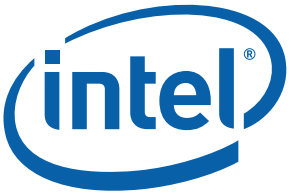


Broadwell PCH-LP - Intel® Management Engine Firmware 10.0

1.5MB Firmware Bring Up Guide

June 2014

Revision 1.0 - Release

Intel Confidential

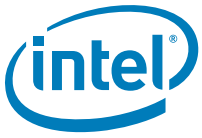
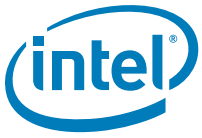
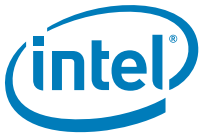


Table of Contents



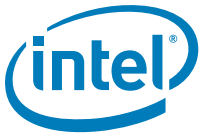


Figures

Tables

Revision History

10.0.0.1042	Alpha Release: See change bars on the left side of the page.	December 2013
10.0.20.1156	Beta Release: See change bars on the left side of the page.	March 2014
10.0.20.1258	PC Release: See change bars on the left side of the page.	May 2014
1.0	Final Release: See change bars on the left side of the page.	June 2014



1 Introduction

This document covers the Intel® Management Engine Firmware (Intel® ME) 10.0 - 1.5MB SKU Firmware bring up procedure. Intel® ME is tied to essential platform functionality — this dependency cannot be avoided for engineering reasons.

The bring up procedure primarily involves building a Serial Peripheral Interface (SPI) Flash image that will contain:

- **[required]** Descriptor region — Contains sizing information for all other SPI Flash image regions, SPI settings (including Vendor Specific Configuration - or VSCC - tables, SPI device parameters), and region access permissions.
- **[required]** BIOS region — Contains firmware for the processor (or host) and/or Embedded Controller (EC).
- **[required]** Intel® ME FW region — Contains firmware for the Intel® Management Engine.
- **[optional]** GbE region — Contains firmware for Intel LAN solution.

For more details on SPI Flash layout, see the document **PCH-LP SPI Programming Guide** and Appendix A. Once the SPI Flash image is built, it will be programmed to the target based platform and the platform will be booted. This document also covers any tests and checks required to ensure that this boot process is successful and that Intel® ME 1.5MB FW is operating as expected.

1.1 Intel® ME FW Features

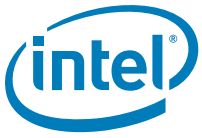
This firmware release includes the following applications:

- Platform Clocks – Tune clock silicon to the parameters of a specific board, configure clocks at run time, and power management clocks. **Benefit:** Allows extensive customizability and soft control of “Third generation” clock solution and makes clocks available before CPU powers up.
- Silicon Workaround Capability – Intel® ME FW will have limited capabilities to perform targeted workarounds for silicon issues. **Benefit:** Allows Intel® ME FW to address some issues that otherwise would require a new silicon stepping.
- Thermal Reporting – Intel® ME FW has the ability to collect platform thermal data and provide that data to embedded controllers and super I/O devices over SMLINK1 as well as in memory map I/O space.

1.2 Prerequisites

Before this document is read and utilized, it is essential that the reader first review the 1.5MB FW Release Notes (included with this Intel® ME 1.5MB FW kit).

This document is constructed so that the reader can complete the bring up steps as given for the Intel Customer Reference Board (CRB). However, in the case that bring up is being performed on a different based platform, this document will highlight any changes that must be imposed onto the bring up steps accordingly.



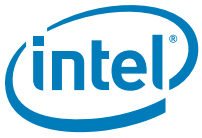
This document makes only the following limited assumptions regarding hardware:

- The platform is based
- The platform is equipped with one or more SPI Flash devices with a total capacity sufficient for storing all relevant firmware images.

1.3 Acronyms and Definitions

1.3.1 General

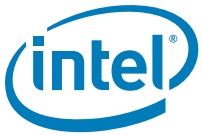
Acronym or Term	Definition
API	Application Programming Interface
ASCII	American Standard Code for Information Interchange
BIOS	Basic Input Output System
DIMM	Dual In-line Memory Module
DLL	Dynamic Link Library
DMI	Direct Media Interface
EC	Embedded Controller
EEPROM	Electrically Erasable Programmable Read Only Memory
FDI	Flexible Display Interface
FPF	Field Programmable Fuses
FW	Firmware
GbE	Gigabit Ethernet
HECI	Host Embedded Controller Interface (aka Intel® MEI)
IBV	Independent BIOS Vendor
ID	Identification
Intel® ICCS	Intel® Integrated Clock Controller Service
Intel® ME	Intel® Management Engine (Intel®ME)
Intel® MEI	Intel® Management Engine Interface (Intel® MEI) (renamed from HECI)
Intel® IPT	Intel® Identity Protection Technology (Intel® IPT)
Intel® PTT	Intel® Platform Trusted Technology (Intel® PPT)
Intel® MSS	Intel® Management and Security Status Application
ISV	Independent Software Vendor
JTAG	Joint Test Action Group
KVM	Keyboard, Video, Mouse
LAN	Local Area Network
LED	Light Emitting Diode
MCP	Multi-Chip Package (Central Processing Unit / Platform Controller Hub)
NVM	Non-Volatile Memory
NVRAM	Non-Volatile Random Access Memory
OOB	Out-of-Band
OS	Operating System
PAVP	Protected Audio and Video Path
PCI	Peripheral Component Interconnect



Acronym or Term	Definition
PCIe*	Peripheral Component Interconnect Express
PHY	Physical Layer (Networking)
PRTC	Protected Real Time Clock
RNG	Random Number Generator
RSA	RSA is a public key encryption method
RTC	Real Time Clock
SBA	Intel® Small Business Advantage
SDK	Software Development Kit
SHA	Secure Hash Algorithm
SMBus	System Management Bus
SPI Flash	Serial Peripheral Interface Flash
TCP/IP	Transmission Control Protocol / Internet Protocol
TPM	Trusted Platform Module
UI	User Interface
UNS	User Notification Service
VSCC	Vendor Specific Configuration
WMI	Windows Management Instrumentation

1.3.2 Intel® Management Engine

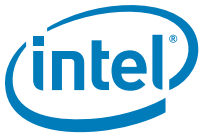
Acronym or Term	Definition
3PDS	3rd Party Data Storage
Agent	Software that runs on a client PC with OS running
Intel® AT	Intel® Anti-Theft Technology (Intel® AT)
End User	The person who uses the computer (either Desktop or Mobile). In corporate, the user usually does not have an administrator privileges.
Host or Host CPU	The processor that is running the operating system. This is different than the management processor running the Intel® Management Engine Firmware.
Host Service/Application	An application that is running on the host CPU
INF	An information file (.inf) used by Microsoft* operating systems that supports the Plug & Play feature. When installing a driver, this file provides the OS the necessary information about driver filenames, driver components, and supported hardware.
Intel® Management Engine Interface (Intel® MEI)	Interface between the Management Engine and the Host system
Intel® MEI driver	Intel® ME host driver that runs on the host and interfaces between ISV Agents and the Intel® ME HW.
IT User	Information Technology User. Typically very technical and uses a management console to ensure multiple PCs on a network function.
LMS	Local Management Service: A SW application which runs on the host machine and provide a secured communication between the ISV agent and the Intel® Management Engine Firmware.
Intel® ME	Intel® Management Engine: The embedded processor residing in the chipset MCP
MECI	ME-VE Communication Interface



Acronym or Term	Definition
NVM	Non-Volatile Memory: A type of memory that will retain its contents even if power is removed.
OOB Interface	Out Of Band interface: This is WSMAN interface over secure or non-secure TCP protocol.
OS not Functional	The Host OS is considered non-functional in Sx power state and any one of the following cases when system is in S0 power state: • OS is hung • After PCI reset • OS watch dog expires • OS is not present
System States	Operating System power states such as S0. See detailed definitions in System States and Power Management section.
UIM	User Identifiable Mark

1.3.3 System States and Power Management

Acronym or Term	Definition
G3	A system state of Mechanical Off where all power is disconnected from the system. G3 power state does not necessarily indicate that RTC power is removed.
M0	Intel® Management Engine power state where all HW power planes are activated. The host power state is S0.
M3	Intel® Management Engine power state where all HW power planes are activated however the host power state is different than S0 (Some host power planes are not activated). Host PCIe* interface are unavailable to the host software. Main memory is not available for Intel® Management Engine use.
M-Off	No power is applied to the management processor subsystem. Intel® Management Engine is not operating.
OS Hibernate	System state where the OS state is saved on the hard drive.
S0	A system state where power is applied to all HW devices and the system is running normally.
S1, S2, S3	A system state where the host CPU is halted but power remains available to the memory system (memory is in self-refresh mode).
S4	A system state where the host CPU and memory are not active.
S5	A system state where all power to the host system is off, however the power cord (and/or battery in mobile designs) is still connected.
Shut Down	Equivalent to the S5 state.
Snooze Mode	Intel® Management Engine activities are mostly suspended to save power. The Intel® Management Engine monitors HW activities and can restore its activities depending on the HW event.
Standby	System state where the OS state is saved in memory and resumed from the memory when mouse/keyboard is clicked.
Sx	All S states which are different than S0.



1.4 Reference Documents

Document	Doc Number / Location*
Shark Bay ULT CRB– Platform Design Guide	TBD / IBL
Intel® Management Engine (Intel® ME) and Embedded Controller Interaction for Shark Bay ULT Platform	471984 / IBL
RS – Intel® Management Engine BIOS Writers Guide	TBD / *
[Shark Bay] Platforms - Intel® Management Engine (Intel® ME) 10.0 - 1.5 MB SKU Firmware for Lynx Point-LP - Compliancy and Testing Guide -Rev. 0.8	xxxxxx / CDI
Intel® 82576 and 82579 Gigabit Ethernet Controllers – Intel Software Support for Cisco's MACsec Protocol Supplicant – 10-Dec-2010	xxxxxx / IBL

Note: * Unless specified otherwise, a document can be ordered by providing its reference number to your Intel Field Applications Engineer.

1.5 Format and Notation

The formats and notations used within this document model are those typically used by BIOS vendors. This section describes the formatting and the notations that will be followed in this document.

Table 1-1. Number Format Notation

Number Format	Notation	Example
Decimal (default)	d	14d. Note that any number without an explicit suffix can be assumed to be decimal.
Binary	b	1110b
Hex	h	0Eh
Hex	0x	0x0E

Table 1-2. Data Format Notation

Data Type	Notation	Size
Bit	b	Smallest unit, 0 or 1
Byte	B	8 bits
Word	W	16 bits or 2 bytes
Double-word	DW	32 bits or 4 bytes
Quad-word	QW	8 bytes or 4 words
Kilobyte	KB	1024 bytes
Megabit	Mb	1,048,576 bits or 128 KB
Megabyte	MB	1,048,576 bytes or 1024 KB
Gigabit	Gb	1,073,741,824 bits
Gigabyte	GB	1024 MB

1.6 Kit Contents

The Intel® ME 1.5MB FW kit can be downloaded from VIP (https://platformsw.intel.com/). The contents of this kit are detailed below (Note that only key files are listed).

