security vulnerability CVE-2018-3628 (http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=2018-3628) Details anticipated to be published June 11th 2018	**Affected Component:** fw.network_service.network For more details, refer to NDA Technical Security Advisory PSIRT-TA-201803-001 (DocID# 576603)	10.0.57.3000
1305593302	Mitigated security vulnerability CVE-2018-3629 (http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=2018-3629) Details anticipated to be published June 11th 2018	**Affected Component:** fw.network_service.network For more details, refer to NDA Technical Security Advisory PSIRT-TA-201803-001 (DocID# 576603)	10.0.57.3000
1305443822	Mitigated security vulnerability CVE-2018-3632 (http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=2018-3632) Details anticipated to be published June 11th 2018	**Affected Component:** FW.amt.environment_detection For more details, refer to NDA Technical Security Advisory PSIRT-TA-201803-001 (DocID# 576603)	10.0.57.3000

8.10 RCRs

RCR #	Description / Background	Build
1304204249	**Description**: Removed RC4 cipher suite support from Intel® AMT. **Background:** Intel® AMT supports RC4 cipher suite as part of the TLS implementation. The RC4 cipher suite has been in the product since Intel® AMT 1.0. At that time, it was the primary cipher suite used by popular Web Browsers. Since then, newer cipher suites have been integrated into the product. RC4 cipher suite is no longer considered to provide a sufficient level of security for TLS sessions.	10.0.55.3000
1304144973	**Description**: Added SHA2 root certificate hashes to support Remote Configuration **Background:** Microsoft has announced its decision to deprecate the use of SHA1 on January 1, 2017 and to replace it by SHA256. All certificates, roots and intermediates signed in SHA1 will no longer be recognized. Plans within the industry have been made to transition from SHA1 to SHA256 (SHA2). Certificate Authorities have started issuing new SHA2 certificates.	10.0.50.1004

RCR #	Description / Background	Build
1804188649	**Description**: Replaced all existing default SHA1 hashes from SHA1 hash with SHA256 hashes (for the same root certificates) **Background:** Microsoft has announced its decision to deprecate the use of SHA1 on January 1, 2017 and to replace it by SHA256. All certificates, roots and intermediates signed in SHA1 will no longer be recognized. Plans within the industry have been made to transition from SHA1 to SHA256 (SHA2). Certificate Authorities have started issuing new SHA2 certificates.	10.0.50.1004
CCG0100011204	**Description:** Validate functionality of ME System Tools and ME Tools under Microsoft Windows* 10 PE. **Background:** Microsoft is releasing Windows* 10 PE. The RCR is to validate that tools function properly on this OS.	10.0.47.1006
CCG0100011196	Remove NFF from ME10 firmware and tools. **Background**: NFF is no longer POR. Support removed from firmware and tools.	10.0.46.1002
CCG0100011142	**Description:** Validate functionality under Microsoft Windows* 10 **Background:** Microsoft is releasing Windows* 10. The RCR is to validate that Intel® ME 10 firmware with Intel® ME 11 software function properly under Windows 10.	.10.045.1024
CCG0100011054	**Description:** Add support for Microsoft Play Ready 3 for Microsoft Windows 10. **Background:** Microsoft Play Ready 3 is a feature of Microsoft Windows 10.	.10.045.1024
CCG0100011142	**Description:** Validate functionality under Microsoft Windows* 10 **Background:** Microsoft is releasing Windows* 10. The RCR is to validate that Intel® ME 10 firmware with Intel® ME 11 software function properly under Windows 10.	.10.045.1024
CCG0100011054	**Description:** Add support for Microsoft Play Ready 3 for Microsoft Windows 10. **Background:** Microsoft Play Ready 3 is a feature of Microsoft Windows 10.	.10.045.1024
CCG0100011159	**Description:** Implement HDCP 2.2 Errata for Intel® WiDi support	10.0.45.1024