Table 1-3. Kit Contents (Sheet 1 of 3)

File or [Directory]	Content Description
[root]	Root directory
1.5MB FW Bring Up Guide.pdf	This document
Mobile 4th Generation Intel® Core™ Processor (U-Series) Platform I/O PCH-LP SPI Programming Guide.pdf	How to program SPI device parameters, VSCC tables, descriptor region details. Also contains a complete SPI Flash softstrap reference.
[Image Components]	
[BIOS]	
BDW_MP2_PV_ECP_79_acm2975_PreprodSigned_Release.rom **BDW_MP2_PV_ECP_79_acm2975_ProdSigned_Release.rom**	BIOS image only for Intel CRB. This BIOS image works for ULT mobile CRBs. **For other Broadwell PCH-LP platforms, a custom BIOS image will be required.**
[GbE]	
NAHUM6_LP_CLARKVILLE_ULT_6.bin	Intel® LAN PHY LPT-LP firmware image.
NAHUM6_WPT_0_2.bin	Intel® LAN PHY WPT firmware image. T
[ME]	
ME10.0_1.5M_PreProduction_Rom_Bypass.bin	Intel® ME firmware image (**Non Production FW Rom Bypass**) - supports **unfused** Broadwell PCH-LP Platform I/O MCP steppings: • Unfused (Super SKU) **Note: For PAVP Testing**, you must match Production FW with Production Part and Non Production FW with Non Production Parts.
ME10.0_1.5M_PreProduction.bin	Intel® ME firmware image (**Non Production FW**) - supports **unfused** Broadwell PCH-LP Platform I/O MCP steppings: • Fused (Pre-QS and QS) **Note: For PAVP Testing**, you must match Production FW with Production Part and Non Production FW with Non Production Parts.
ME10.0_1.5M_Production.bin	Intel® ME firmware image (**Production FW**) - supports **fused** Broadwell PCH-LP Platform I/O MCP steppings: • Fused (Pre-QS and QS) **Note: For PAVP Testing**, you must match Production FW with Production Part and Non Production FW with Non Production Parts.

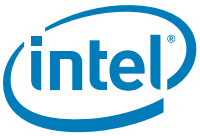


Table 1-3. Kit Contents (Sheet 2 of 3)

File or [Directory]	Content Description
ME10.0_1.5M_PreProduction.bin	Intel® ME firmware image (**Non Production FW**) - supports **unfused** Broadwell PCH-LP Platform I/O MCP steppings: • Unfused (Super SKU) **Note: For PAVP Testing**, you must match Production FW with Production Part and Non Production FW with Non Production Parts.
[Installers]	
Intel(R)_ME_SW_Installation_Guide_WPT_10.pdf	Intel® ME Software installation Guide.
[ME_SW_MSI]	
SetupME.exe	Install executable MSI installer of Intel® ME Drivers for Windows* OS for Pre-Production MCPs. See readme.txt for more information.
[Tools]	
[ICC_Tools]	
[CCT]	
DOS	
cct.exe	Clock Control Tool (CCT)
EFI	
cct.efi	CCT for EFI
Windows	
cct.ini	Configuration file for CCT
cctWin.exe	CCT for Windows*
[System Tools]	
[Flash Image Tool]	
fitc.exe	Flash Image Tool (FITC)
fitc.ini	Configuration file for FITC
newfiletmpl.xml	FITC Configuration XML file
vsccommn.bin	Binary containing the supported SPI parts
[Flash Programming Tool]	
[DOS]	
fparts.txt	List of supported SPI Flash devices with specific Flash parameters
fpt.exe	Flash Programming Tool (FPT) for DOS
[EFI]	
fparts.txt	List of supported SPI Flash devices with specific Flash parameters
fpt.efi	Flash Programming Tool (FPT) for EFI
[Windows]	
fparts.txt	List of supported SPI Flash devices with specific Flash parameters
fptw.exe	Flash Programming Tool (FPT) for Windows*
[Windows64]	

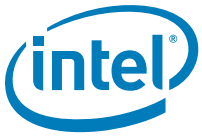


Table 1-3. Kit Contents (Sheet 3 of 3)

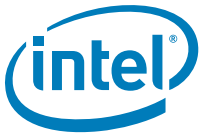
File or [Directory]	Content Description
fparts.txt	List of supported SPI Flash devices with specific Flash parameters
fptw64.exe	Flash Programming Tool (FPT) for Windows* (64-bit) OS
[FWUpdate]	
[EFI]	
FWUpdLcl.efi	FW Update Tool (EFI version)
[Local-DOS]	
FWUpdLcl.exe	FW Update Tool (DOS version)
[Local-Win]	
FWUpdLcl.exe	FW Update Tool (Windows* version 32bit)
[Local-Win64]	
FWUpdLcl64.exe	FW Update Tool (Windows* version 64bit)
[MEInfo]	
[DOS]	
MEInfo.exe	Intel®ME Information Tool (DOS version)
[EFI]	
MEInfo.efi	Intel®ME Information Tool (EFI version)
[Windows]	
MEInfoWin.exe	Intel®ME Information Tool (Windows* version 32bit)
[Windows64]	
MEInfoWin64.exe	Intel®ME Information Tool (Windows* version 64bit)
[MEManuf]	
[DOS]	
MEManuf.cfg	Intel®ME Manufacturing Tool config file
MEManuf.exe	Intel®ME Manufacturing Tool (DOS version)
vsccommn.bin	Binary containing the supported SPI parts
[EFI]	
MEManuf.cfg	Intel®ME Manufacturing Tool config file
MEManuf.efi	Intel®ME Manufacturing Tool (EFI version)
vsccommn.bin	Binary containing the supported SPI parts
[Windows]	
MEManuf.cfg	Intel®ME Manufacturing Tool config file
MEManufWin.exe	Intel®ME Manufacturing Tool (Windows* version 32bit)
vsccommn.bin	Binary containing the supported SPI parts
[Windows64]	
MEManuf.cfg	Intel®ME Manufacturing Tool config file
MEManufWin64.exe	Intel®ME Manufacturing Tool (Windows* version 64bit)
vsccommn.bin	Binary containing the supported SPI parts

1.7 External Hardware Requirements for Bring Up

Acquire the following hardware tools before moving on to the next step.

Windows* OS System	Flash Burner	DOS Bootable USB Key
		
Equipment: • Laptop or desktop that supports win32 applications **Purpose:** • Will run firmware image assembly and build process software.	**Equipment:** • (Optional) For platforms that don't boot, a Flash Chip Programmer will be required • For platforms that can boot to DOS or Windows*, a Flash Programming Tool (FPT) is provided in this kit **Purpose:** • Will burn firmware images onto the target system Flash device(s).	**Equipment:** • A DOS Bootable USB Key (Size > 512 MB) **Purpose:** • Acting as a bootable device and will be used to run Flash Programming Tool (fpt.exe) directly on the system that is undergoing Bring Up process. • Or will be used to transfer a firmware image onto a Flash burner.

§ §



2 Image Creation: Flash Image Tool (FITC)

Flash Image Tool (FITC) will be used to generate a full SPI Flash binary image with Descriptor, GbE, BIOS, and Intel® ME Regions. Use the steps shown in following sections.

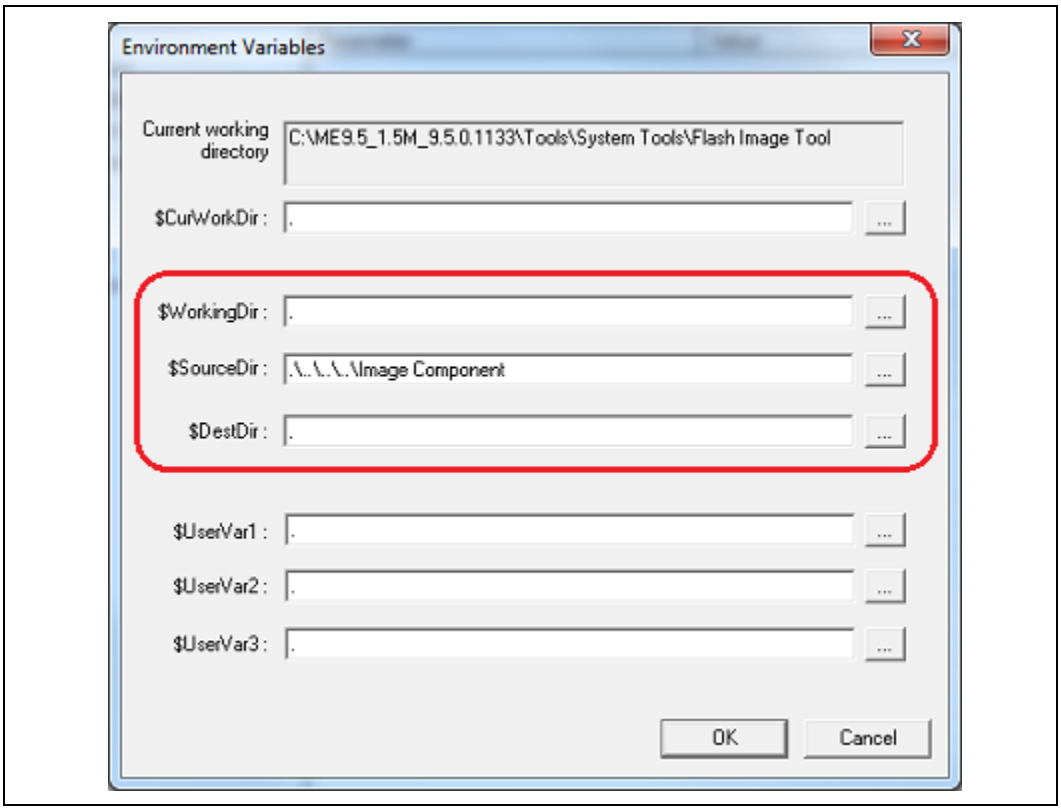
Note: The FITC Tool may be updated throughout the release cycles. As a general rule, please ensure you use the tools, images and other content from the same kit and refrain from using different version tools.

After this SPI Flash image is created, it will need to be burned onto the target platform's SPI Flash device(s). Section 3, "Programming SPI Flash Devices and Checking Firmware Status" later in this document provides steps to do this.

2.1 Start FITC and Set Up The Build Environment

1. Invoke Flash Image Tool. Using Explorer*, navigate to **[root]\Tools\System Tools\Flash Image Tool**. Ensure that FITC's directory contents are intact (see Section 1.6). Double-click **fitc.exe**.
2. In the main menu select **Build | Environment Variables…**. Edit your configuration as shown below. Note that in the example, **[root]\Tools\System Tools\Flash Image Tool** is **"."**.
   - Keep the Working Directory $WorkingDir as "."
   - Source Directory $SourceDir is where FITC will look to find binary images during the image creation process, change $SourceDir to ".\..\..\..\Image Components"
   - Destination Directory $DestDir is where FITC will save the SPI Flash binary image, keep $DestDir as "."

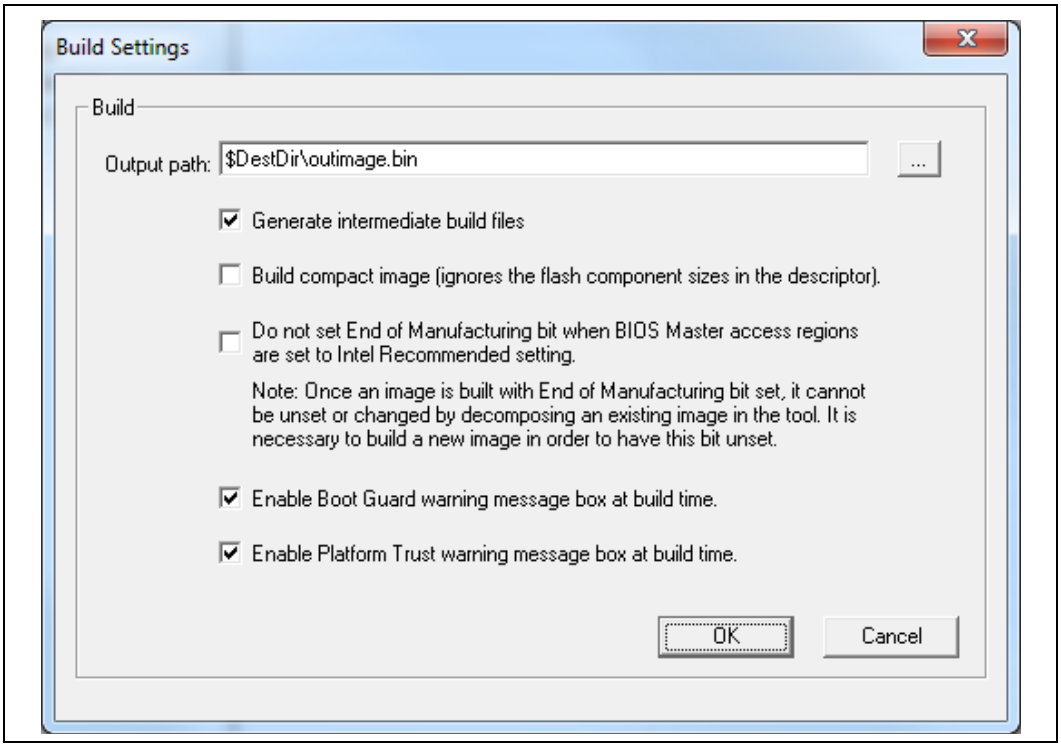
Figure 2-1. Build | Environment Variables



3. Click **OK** to apply your changes.

4. In the main menu select **Build | Build Settings…**. Leave the defaults for **Output path, Generate intermediate build files, and Build compact image** as shown. Click **OK** to apply your changes.

Figure 2-2. Build | Build Settings…

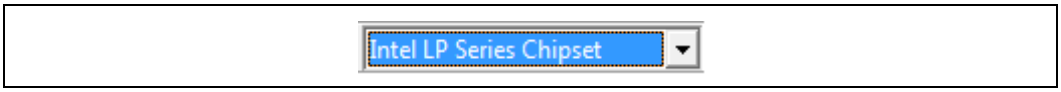


5. In the main menu select **File | Open…**. In the Open dialog that appears navigate to **[root]\Tools\System Tools\Flash Image Tool**. Click on **newfiletmpl.xml** and click **OK**.

2.2 Configure MCP Silicon Stepping

Leave the **MCP Silicon Stepping Combo Box** at its default value of **Intel® LP Series Chipset**.

Figure 2-3. MCP Silicon Stepping Combo Box



2.3 Set Up SPI Flash Regions

Table 2-1. Flash Image | PDR Region

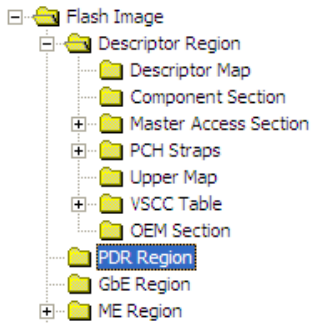
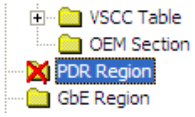
Location	Parameter	CRB Set To	Settings for Any Platform
Follow navigation tree below: • Select the Flash Image • Select **Flash Image | PDR Region** • Set the parameters in the **PDR Region** section as shown 	PDR Region Length	PDR Region is disabled	Displays Region size information when **Binary input file** is specified.
	Binary Input File	PDR Region is disabled	Load a Platform Data Region binary if required and available.
...or if NOT using Platform Data Region (PDR)			
A red "X" will indicate whether this Region is disabled. If this Region is not disabled, disable it by right-clicking on **Flash Image | PDR Region** and selecting **Disable Region**.			

Table 2-2. Flash Image | GbE Region

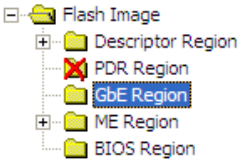
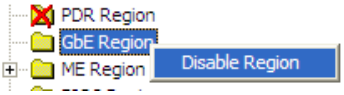
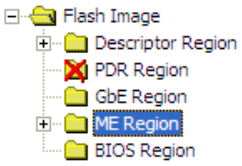
Location	Parameter	CRB Set To	Settings for Any Platform
Follow navigation tree below: • Select the Flash Image • Select **Flash Image | GbE Region** • Set the parameters in the **GbE Region** section as shown 	**Yellow means custom settings may be required.**		
	GbE LAN region length	0x00000000	Note: This value will be field automatically populated by FITc during image build.
	Binary input file	Navigate to your **Source Directory** (as specified in Section 2.1) and switch to the **GbE** subdirectory. Choose the appropriate Intel GbE LAN Firmware binary image. **If not using Intel LAN then leave this parameter blank.**	
	Intel® Integrated LAN Enable	false	This field only is editable after an Intel integrated LAN image is loaded. If not planning to validate Intel LAN on target platform, or for debug reasons, set to **false**.
	Major Version	0	Displays major revision value for Intel LAN GbE FW version when **Binary input file** is specified.
	Minor Version	0	Displays minor revision value for Intel LAN GbE FW version when **Binary input file** is specified.
	Image ID	0	Displays image ID value for Intel LAN GbE FW version when **Binary input file** is specified.
...or if not using Intel wired LAN device			
A red "X" will indicate whether this Region is disabled. If this Region is not disabled, disable it by right-clicking on **Flash Image | GbE Region** and selecting **Disable Region**.			

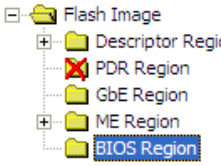
Table 2-3. Flash Image | ME Region

Location	Parameter	CRB Set To	Settings for Any Platform
Follow navigation tree below: • Select the Flash Image tab • Select **Flash Image | ME Region** • Set the parameters in the **ME Region** section as shown • **Note:** Loading an ME FW binary image that contains ME ROM Bypass unlocks the **ME Boot from Flash** parameter in **Flash Image | Descriptor Region | PCH Straps | PCH Strap 10** 	**Yellow means custom settings may be required, otherwise use CRB setting.**		
	Binary input file	Navigate to your **Source Directory** (as specified in Section 2.1) and switch to the **Firmware** subdirectory. Choose the Intel® ME FW binary image. ***Note:*** You may choose to build the Intel® ME Region only. To do so, **Flash Image | Descriptor Region | Descriptor Map** parameter **Number of Flash components** must be set to **0**. ***Note:*** Loading an Intel® ME FW binary image that contains ME ROM Bypass unlocks the **ME Boot from Flash** parameter in **Flash Image | Descriptor Region | PCH Straps | PCH Strap 10**.	
	WCOD Id	0x08B1 WILKINS	Determines which WLAN micro code will be supported in the firmware image
	LOCL Id	0x01 EN	Determines which localized language data will be used by firmware for secure output screens (Examples: SOL / KVM)
	* Partition Rom Bypass Enabled		Not a parameter. This information panel appears when an ME FW image enables ME boot directly from Flash.
	Major Version	0	Displays major revision value for ME FW version when **Binary input file** is specified.
	Minor Version	0	Displays minor revision value for ME FW version when **Binary input file** is specified.
	Hotfix Version	0	Displays hotfix value for ME FW version when **Binary input file** is specified.
	Build Version	0	Displays build value for ME FW version when **Binary input file** is specified.

Note: Starting with Intel® ME 8.0, the FW image provided in the kits includes additional code partitions which are used by both full and partial FW update mechanisms as a result of these changes the image is larger than FW images from previous generations. In addition to this change the FW image in the kits will be used for generating full image binaries using FITc and full or partial FW updates using FWUpdIcl.

Customers will not be able to write the image provided in the kits directly to flash. The image must be loaded into FITc tool then built in order to create a working ME region.

Table 2-4. Flash Image | BIOS Region

Location	Parameter	CRB Set To	Settings for Any Platform
Follow navigation tree below: • Select the Flash Image tab • Select **Flash Image | BIOS Region** • Set the parameters in the **BIOS Region** section as shown 	**Yellow means custom settings may be required, otherwise use CRB setting.**		
	BIOS region length	0x00000000	This field allows user to allocate a specific size in the SPI Flash for the BIOS image. If set to 0, FITC will automatically set the size based on the BIOS image.
	Binary input file	For the Intel CRB navigate to your **Source Directory** (as specified in Section 2.1) and switch to the **BIOS** subdirectory. Choose the BIOS binary image.	For all other platforms point this parameter to the appropriate BIOS image. If BIOS is stored in a separate SPI Flash device or in FWH (see Configurations "B", "C", and "D" in Appendix A) then leave this parameter blank.

2.4 Set Up Descriptor and SPI Flash Device(s)

Table 2-5. Flash Image | Descriptor Region

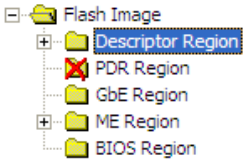
Location	Parameter	CRB Set To	Settings for Any Platform
Follow navigation tree below: • Select the **Flash Image** tab. Select **Flash Image | Descriptor Region** • Set the parameters in the **Descriptor Region** section as shown 	**Yellow means custom settings may be required, otherwise use CRB setting.**		
	Descriptor region length	0x00000000	Leave this at zero. Allows FITC to auto-size the descriptor region length.