RCR #	Description / Background	Build
CCG0100011172	**Description:** Add Support for 896 bit certificates **Details**: Functionality added to DAL to support 896 bit key size for the following RSA operations: • Raw RSA encryption • RSA encryption (with PKCS1 padding scheme or OAEP padding scheme) • RSA signing (with SHA1 and SHA256 hashing algorithms and PKCS1 padding scheme). • RSA Key generation	
CCG0100011163	**Description:** Remove SSL 3.0 support from Intel® ME firmware **Background:** SSL 3.0 was vulnerable to the Padding Oracle On Downgraded Legacy (POODLE) attack	10.0.35.1012
CCG0100011163	**Description:** Remove SSL 3.0 support from Intel® ME firmware **Background:** SSL 3.0 was vulnerable to the Padding Oracle On Downgraded Legacy (POODLE) attack	10.0.33.1012
CCG0100011067	**Description:** Add 2 new fields under the "Features Supported" tab within the FITc tool and update FITc XML for Intel® Network Frame Forwarder. **Background:** Intel® Network Frame Forwarder is an Intel® ME feature that is part of a broader SW solution targeted at allowing browser applications to access platform capabilities as web services. The full SW solution will be used by ISVs and can be pre-installed by OEMs. Frame Forwarder is a commonly used mechanism that allows applications to access web assets across multiple networks. Intel® NFF is an implementation of this base functionality embedded within Intel® ME Firmware (Intel® ME 10) and is used to route frames received via USB-R interface to host based applications. Additional details can be found in CDI doc# 552661.	10.0.30.1060 RCR was added in 10.0.30.1060 PC2 kit but was not included in Release Notes
CCG0100011083	**Description:** Removal of RPMC from 10.0.30.1060 PV2 release and future kits. **Background:** RPMC was introduced as a new feature with Intel® ME 10 BDW to provide replay protection to Intel® ME and binding between the PCH and the SPI parts on the board allowing data to be stored in the SPI which is not based on RTC power.	10.0.30.1060
CCG0100011029	**Description:** Allow host to read PCH Protected RTC via MEI message.	10.0.25.1030

RCR #	Description / Background	Build
	Background: Customers may require a reliable method to track how long each system has been running across an entire lifespan and request read access to a stable RTC unmodifiable by host software.	
CCG0100011026	**Description:** NFC State Control via BIOS. **Background:** Adds support for BIOS to enable/disable NFC if NFC is 'Enabled' in FW image using FITc/FOV allowing IT administrators in the field to control NFC.	10.0.25.1030
CCG0100198241	**Description:** Add an option to prevent Intel® IFR SW installation in the Intel® ME SW installer. **Background:** The Intel® ME 10 SW installer for Intel® ME 10 and backwards compatible to Intel® ME 9.x and 8.1 platforms uses a MSI Installer instead of the previous open package and does not allow OxMs or end customers from deselecting features during an installation.	10.0.25.1030
CCG0100010800	**Description:** Add FW support to allow disabling Intel® ME FW watch dog timer (WDT) even when SPI descriptors are locked. **Background:** Watch Dog Timer is a timer that is used by the Intel® ME to prevent any possible hang. The WDT will be triggered if there is no activity from the ARC processor for more than 30 seconds.	10.0.25.1030
CCG0100010579	**Description:** Control Intel® ME Unconfigure on RTC Clear. **Background:** The Intel® ME now provides a method for controlling the Intel® ME unconfigure (return to factory defaults) event upon detection of an RTC clear event via BIOS.	10.0.25.1030
CCG0100010734	**Description:** Add support for Microsoft Windows* 7 with 1.5 MB SKU FW. **Background:** Request to add Windows 7 and 1.5MB firmware support for small business SKU's still shipping with Windows* 7.	10.0.25.1030