Table 2-6. Flash Image | Descriptor Region | Descriptor Map

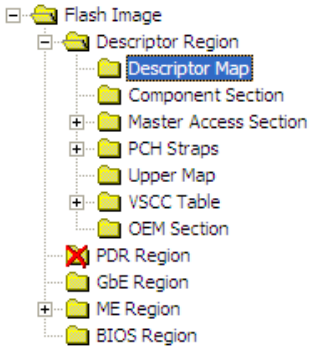
Location	Parameter	CRB Set To	Settings for Any Platform
Follow navigation tree below: • Select the **Flash Image** tab • Select **Flash Image | Descriptor Region | Descriptor Map** • Set the parameters in the **Descriptor Map** section as shown 	**Yellow means custom settings may be required, otherwise use CRB setting.**		
	Region base address	0x04	Read Only, See SPI programming Guide for details.
	Number of Flash components	2	Number of SPI Flash devices on the platform **1** or **2** = Total SPI Flash devices **0** = Build ME region only ***Note:*** The number of Flash components is dependent on the platform design.
	Component base address	0x03	Read Only, See SPI programming Guide for details.
	Number of PCH straps	21	Read Only, See SPI programming Guide for details.
	PCH straps base address	0x10	Read Only, See SPI programming Guide for details.
	Number of Masters	2	Read Only, See SPI programming Guide for details.
	Master base address	0x06	Read Only, See SPI programming Guide for details.
	Number of PROC straps	1	Read Only, See SPI programming Guide for details.
	PROC straps base address	0x20	Read Only, See SPI programming Guide for details.

Table 2-7. Flash Image | Descriptor Region | Component Section

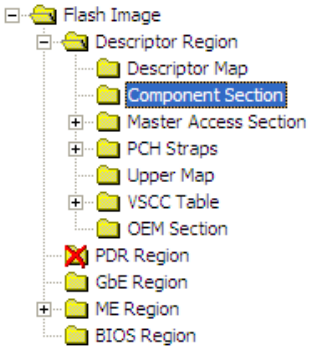
Location	Parameter	CRB Set To	Settings for Any Platform
Follow navigation tree below: • Select the **Flash Image** tab. Select F**lash Image | Descriptor Region | Component Section** • Set the parameters in the **Component Section** section as shown 	**Yellow means custom settings may be required, otherwise use CRB setting.**		
	Read ID and Read Status clock frequency	50MHz	Lowest common frequency of all SPI Flash parts on the platform.
	Write and erase clock frequency	50MHz	Lowest common frequency of all SPI Flash parts on the platform.
	Fast read clock frequency	50MHz	In order for MCP HW to override its own internal default value (20 MHz), **Fast read support** must be set To **true**.
	Fast read support	true	**true** = Enables opcode 0Bh opcode on a read. This allows for faster read frequencies on serial flash by having a single dummy byte before valid data is output from the flash.
	Read clock frequency	20MHz	Treat as reserved.
	Flash component 2 density	8MB	Size of second SPI Flash part on the platform. ***Note:*** This value will be grayed out if the number of SPI Flash components is set to 1 in the Descriptor Map options.
	Flash component 1 density	8MB	Size of first SPI Flash part on the platform.
	Dual Output Fast Read Support	true	This field enables the opcode 3Bh to use Single Input Dual Output Fast Read. This speeds up the fast read throughput of the serial flash part. ***Note:*** This should only be set to 'true' if all Serial Flash parts support the 3Bh command. See *4th Gen Intel Core Processor U-Series SPI Programming Guide* for more details.
	Invalid instruction 0	0	Opcode entered here will not be allowed by the MCP's SPI controller for HW sequencing. See 4th Gen Intel Core Processor U-Series SPI Programming Guide for more details. **0** = no instruction is specified
	Invalid instruction 1	0	
	Invalid instruction 2	0	
	Invalid instruction 3	0	
	Invalid instruction 4	0	
	Invalid instruction 5	0	
	Invalid instruction 6	0	
	Invalid instruction 7	0	

Table 2-8. Flash Image | Descriptor Region | Master Access Section | CPU/BIOS

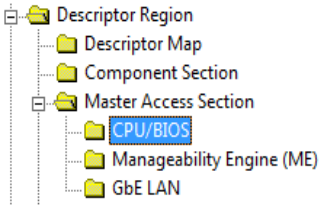
Location	Parameter	CRB Set To	Settings for Any Platform
Follow navigation tree below: • Select the **Flash Image** tab • Select **Flash Image | Descriptor Region | Master Access Section | CPU/BIOS** • Set the parameters in the **CPU/BIOS** section as shown 	**Yellow means custom settings may be required.**		
	PCI Bus ID	0	Treat as reserved.
	PCI Device ID	0	Treat as reserved.
	PCI Function ID	0	Treat as reserved.
	Read Access	0xFF	Controls read access by BIOS to: • Bit 0: Descriptor (region 0) • Bit 1: BIOS region (region 1) • Bit 2: ME FW region (region 2) • Bit 3: GbE FW region (region 3) • Bit 4: PDR Region (region 4) • Bits 5-7: Regions 5 through 7 **0x0B** = Production platform **0xFF (default)** = Non-production/debug platform
	Write Access	0xFF	Controls write access by BIOS. Structure is identical to **Read access** parameter. **0x0A** = Production platform **0xFF (default)** = Non-production/debug platform

Table 2-9. Flash Image | Descriptor Region | Master Access Section | Manageability Engine (ME)

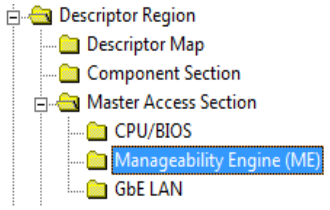
Location	Parameter	CRB Set To	Settings for target platform
Follow navigation tree below: • Select the **Flash Image** tab • Select **Flash Image | Descriptor Region | Master Access Section | Manageability Engine (ME)** • Set the parameters in the **Manageability Engine (ME)** section as shown 	**Yellow means custom settings may be required.**		
	PCI Bus ID	0	Treat as reserved.
	PCI Device ID	0	Treat as reserved.
	PCI Function ID	0	Treat as reserved.
	Read access	0xFF	Controls read access by ME to: • Bit 0: Descriptor (region 0) • Bit 1: BIOS region (region 1) • Bit 2: ME FW region (region 2) • Bit 3: GbE FW region (region 3) • Bit 4: PDR Region (region 4) • Bits 5-7: Regions 5 through 7 **0x0D** = Production platform **0xFF (default)** = Non-production/debug platform
	Write access	0xFF	Controls write access by ME FW. Structure is identical to **Read access** parameter. **0x0C** = Production platform **0xFF (default)** = Non-production/debug platform

Table 2-10. Flash Image | Descriptor Region | Master Access Section | GbE LAN

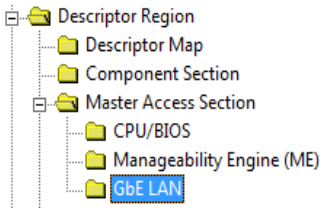
Location	Parameter	CRB Set To	Settings for Any Platform
Follow navigation tree below: • Select the **Flash Image** tab • Select **Flash Image | Descriptor Region | Master Access Section | GbE LAN** • Set the parameters in the **GbE LAN** section as shown 	**Yellow means custom settings may be required.**		
	PCI Bus ID	1	Treat as reserved.
	PCI Device ID	3	Treat as reserved.
	PCI Function ID	0	Treat as reserved.
	Read access	0xFF	Controls read access by GbE FW to: • Bit 0: Descriptor (region 0) • Bit 1: BIOS region (region 1) • Bit 2: ME FW region (region 2) • Bit 3: GbE FW region (region 3) • Bit 4: PDR Region (region 4) • Bits 5-7: Regions 5 through 7 **0x08** = Production platform **0xFF (default)** = Non-production/debug platform
	Write access	0xFF	Controls write access by GbE FW. Structure is identical to **Read access** parameter. **0x08** = Production platform **0xFF (default)** = Non-production/debug platform

Table 2-11. Flash Image | Descriptor Region | VSCC Table | W25Q64BV (example)

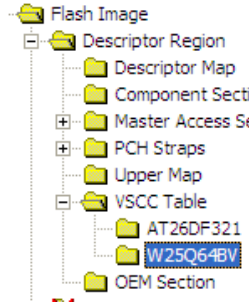
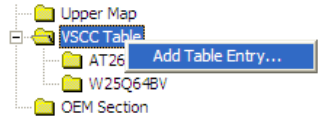
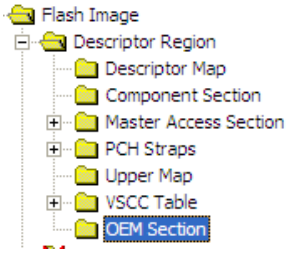
Location	Parameter	CRB Set To	Settings for Any Platform
Follow navigation tree below: • Select **Flash Image | Descriptor Region | VSCC Table |** • Set the parameters for the Atmel 4-MB SPI part in the **W25Q64BV** section as shown  • Right click VSSC Table to add a Flash entry. 	**Yellow means custom settings may be required.**		
	VendorID	Intel® CRBs use **0xEF**	For information on values that need to be entered in this section, refer to the Intel® *LPT-LP SPI programming Guide* and the SPI Flash device 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. Section *VSCC0 — Vendor Specific Component Capabilities 0* in the Intel® *WPT-LP SPI programming Guide* describes the 32-bit VSCC register value. Default is **0x00**. ***Note:***
	Device ID 0	Intel® CRBs use **0x40**	Use values obtained by using Vendor Serial Flash datasheet and Intel® *WPT-LP SPI programming Guide* Default is **0x00**.
	Device ID 1	Intel® CRBs use **0x17**	Use values obtained by using Vendor Serial Flash datasheet and Intel® *WPT-LP SPI programming Guide* Default is **0x00**. ***Note:*** For Broadwell-Y platforms set to value to **0x18**

Table 2-12. Flash Image | Descriptor Region | OEM Section

Location	Parameter	CRB Set To	Settings for Any Platform
Follow navigation tree below: • Select **Flash Image | Descriptor Region | OEM Section** • Set the parameters in the **OEM Section** section as shown 	**Yellow means custom settings may be required.**		
	Binary input file	(leave blank) Note: On Mobile CRBs modifying this value may cause Multi-BIOS not to behave properly	This is an optional field. Input depends on Customer Design and features support.

2.4.1 Set Up Soft-Straps

Table 2-13. Flash Image | Descriptor Region | PCH Straps | PCH Strap 0 (Sheet 1 of 2)

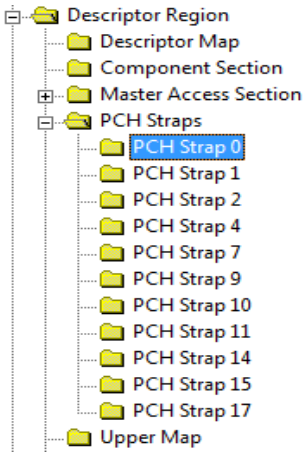
Location	Parameter	CRB Set To	Settings for Any Platform
Follow navigation tree below: • Select the **Flash Image** tab • Select **Flash Image | Descriptor Region | PCH Straps | PCH Strap 0** • Set the parameters in the **PCH Strap 0** section as shown 	**Yellow means custom settings may be required.**		
	BIOS Boot Block Size	64KB	BIOS Boot Block (BBB) is bare minimum BIOS code required to boot a platform. This soft-strap allows for proper address bit to be inverted as required by BBB Size. **64KB (default)** = Invert A16 if Top Swap is set **128KB** = Invert A17 if Top Swap is set **256KB** = Invert A18 if Top Swap is set If BIOS is stored in a separate SPI Flash device or in FWH (see Configurations "B", "C", and "D" in Appendix A then leave this parameter at **64KB**. ***Note:*** This must be determined by the target platform BIOS developer.
	DMI RequesterID Check Disable	false	Indicates if RequesterID checking during DMI accesses is disabled. This parameter should only for server platforms that contain multiple Processors. **false (default)** = Single Processor Platform **true** = Multiple Processor Platform ***Note:*** A quad/dual core processor counts as a single processor for this parameter.
	MACsec Disable	false	This setting should be set to 'false' to enable MACsec. The "MACsec ready" bit in the ME descriptor region should be enabled for support. • This bit must be set in the manufacturing plant and cannot be changed after shipment. **Note:** If MACsec is enabled in IT infrastructure will not function properly. See 'CDI #461067' for further details. ***Note:*** This field is read only if Intel integrated LAN is disabled. See Table 2-2
	LAN PHY Power Control GPIO12 Select	GPIO12 is used in native mode as LANPHYPC	**GPIO12 is used in native mode as LANPHYPC (default)** = Only required if target platform has Intel wired LAN and MCP GP12 is used as LAN_PHYPC for Intel LAN. **GPIO12 default is General Purpose (GP) output** = MCP GP12 is used as General Purpose Input/Output (GPIO) pin. Must be **0** if Third-party LAN and no Intel wired LAN is present. **Note:** Please consult with the target hardware designer to determine this setting.

Table 2-14. Flash Image | Descriptor Region | PCH Straps | PCH Strap 0 (Sheet 2 of 2)

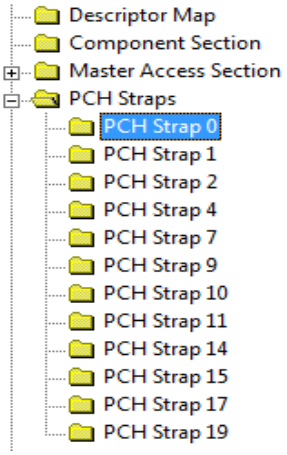
Location	Parameter	CRB Set To	Settings for Any Platform
Follow navigation tree below: • Select the **Flash Image** tab • Select **Flash Image | Descriptor Region | PCH Straps | PCH Strap 0** • Set the parameters in the **PCH Strap 0** section as shown 	**Yellow means custom settings may be required.**		
	Intel® ME SMBus Enable	true	**true** = Set for all platforms
	Intel® ME SMBus Frequency	Standard Mode (up to 100kHz)	Treat as reserved.
	SMLink0 Enable	true	**true (default)** = Intel LAN is present **false** = Third-party LAN is present
	SMLink0 Frequency	Fast Mode Plus (up to 1MHz)	Treat as reserved.
	SMLink1 Enable	true	**true (default)** = SMLink1 is being used by EC/SIO/BMC for Thermal Reporting. **false** = Set for all other platforms
	SMLink1 Frequency	Standard Mode (up to 100kHz)	Treat as reserved.

Table 2-15. Flash Image | Descriptor Region | PCH Straps | PCH Strap 1

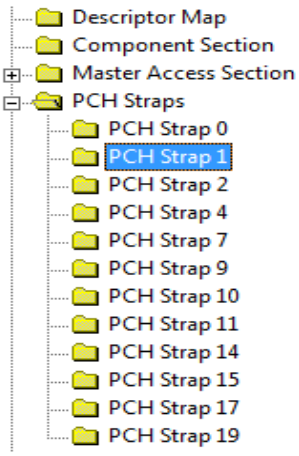
Location	Parameter	CRB Set To	Settings for Any Platform
Follow navigation tree below: • Select the **Flash Image** tab • Select **Flash Image | Descriptor Region | PCH Straps | PCH Strap 1** • Set the parameters in the **PCH Strap 1** section as shown 	**Yellow means custom settings may be required.**		
	TPM CLock Frequency	33MHz	This field identifies the frequency that should be used with the TPM on SPI. This field is undefined if the TPM on SPI is disabled by softstrap
	TPM on SPI	false	
	Dual Output Read Enable	true	This soft strap only has effect if Dual Output read is discovered as supported via SFDP If parameter table is not detected via SFDP, this bit has no effect and Dual Output Read is controlled via the Flash Descriptor Component Section. Dual Output Fast Read Support Bit
	Dual IO Read Enable	true	This soft strap only has effect if Dual I/O Read is discovered as supported via SFDP
	Quad Output Read Enable	true	This soft strap only has effect if Quad Output Read is discovered as supported via SFDP
	Quad IO Read Enable	true	This soft strap only has effect if Quad Output Read is discovered as supported via SFDP

Table 2-16. Flash Image | Descriptor Region | PCH Straps | PCH Strap 2

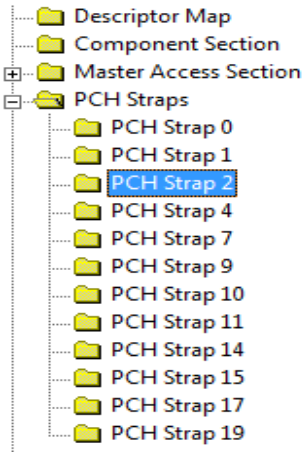
Location	Parameter	CRB Set To	Settings for Any Platform
Follow navigation tree below: • Select the **Flash Image** tab • Select **Flash Image | Descriptor Region | PCH Straps | PCH Strap 2** • Set the parameters in the **PCH Strap 2** section as shown 	**Yellow means custom settings may be required.**		
	Intel® ME SMBus I2C Address Enable	false	Treat as reserved.
	Intel® ME SMBus I2C Address (SMBI2CA)	0x00	Treat as reserved.
	Intel® ME SMBus MCTP Address Enable	false	Treat as reserved.
	Intel® ME SMBus MCTP Address	0x00	Treat as reserved.
	Intel® ME SMBus ASD Address Enable (MESMASDEN)	false	Treat as reserved.
	Intel® ME SMBus ASD Address (MESMASDA)	0x00	Treat as reserved.

Table 2-17. Flash Image | Descriptor Region | PCH Straps | PCH Strap 4

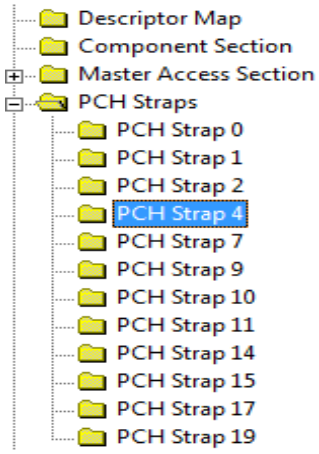
Location	Parameter	CRB Set To	Settings for Any Platform
Follow navigation tree below: • Select the **Flash Image** tab • Select **Flash Image | Descriptor Region | PCH Straps | PCH Strap 4** • Set the parameters in the **PCH Strap 4** 	**Yellow means custom settings may be required.**		
	GbE PHY SMBus Address	0x64	Intel wired LAN PHY SMBus address. No change required for this soft-strap value.
	GbE MAC SMBus Address	0x70	Intel wired LAN MAC SMBus address. No change required for this soft-strap value.
	GbE MAC SMBus Address Enable	true	**true (default)** = Intel integrated LAN is enabled **false** = Third-party LAN is present ***Note:*** This field is read only if Intel integrated LAN is disabled. See Table 2-2
	PHY Connectivity	10: PHY on SMLink0	**10: PHY Connectivity** = Intel LAN is present **00: No PHY Connected (default)** = Third-party LAN is present only ***Note:*** This field is read only if Intel integrated LAN is disabled. See Table 2-2

Table 2-18. Flash Image | Descriptor Region | PCH Straps | PCH Strap 7

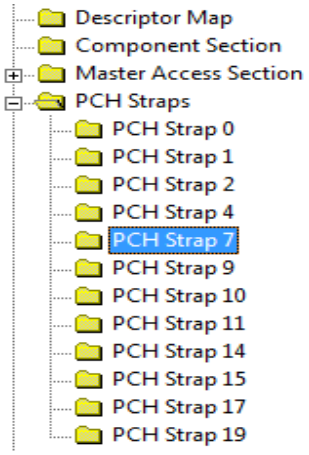
Location	Parameter	CRB Set To	Settings for Any Platform
Follow navigation tree below: • Select the **Flash Image** tab. • Select **Flash Image | Descriptor Region | PCH Straps | PCH Strap 7** • Set the parameters in the **PCH Strap 7** 	Intel® ME SMBus Subsystem Vendor & Device ID for ASF2	0x00000000	Treat as reserved.