RCR #	Description / Background	Build
CCG0100197668	**Description:** Pre-manufacturing DCI Control. **Background:** DCI enables closed chassis debug using a USB3 port. This RCR allows OEMs to enable DCI on platforms in Pre-manufacturing state through the PCH soft strap 10, bit 5.	10.0.20.1156
CCG0100196813	**Description:** FITC SKU Emulation– No Emulation Support preproduction. **Background:** The Intel® ME10 Firmware will support both BDW PCH-LP and HSW PCH-LP. The lack of a no emulation option in the SKU emulation drop down box when loading pre-production FW in FITC, is causing the need for 2 firmware images to be produced (one for HSW and one for BDW) since each force a different SKU emulation.	10.0.20.1156
CCG0100010944 / CCG0100010294	**Description:** NFC over NCI support on HSW with Intel® ME10. **Background:** NCI protocol support is a Windows* 8.1 logo requirement and must be supported by NFC solution providers. Intel® ME FW will support the NCI protocol for communication with the NFC module on HSW platforms with Intel® ME FW 10 and support of the old HCI protocol will be deprecated.	10.0.20.1156
CCG0100010916	**Description:** Adding BUS driver capabilities to Intel® MEI Driver. **Background:** The Intel® MEI driver acts as a communication channel between Host SW and Intel® ME FW clients. The OS can load/unload them in any order, therefore, an OS could unload Intel® MEI driver before unloading the NFC Driver which may lead to communication and timing issues between NFC and Intel® MEI driver.	10.0.20.1156
CCG0100010898	**Description:** Multiple Chipset Init Table Support. **Background:** Intel® ME 10 firmware is required to support both Haswell-LP and Broadwell-LP PCH hardware with the same firmware build. Multiple Chipset Init tables are required to ensure proper system operation and this RCR allows multiple chipset table to be used with one FW image.	10.0.20.1156

RCR #	Description / Background	Build
CCG0100010879	**Description:** Intel® Platform Protection Technology Support on Intel® vPro™ Platforms with Intel® TXT Disabled **Background:** Intel® Platform Protection Technology is supported on Corporate SKUs (5MB) in addition to Consumer SKUs (1.5MB). Since Intel® Platform Protection Technology and Intel® TXT are incompatible, currently the support of Intel® Platform Protection Technology on an Intel® vPro™ machine is not explicitly defined This RCR confirms that Intel® Platform Protection Technology is supported on a Corporate SKU (5MB) vPro platform, when Intel® TXT is disabled.	10.0.20.1156
CCG0100010776	**Description:** Intel® PTT Gen2 functionality (excluding SPI RPMC) to Intel® ME10 on Haswell-LP. **Background:** Platforms launching after 1.1.2015, will need to support Intel® PTT Gen2 command profile (excluding SPI RPMC), in order to be able to get the Windows* 8.1 logo certification. This RCR asks for Intel® ME10 to support SHA2 PCRs + ECC + EK cert (a.k.a. Intel® PTT Gen2) on Haswell-LP platforms.	10.0.20.1156
CCG0100010822	**Description:** Remove Chip Erase Command Support from FPT. **Background:** FPT will not support the chip erase (-c) command any longer to accommodate RCR CCG0100010574.	10.0.20.1156
CCG0100010623	**Description:** SPI RPMC (also known as Intel® PTT Gen2) Default Mode Change. **Background:** SPI Based monotonic counters is a new approach for enabling anti-replay monotonic counters (RPMC) on the platform. It requires enabling a SPI part with special support for anti-replay monotonic counters. SPI RPMC can be enabled/disabled via FITC (Enabled by default).	10.0.20.1156

RCR #	Description / Background	Build
CCG0100010579	**Description:** BIOS Control on Intel® ME un-configure when RTC is cleared. **Background:** OEMs can design their platform without RTC coin battery and use the Main Battery to power the RTC well. Some applications of Intel® ME store information on the RTC well. When the RTC well is cleared, Intel® ME performs the Intel® ME Unconfigure operation which could cause loss of all data stored in RTC and thus, reverting some of the application to factory default (e.g. Intel® AM Un-provision). In order to mitigate the risk in an RTC less design, this RCR allows BIOS to control the Intel® ME un-configure operation upon RTC clear.	10.0.20.1156
CCG0100010574	**Description:** Flash Device Hardening - NIST-800-147 Manufacturing Tools Support. **Background:** As part of security improvements, FITC will set the default value for the Invalid Opcode (0-7) settings. FITC will set the Invalid Opcode values in the descriptor as follows: Instruction 0 – 0x21 Instruction 1 –0x42 Instruction 2 –0x60 Instruction 3 – 0xAD Instruction 4 –0xB7 Instruction 5 –0xB9 Instruction 6 – 0xC4 Instruction 7-0xC7 The blocked Opcodes are communicated to the PCH SPI Controller by the OEM, through the flash image (In the descriptor region) FPT will read the FLILL and FLILL1 invalid opcode registers when a chip erase is requested. If the chip erase opcode is in the black list, the tool will return an error indicating that the command is prevent from executing and the user should use the block erase command instead.	10.0.20.1156
CCG0100010496	**Description:** Add FWSTS bit to indicate if SPI log is empty or non-empty. **Background:** When Intel® ME Firmware detects any critical errors/events, MDES SPI Flash logging feature will store those messages in the SPI flash. Currently there is no mechanism available to indicate if SPI log is empty or non-empty. RCR adds FWSTS bit to indicate if SPI log is empty or non-empty and defines bit 15 to Extended Firmware status (FWSTS2). Additionally, MEINFO tool will indicate if SPI log is empty or not.	10.0.20.1156
CCG0100010465	**Description:** Simplify SPI refurbish process for SPI RPMC (a.k.a Intel® PTT Gen2). **Background:** Intel® PTT Gen2 (SPI Based Monotonic Counters) requires binding between the PCH and the SPI and exchange of a root key over the SPI bus. When the SPI part is replaced, a rebind	10.0.20.1156