Table 2-19. Flash Image | Descriptor Region | PCH Straps | PCH Strap 9

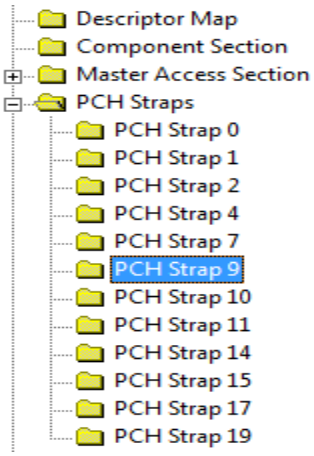
Location	Parameter	CRB Set To	Settings for Any Platform
Follow navigation tree below: • Select the **Flash Image** tab • Select **Flash Image | Descriptor Region | PCH Straps | PCH Strap 9** • Set the parameters in the **PCH Strap 9** 	**Yellow means custom settings may be required.**		
	TEMP_ALERT# or SML1ALERT# Select	TEMP_ALERT#	Treat as reserved.Treat as Reserved.
	Subtractive Decode Agent Enable	true	**true** = A PCI Bridge chip is connected to the MCP **false (default)** = A PCI Bridge chip is not connected to the MCP ***Note:*** Please consult the target hardware designer to determine this setting
	Intel® PHY Over PCI Express Enable	true	Treat as reserved.Treat as Reserved.
	GbE PCIe Port Select	100:Port 5 Lane 2	Only necessary if Intel LAN is present. **101** = Third-party LAN is present (don't care setting) ***Note:*** This field is read only if Intel integrated LAN is disabled. See Table 2-2 **000** = Port 3 **001** = Port 4 **010** = Port 5 Lane 0 **011** = Port 5 Lane 1 **100** = Port 5 Lane 2 **101** = Port 5 Lane 3
	PCIe Lane Reversal 2	false	This parameter must reflect platform topology. **Note:** This parameter can only be set to **PCIe Lanes 4-7 are reversed** if **PCIe Port configuration 2** is set to **1x4**.
	PCIe Lane Reversal 1	false	This parameter must reflect platform topology. **Note:** This parameter can only be set to **PCIe Lanes 0-3 are reversed** if **PCIe Port configuration 1** is set to **1x4**.
	PCIe Port Configuration 1	00: 4x1 Ports 1-4 (x1)	***Note:*** Please consult the target hardware designer to determine this setting
	USB3 Port 3 PCIe Port 1 Mode	PCIe Lane 1 is statically assigned to PCI Express (or GbE)	This soft strap set the dafault value of the USB3 PCI Express Port 2 Mode register that resides in the core well: PCIe Lane 1 is statically assigned to PCI Express (or GbE) PCIe Lane 1 is statically assigned to USB3 Port 3 ***Note:*** Please consult the target hardware designer to determine this setting
	USB3 Port 4 PCIe Port 2 Mode	PCIe Lane 2 is statically assigned to USB3 Port 4	This soft strap set the dafault value of the USB3 PCI Express Port 1 Mode register that resides in the core well: PCIe Lane 2 is statically assigned to PCI Express (or GbE) PCIe Lane 2 is statically assigned to USB3 Port 4 ***Note:*** Please consult the target hardware designer to determine this setting

Table 2-20. Flash Image | Descriptor Region | PCH Straps | PCH Strap 10

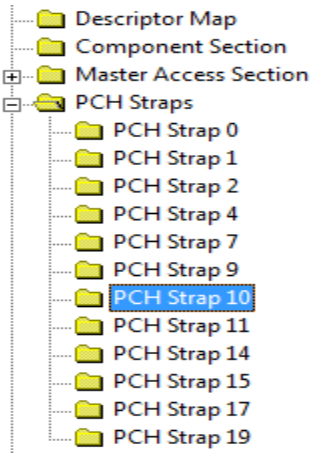
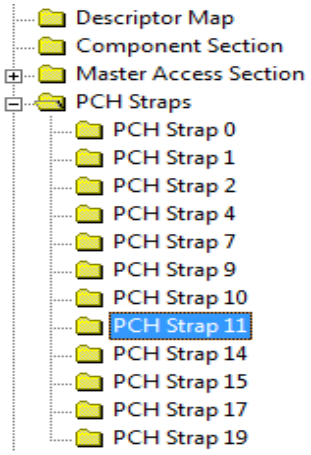
Location	Parameter	CRB Set To	Settings for Any Platform
Follow navigation tree below: • Select the **Flash Image** tab • Select **Flash Image | Descriptor Region | PCH Straps | PCH Strap 10** • Set the parameters in the **PCH Strap 10** section as shown 	**Yellow means custom settings may be required.**		
	Note: Intel® ICCS settings from PCH Strap 10 is removed and are moved to **Flash Image | ME Region | Configuration| Integrated Clock Controller.**		
	ME boot from Flash	true	**false (default)** = No ME Region binary loaded, or ME Region binary does not contain ME ROM bypass image **Note: On B0 and later MCP stepping parts this setting should be set to 'false'**
	Reserved	false	This value must be set to '**false**'
	ME Debug SMBus Emergency Mode Enable	false	**Note:** This option should not be enabled. Treat as Reserved.
	ME Debug SMBus Emergency Mode Address	0x00	**0x38** = Recommended SMBus address for ME Debug Set for non-production/debug platforms. **0x00** = Set for production platforms.
	ME Debug LAN Emergency Mode	false	**Note:** This option should not be enabled. Treat as Reserved.
	ME Debug Extended Data Enable	Disabled (default)	MDES Extended Data: Disabled (default) MDES data transmitted over SMBUS by boot path (including ROM)
	ME Reset Capture on CL_RST1#	false	Determines if ME reset assert/de-assert can be observed on MCP pin CL_RST1#. **true** = ME reset assert/de-assert can be observed on MCP pin CL_RST1# **false** = CL_RST1# usage is available as per *Wildcat Point-LP EDS*
	Deep SX Enable	false	**true (default)** = Platform HW configuration supports DSW rail and entry into Deep S3, S4 / S5. **false** = For platform that do not support DSW rail or Deep S3, S4 / S5. ***Note:*** Please consult with the target hardware designer to determine this setting. ***Note:*** See Section 4.1 – for details on configuring this option.
	Intel® Platform Trust Technology Permanent Disable	No	This option enables / disables the Intel® Platform Trust Technology using soft strap. **Yes** - Disable Intel® Platform Trust Technology **No** - **(default)** Enable Intel® Platform Trust Technology See Appendix D for configuration details
	DCI Pre-manufacturing Enable	Disabled	This setting configures the DCI interface for the platform.

Table 2-21. Flash Image | Descriptor Region | PCH Straps | PCH Strap 11

Location	Parameter	CRB Set To	Settings for Any Platform
Follow navigation tree below: • Select the **Flash Image** tab • Select **Flash Image | Descriptor Region | PCH Straps | PCH Strap 11** • Set the parameters in the **PCH Strap 11** section as shown 	**Yellow means custom settings may be required.**		
	SMLink1 I2C Target Address Enable	CRB uses **false**	**true (default)** = Enable EC/SIO/BMC to interact Thermal Reporting feature over SMLink1 **false** = Platform has no EC/SIO/BMC on SMLink1
	SMLink1 I2C Target Address	CRB uses **0x0**	This parameter defines a write address for PCH over SMLink1. Set this to an address supported by EC/SIO/BMC hardware. Note that PCH/Intel® ME acts as slave on SMLink and EC/SIO/BMC acts as master. **0x4C (default)** = PCH SMBus write address for EC on mobile CRB **0x00** = Platform has no EC/SIO/BMC on SMLink1
	SMLink1 GP Target Address Enable	CRB uses **false**	**true (default)** = Enable EC/SIO/BMC to interact Thermal Reporting feature over SMLink1 **false** = Platform has no EC/SIO/BMC on SMLink1
	SMLink1 GP Target Address	CRB uses **0x0**	This parameter defines a read address for PCH over SMLink1. Set this to an address supported by EC/SIO/BMC hardware. Note that PCH/Intel® ME acts as slave on SMLink and EC/SIO/BMC acts as master. **0x4B (default)** = PCH SMBus read address for EC on mobile CRB **0x00** = Platform has no EC/SIO/BMC on SMLink1

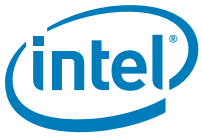


Table 2-22. Flash Image | Descriptor Region | PCH Straps | PCH Strap 14

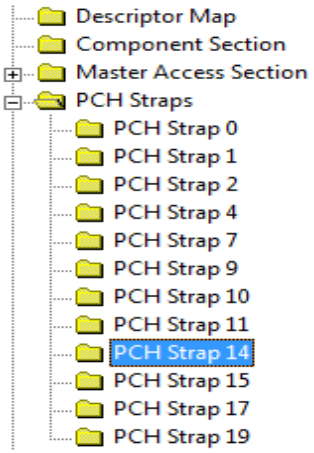
Location	Parameter	CRB Set To	Settings for Any Platform
Follow navigation tree below: • Select the **Flash Image** tab • Select **Flash Image | Descriptor Region | PCH Straps | PCH Strap 14** • Set the parameters in the **PCH Strap 14** section as shown 	**Yellow means custom settings may be required.**		
	SMLink1/GPIO Select	Pins assigned to GPIO [GPIO74/ GPIO75]	This setting determies if the GPIO 74 and GPIO 75 pins are assigned to Native mode or assigned to GPIO. Pins assigned to GPIO [GPIO74/GPIO75] Pins assigned to Native mode [SMLink1_Data/SMLink1_Clk]
	PCIe Lane Reversal 3	PCIe Port 6 Lane 0-3 are not reserved	This configures the Lane Reversal behavior for PCIe Port 6 if configured as a 4x1 port. PCIe Port 6 Lane 0-3 are not reserved PCIe Port 6 Lane 0-3 are reserved when configured as 1x4
	PCIe Port Configuration Strap 3	11: 1x4	This configures the default value of the PCIe port COnfiguration 2 register for PCIe Port 6. 00: 1x1 10: 1x2 11: 1x4
	PCIe Port Configuration Strap 2	11: 1x4	This configures the default value of the PCIe port COnfiguration 2 register for PCIe Port 5. 00: 1x1 10: 1x2 11: 1x4
	SATA Port 0 PCIe Port 6 Lane 3 Mode	Statically assigned to SATA Port 0	This configures the SATA Port 0 PCIe Port 6 Lane 3 mode. Statically assigned to SATA Port 0 Statically assigned to PCIe Port 6 Lane 3 Reserved Assigned based on the native mode of GPIO34 pin
	SATA Port 1 PCIe Port 6 Lane 2 Mode	Statically assigned to SATA Port 1	This configures the SATA Port 1 PCIe Port 6 Lane 3 mode. Statically assigned to SATA Port 1 Statically assigned to PCIe Port 6 Lane 2 Reserved Assigned based on the native mode of GPIO35 pin
	SATA Port 2 PCIe Port 6 Lane 1 Mode	Statically assigned to SATA Port 2	This configures the SATA Port 2 PCIe Port 6 Lane 3 mode. Statically assigned to SATA Port 2 Statically assigned to PCIe Port 6 Lane 1 Reserved Assigned based on the native mode of GPIO36 pin
	SATA Port 3 PCIe Port 6 Lane 0 Mode	Assigned based on the native mode of GPIO37 pin	This configures the SATA Port 3 PCIe Port 6 Lane 3 mode. Statically assigned to SATA Port 3 Statically assigned to PCIe Port 6 Lane 0 Reserved Assigned based on the native mode of GPIO37 pin
	Backbone Clock Source Select	OPI PLL is the source	This setting configures the Backbone Clock Source. OPI PLL is the source PCIe PLL is the source

Table 2-23. Flash Image | Descriptor Region | PCH Straps | PCH Strap 15

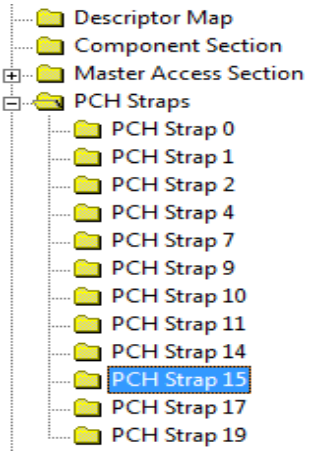
Location	Parameter	CRB Set To	Settings for Any Platform
Follow navigation tree below: • Select the **Flash Image** tab • Select **Flash Image | Descriptor Region | PCH Straps | PCH Strap 15** • Set the parameters in the **PCH Strap 15** section as shown 	**Yellow means custom settings may be required.**		
	PCIe Power Stable Timer Enable	t205b timer is disabled	This strap controls the behavior of the t205b timer. t205b timer is disabled MCP will count 99ms from PWROK assertion before PLTRST# is de-asserted ***Note:*** See *Wildcat Point-LP EDS* for details
	SLP_WLAN#/GPIO29 Select	false	**true =** Enables GPIO29 and disables SLP_WLAN# functionality. **false** =Set to false to use have GPIO behave as SLP_WLAN#.
	t1001 Timing	1 ms	This setting controls t1001 timing from CPUWRGD assertion to SUS_STAT#. **1ms (default)** **30us** **5ms** **2ms** ***Note:*** See *Wildcat Point-LP EDS* for details
	t573 Timing	1ms	This setting controls minimum t573 timing from XCK_PLL locked to CPUWRGD. **100 ms (default)** **50 ms** **5 ms** **1 ms** ***Note:*** See *Wildcat Point-LP EDS* for details
	Intel® Integrated LAN Enable	true	**true** = Intel LAN is enabled **false** = Intel LAN is disabled ***Note:*** This field is read only if Intel integrated LAN is disabled. See Table 2-2.
	Deep Sx Platform	false	**true (default)** = Platform HW configuration supports DSW rail and entry into Deep S3, S4 / S5. **false** = For platform that do not support DSW rail or Deep S3, S4 / S5. ***Note:*** Please consult with the target hardware designer to determine this setting. ***Note:*** See Section 4.1 – for details on configuring this option.

Table 2-24. Flash Image | Descriptor Region | PCH Straps | PCH Strap 17

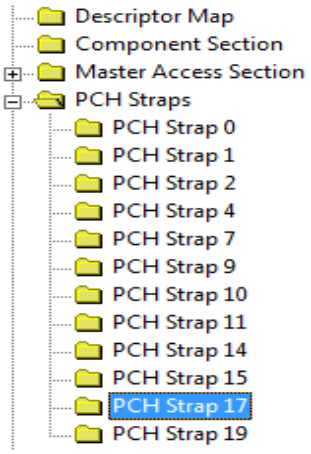
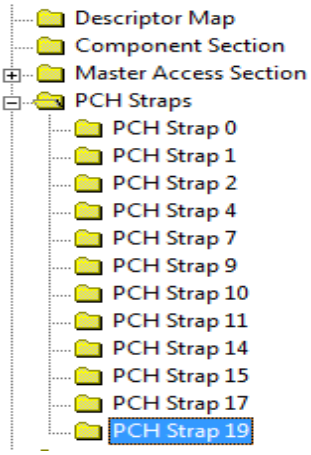
Location	Parameter	CRB Set To	Settings for Any Platform
Follow navigation tree below: • Select **Flash Image | Descriptor Region | PCH Straps | PCH Strap 17** • Set the parameters in the **PCH Strap 17** section as shown 	**Yellow means custom settings may be required.**		
	BTM/FCIM Select	Full Clock Integrated Mode	If MCP clock boot mode is specified by soft strap then this parameter specifies whether the MCP clocks boot in Full Clock Integrated Mode (FCIM) or Buffer Through Mode (BTM). **NOTE:** Buffer Through Mode (BTM) is **NOT** POR mode supported by Broadwell PCH-LP Platform I/O and it will not be validated by Intel.

Table 2-25. Flash Image | Descriptor Region | PCH Straps | PCH Strap 19

Location	Parameter	CRB Set To	Settings for Any Platform
Follow navigation tree below: • Select the **Flash Image** tab • Select **Flash Image | Descriptor Region | PCH Straps | PCH Strap 19** • Set the parameters in the **PCH Strap 19** section as shown 	**Yellow means custom settings may be required.**		
	SATA MPHY Power Control Default	0=configures pin as SATA MPHY PC (out)	This strap configures the default state of GPIO35/ SATAP1_PCIE6L2B_MODE/SATAPC. 0 = Set as SATA MPHY Power Control (SATAPC) - Default 1 = Enable SATA Port 1 PCIe Port 6 Lane 2 Mode (SATAP1_PCIEP6L2_MODE)
	USB3 MPHY Power Control Default	0=configures pin as USB3 MPHY PC (out)	This strap configures the default state of GPIO76/BMBUSYB/USB3PC. If it is not set as USB3PC, the pin will switch to GPIO (Input) until it is configured by SW to BMBUSY#. 0 = Set as USB3 MPHY Power Control (USB3PC) - Default 1 = Set as GPIO76

2.5 Configure MCP Silicon SKU

Use the **SKU Manager Combo Box** to select the appropriate platform type for your specific chipset.

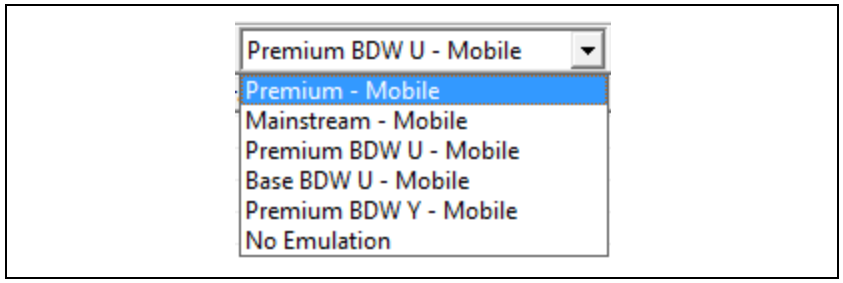
For Intel® ME 1.5MB FW, the only valid choices are:

- Mobile 4th Generation Intel® Core™ Processor (U-Series) Platform I/OBroadwell PCH-LP Platform I/O Chipset
  - — Premium - Mobile
  - — Mainstream - Mobile
  - — Premium BDW U - Mobile
  - — Base BDW U - Mobile
  - — Premium BDW Y - Mobile
  - — No Emulation

Note: To configure a single image that will work on **Haswell / Wildcat Point** and **Broadwell / Wildcat Point** MCPs set the SKU dropdown selection to **No Emulation**.

Note: For **Haswell / Wildcat Point** Super SKU MCPs the LPC Device ID will not show as **9CC1h** as noted in the Wildcat POint-LP EDS specifications it will be shown as **9CC3h**

Figure 2-4. SKU Manager Combo Box



When a MCP SKU is selected in FITC, Super SKU MCP silicon will then behave as if it were the selected Production SKU MCP silicon from Intel® ME FW perspective. The SKU Manager selection option has no effect on Production SKU MCP silicon. Features cannot be enabled on such SKUs that do not support them.

Note: The SKU Manager combination box changes the LPC device ID which is used to identify the MCP. If there are issues with drivers, host software, or BIOS that do not recognize the MCP, then select the appropriate SKU with Super SKU DID.

Note: For more information see Section 4.1 for Intel® ME FW features listed by Production SKU silicon.

Note: Sections of FITC other than the **Features Supported** folder under **Flash Image ME| Region| Configuration** will not reflect what is disabled for the selected MCP silicon SKU and/or ME FW binary.

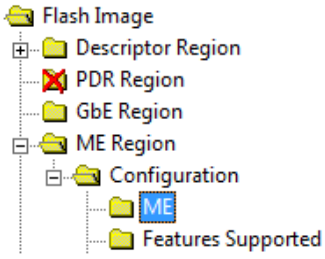
2.6 Intel®ME FW Feature Configuration

Note: Do not load or change any parameters in the Configuration tab until you load an Intel®ME Region binary (see Table 2-3).

Note: **For LynxPoint / Wildcat Point MCP configurations use the PreProduction_Rom_Bypass binary.**

2.6.1 Firmware Features and Capabilities

Table 2-26. Flash Image | ME Region | Configuration | ME (Sheet 1 of 2)

Location	Parameter	CRB Set To	Settings for Any Platform
Follow navigation tree below: • Select **Flash Image | ME Region | Configuration | ME** • Set the parameters in the **ME** section as shown 	**Yellow means custom settings may be required.**		
	FW Update OEM ID	00000000-0000-0000-0000-000000000000	This field provides the ability to target FWUpdate (FWUpdLcl.exe) by Platform OEM. This ID will make sure that customers can only update a platform with an image coming from the platform OEM. If set to an all zeros, then any input is valid when doing a firmware update.
	LAN Power Well Config	3	Intel LAN power configuration selection: **0** = Core Well (SLP_S3#) **1** = Sus Well (RSMRST#) **2** = ME Well (SLP_M#) **3 (recommended)** = SLP_LAN#
	WLAN Power Well Config	0x86	**0x80** = Disabled **0x82** = Sus Well **0x83** = ME Well **0x86** = WLAN Sleep via SLP_WLAN# (default)
	M3 Power Rails Availability	true	**true** = M3 power rails designed on platform (ME is powered by standby) **false** = M3 power rails not designed on platform (ME is powered by core) ***Note:*** Please consult the target hardware designer to determine this setting.
	Host ME Region Flash Protection Override	true	**false** = Disable HMFPRO LOCK and HMFPRO ENABLE Intel® MEI messages for BIOS-based FW Update **true** = Enable this capability ***Note:*** Please consult the target BIOS developer to determine this setting.
	PROC_MISSING	No onboard glue logic	Only set if there is glue logic present on the board to enable if the processor is missing. **Note:** This field is read only if a Mobile SKU is selected in the SKU Manager pull down box. ***Note:*** Please consult the target hardware designer to determine this setting.