RCR #	Description / Background	Build
	is required. In order to make sure the rebind is done in authorized environment, by authorized personal, an external means of authentication is required. OEM was required to implement authentication server environment in manufacturing line or in refurbish lab.	
CCG0100010311	**Description:** Adding Intel® ME10 Support to Haswell+ LPT-LP MCP products. **Background:** Intel® ME10 Will be able to load on a Haswell ULT based platform (Haswell + LPT-LP MCP). When running on this HW configuration, Intel® ME10 will not have any new feature. Only baseline transfer from Intel® ME9.5 is supported.	10.0.20.1156
CCG0100010234	**Description:** Intel® PTT support in TPM2.0 profile. **Background:** Intel® PTT will support the TPM2.0 PC Client command Profile, ECC-DSA algorithm agility and SHA2-PCRs on Intel® ME10 FW, running on Broadwell HW.	10.0.20.1156
CCG0100010195	**Description:** Enable OOB Remote Monitor Screen Blanking (ORMSB) for an Intel® AMT enabled devices. **Background:** System managers of public unattended systems (e.g. digital signage devices, ATMs, etc.) require in cases such as crashes, maintenance, and healing sessions to hide display from public view while system keeps running.	10.0.20.1156
CCG0100010832	**Description:** Add an option to program the FQDN and PKI suffix through FOV interface. **Background:** Calls out for requirement to add FOV variables for FQDN and PKI suffix in the factory. The FQDN and PKI suffix FOVs to be added are to help end customers provision in ACM mode for Wireless LAN only Intel® vPro platforms to prevent additional manual steps.	10.0.20.1156
CCG0100010625	**Description:** Allow FQDN & PKI DNS Suffix Programming in Favor of Admin Control Mode provisioning on LAN-less Platforms. **Background:** Allows Intel® Vpro™ provisioning via Host Based Configuration in Administrator Control Mode (ACM) when secure FQDN is programed (via FITC, Intel® MEBX or USB).	10.0.20.1156
CCG0100010639	**Description:** AMT SMI client over Intel® MEI2 will be removal. **Background:**	10.0.20.1156

RCR #	Description / Background	Build
	Intel® ME supports special Intel® AMT SMI client over MEI2. Original target was receiving host alerts and logging alerting events.	
CCG0100010643	**Description:** The version of HDCP used by Intel® WiDi has been updated to version 2.2 **Background:** Intel® WiDi uses HDCP to stream protected content over the Intel® WiDi link.	10.0.20.1156
CCG0100010501	**Description:** Adding Remote Wake Capability into Intel® ME10 and Enable it by Default. **Background:** Remote Wake is one of the features of Intel® Smart Connect technology and can work over wired LAN (a.k.a. LAN) or wireless LAN (a.k.a. WLAN). In the Shark Bay ULT platform, Remote Wake over LAN was not supported but in Intel® ME10, Remote Wake will be supported over LAN (on non Connected Standby platforms) as well as WLAN (Targeting mostly All In One designs) Remote Wake will be enabled by default.	10.0.20.1156
CCG0100010434	**Description:** Windows* 8.1 Validation Requirements for Intel® ME FW 10. **Background:** Adds support for Windows* 8.1.	10.0.20.1156
CCG0100010402	**Description:** Support all mobile DeepSx on AC power states which do not require M3 operation. **Background:** Currently DeepSx is supported for Mobile platform in DC mode and Desktop platform in AC mode. Request adds validation coverage to support DeepSx for mobile platform in AC mode.	10.0.20.1156
CCG0100010397	**Description:** Reboot Request after Intel® AMT Provisioning. **Background:** Intel® ME Power Gating is supported in the 5MB SKU of Intel® ME10. In order to allow Intel® ME to enter power gating (PG), the SOL device is not exposed to the OS, while Intel® AMT is not provisioned. As a result, SOL device is unavailable immediately after provisioning, until the machine reboots After Intel® AMT provisioning, IMSS will notify the user that the machine needs to be rebooted due to a configuration change that was initiated by the system administrator. The user will be given the option to choose reboot now or, defer the reboot. If the user chooses reboot now, the IMSS will initiate a reboot. All strings will be localized.	10.0.20.1156

RCR #	Description / Background	Build
CCG0100010327	**Description:** Remove Configuration Tools from FW Kit. **Background:** Remove the Configuration Tools folder, and all its contents, from the Intel® ME 5MB FW kits. The USBFile.exe tool, which is in a sub-folder of the Configuration Server, is moved to the UdpParam tool folder.	10.0.20.1156
CCG0100010284	**Description:** Restore ~Graceful RCO `Ability during Windows* Connected Standby state. **Background:** Intel® AMT will be supported in Windows* Connected Standby (CS) state in Intel® ME10 (on BDW platform). Intel® AMT supports Legacy RCO (Remote Control Operation) and has the ability to make a remote power operations such as shutdown, reset, power on, etc. Intel® AMT supports next graceful RCOs: shutdown, reset, sleep & hibernate Intel® AMT will support the above RCOs while the system is in CS state.	10.0.20.1156
CCG0100010592	**Description:** Remove EOM checkbox and tag in FITC/FIT and FPT commands for setting mfg done bit. **Background:** A few generations ago Intel combined setting the "mfg done" bit ("fpt -u -n globallocked -v 0x1") and flash access permission to Intel recommended values ("fpt -lock") into "fpt -closemnf". Moreover "fpt –dumplock" displayed the current lock settings read from the descriptor region and was replaced with "fpt –i". Removing the fpt –lock and fpt –dumplock and checkbox in FITC will remove redundancy, confusion about their difference and erroneous configurations.	10.0.0.1042
CCG0100010711	**Description:** Re-enable FITC to choose load series resistance for LPC Clocks for Intel® ME 10 platforms. **Background:** The LPC Clock setting parameter within FITC under ME Region->Integrated Clock Controller->Profile allows customers to control LPC Clock settings (single load (25 ohm) vs. double load series resistance (17 ohm)). In Intel® ME 9.5 Beta and later releases, the FITC tool parameter for double load was removed leaving single load as the only option.	10.0.0.1012

RCR #	Description / Background	Build
CCG0100010225	**Description:** Implementation of a UDP interface for Intel® RWT. **Background:** Along with support for sending Keep Alive packets over a TCP session, this change adds support for sending Keep Alive packets encapsulated in UDP packets. The Intel® RWT agent will determine the best suited protocol for the network, namely TCP or UDP and instruct the Intel® ME to send Keep Alive packets of the appropriate format.	10.0.0.1012
CCG0100010208	**Description:** A field in WS-Event has been added that when CILA is triggered, identifies the originating system and how or why it was generated at generation time. **Background:** ISV solutions dependent upon the CILA and CIRA WS-Eventing alerts were not scalable because there were no means to identify the hostname of the originating system or how or why a CILA alert was generated.	10.0.0.1012
CCG0100010128	**Description:** Legacy AMTHI commands removed in Intel® ME 10. **Background:** AMTHI commands marked as deprecated have been removed to reduce FW code.	10.0.0.1012

§