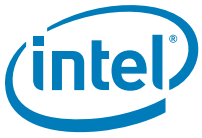
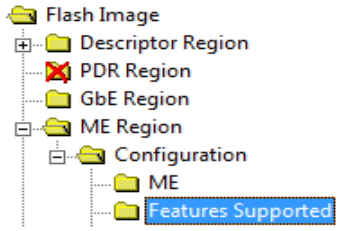


Table 2-26. Flash Image | ME Region | Configuration | ME (Sheet 2 of 2)

Location	Parameter	CRB Set To	Settings for Any Platform
	Processor Emulation	**EMULATE Intel (R) Core (TM) branded Processor**	Set this parameter to the type of processor that the target system will use during production. This field will emulate that processor class for pre-production silicon.
	OEM Tag	0x00000000	This value allows OEMs to set a unique number value in their firmware images to allow for easier identification.
	Hide FW Update Control	false	This option determines if the MEBx FW Update is visible or hidden from end users. **'false'** - The Intel® MEBx FW update option will be visible to end users. **'true'** - The Intel® MEBx FW update option will not be visible to the end user.
	Debug Si Features	0x00000000	Allows OEM Control to enable FW features to assist with the debug of the platform. This control has no effect if used on production silicon. **Bit 0:** Disable DRAM_INIT_DONE timeout **Bit 1:** Disable FW WDT (when descriptor is unlocked) **Bit 2:** Disable CPU_RESET_DONE timeout **Bit 3:** Override power package to always enter M3 **Bit 4:** Disable Power Gating
	Prod Si Features	0x00000000	Allow OEM Control to enable FW features to assist with the production platform. **Bit 0:** Extend DRAM_INIT_DONE timeout to 30 minutes **Bit 1:** Disable FW WDT (when descriptor is unlocked) **Bit 2:** Disable CPU_RESET_DONE timeout **Bit 3:** Override power package to always enter M3
	M3 Autotest Enabled	false	This enables Intel®ME FW M3 auto test during platform early boot. '**false**' - The Intel®ME FW will not run M3 tests during first boot after plattorm image flash. '**true**' - The Intel®ME FW will run M3 tests during first boot after platform image flash.
	Independent Firmware Recovery Enable	true	This option determines if Independent Firmware Recovery is enabled. '**false**' - Independent Firmware Recovery is disabled in the firmware. '**true**' - Independent Firmware Recovery is enabled in the firmware.
	Screen Blanking Enabled	false	This option will enable monitor screen blanking during remote screen redirection sessions. ***Note:*** This feature is only available on specific CPU models.
	CEK Configuration	Blank	Treat as Reserved

Table 2-27. Flash Image | ME Region | Configuration | Features Supported

Location	Parameter	CRB Set To	Settings for Any Platform
Follow navigation tree below: • Select **Flash Image | ME Region | Configuration | Features Supported** • Set the parameters in the **Features Supported** section as shown 	**Yellow means custom settings may be required.**		
	Enable Intel® Standard Manageability; Disable Intel® AMT	Yes	***Note:*** Setting any of these options to 'Yes' will permanently disable that specific feature. Once the feature is disabled in this manner only re-Flashing the ME region can re-enable the feature. Fields are read only if the feature is not supported by respective MCP SKU selected by MCP SKU pull down (see Section 2.5).
	Intel® Manageability Application Permanently Disabled?	Yes	
	PAVP Permanently Disabled	No	
	KVM Permanently Disabled?	Yes	
	TLS Permanently Disabled?	No	
	Intel® Anti-Theft Technology Permanently disabled	No	
	Intel® ME Network Service Permanently disabled	No	
	Intel® Manageability Application Enable/ Disable	Disabled	Disabled (not supported on 1.5MB FW)
	Intel® Platform Trust Technology Enable/ Disable	Enabled	See Appendix D for configuration details

Note: The Feature supported settings shown above are an example.
Refer to Appendix 4.1 for information on specific SKU related settings.

Table 2-28. Flash Image | ME Region | Configuration | Manageability Application

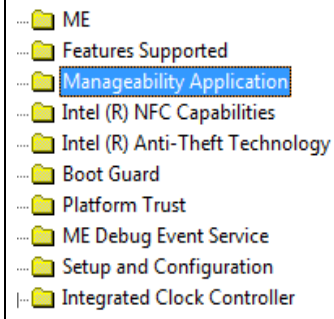
Location	Parameter	CRB Set To	Settings for Any Platform
Follow navigation tree below: • Select **Flash Image | ME Region | Configuration | Manageability Application** • Set the parameters in the **Manageability Application** section as shown 	**Yellow means custom settings may be required.**		
	Boot into BIOS Setup Capable	false	Treat as reserved.
	Pause during BIOS Boot Capable	false	Treat as reserved.
	BIOS Reflash Capable	false	Treat as reserved.
	Enforce Secure Boot over IDER	false	Treat as reserved.
	USBr EHCI 1 Enabled	11b Enabled	Treat as reserved.
	USBr EHCI 2 Enabled	10b Disabled	Treat as reserved.
	Privacy/Security Level	Default	Treat as reserved.
	AMT Idle Timeout	65535	Treat as reserved.

Table 2-29. Flash Image | ME Region | Configuration | Intel® NFC Capabilities

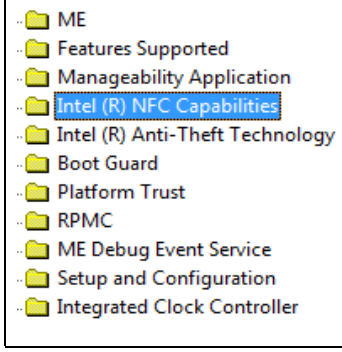
Location	Parameter	CRB Set To	Settings for Any Platform
Follow navigation tree below: • Select **Flash Image | ME Region | Configuration | Intel® NFC Capabilities** Set the parameters in the **Intel® NFC Capabilities** section as shown 	**Yellow means custom settings may be required.**		
	Near Field Communication Enabled	false	This parameter controls whether or not NFC is enabled on the platform. **true -** NFC Enabled **false -** NFC Disabled
	SMBus Address	0x28-NXP	This parameter controls the SMBUS slave address of the NFC HW module. This address may vary from one NFC module vendor to another. Make sure you know the SMBUS address used by your NFC HW module. If you use Magnetics Peak (MGP) module, the address should be set to 0x5E.
	Active GPIO	GPIO26	This parameter determines the GPIO used as IRQ line between the MCP (Intel ME FW) and the NFC module. You should set the GPIO based on the HW design of the platform. Options are: GPIO26 or GPIO73

Table 2-30. Flash Image | ME Region | Configuration | Intel® Anti-Theft Technology

Location	Parameter	CRB Set To	Settings for Any Platform
Follow navigation tree below: • Select **Flash Image | ME Region | Configuration | Intel® Anti-Theft Technology** • Set the parameters in the **Intel® Anti-Theft Technology** section as shown ME Features Supported Manageability Application Intel (R) NFC Capabilities Intel (R) Anti-Theft Technology Boot Guard Platform Trust RPMC ME Debug Event Service Setup and Configuration Integrated Clock Controller	**Yellow means custom settings may be required.**		
	Allow Unsigned Assert Stolen	false	Treat as reserved.
	Intel(R) Anti-Theft BIOS Recovery Timer	Disabled	Treat as reserved.
	Flash Protection Override Policy Hard	Allowed When AT Not Provisioned	Treat as reserved.
	Flash Protection Override Policy Soft	Allowed When AT Not Provisioned	Treat as reserved.

Table 2-31. Flash Image | ME Region | Configuration | Boot Guard

Location	Parameter	CRB Set To	Settings for Any Platform
Follow navigation tree below: • Select **Flash Image | ME Region | Configuration | Boot Guard** Set the parameters in the **Boot Guard** section as shown ME Features Supported Manageability Application Intel (R) NFC Capabilities Intel (R) Anti-Theft Technology Boot Guard Platform Trust RPMC ME Debug Event Service Setup and Configuration Integrated Clock Controller	**Yellow means custom settings may be required.**		
	OEM Public Key Hash	<Raw hash string or certificate file>	This is a 256-bit field representing the SHA-256 hash of the OEM public key that corresponds to the private key used to sign the BIOS-SM. **Enter raw hash string or certificate file.**
	Key Manifest ID	0x0	Contains the has of another public key, used by the ACM to verify the Boot Policy Manifest.
	Boot Guard Profile Configuration	Boot Guard Profile 0 - No_FVME	See Appendix C for profile details.
	CPU Debug Disabled	false	**false** - Do not disable any CPU debug modes. **true** - Disable CPU debug modes.
	BSP Initialization Disabled	false	**false** - If BSP receives an INIT, BSP handles it normally. **true** - If BSP receives an INIT, BSP signals an error to the BSS register and enters unrecoverable shutdown.
Note: After the End of Manufacturing command, these settings will be permenatly set into the FPFs contained in the MCP. If disabled, the specific MCP can never be enabled for Boot Guard **If the MCP has already been set through a previous End of Manufacturing command, these settings will not have any affect.**			

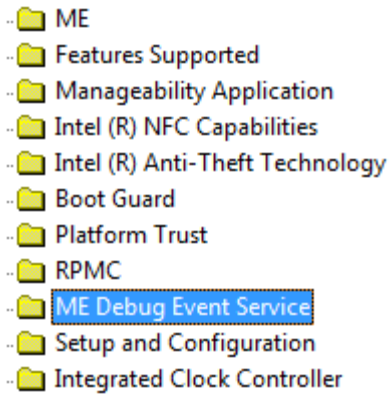
Table 2-32. Flash Image | ME Region | Configuration | Platform Trust

Location	Parameter	CRB Set To	Settings for Any Platform
Follow navigation tree below: • Select **Flash Image | ME Region | Configuration | Platform Trust** • Set the parameters in the **Platform Trust** section as shown ME Features Supported Manageability Application Intel (R) NFC Capabilities Intel (R) Anti-Theft Technology Boot Guard Platform Trust RPMC ME Debug Event Service Setup and Configuration Integrated Clock Controller	**Yellow means custom settings may be required.**		
	Intel® Platform Trust Technology Permanent Disable	No	This value can be changed under PCH Strap 10.
	Intel® Platform Trust Technology Enable / Disable	Enabled	This value can be changed under ME Features Supported.
	Intel PTT HW Enable / Disable	Enabled	Enabled - Intel® Platform Trust Technology is set to enabled Disabled - Intel® Platform Trust Technology is set to disabled See Appendix D for configuration details **Note: After the End of Manufacturing command, this setting will be permenatly set into the FPFs contained in the MCP. If disabled, the specific MCP can never be enabled for Intel® PTT** **If the MCP has already been set through a previous End of Manufacturing command, this setting will not have any affect.**

Table 2-33. Flash Image | ME Region | Configuration | RPMC

Location	Parameter	CRB Set To	Settings for Any Platform
Follow navigation tree below: • Select **Flash Image | ME Region | Configuration | RPMC** • Set the parameters in the **RPMC** section as shown ME Features Supported Manageability Application Intel (R) NFC Capabilities Intel (R) Anti-Theft Technology Boot Guard Platform Trust RPMC ME Debug Event Service Setup and Configuration Integrated Clock Controller	**Yellow means custom settings may be required.**		
	RPMC Supported	true	This option if depenent on SPI part which have RPMC support.
	RPMC Rebinding	true	Setting this option to 'true' will enable the Rebinding of RPMC enabled SPI part(s).

Table 2-34. Flash Image | ME Region | Configuration | ME Debug Event Service

Location	Parameter	ME Debug Enabled SPI Logging* (FITC Default)	Full ME Debug Enabled	Settings for Any Platform
Follow navigation tree below: • Select **Flash Image | ME Region | Configuration | ME Debug Event Service** • Set the parameters in the **ME Debug Event Service** section as shown 	**Green means custom settings may be required (for enabling ME Debug only)**			
	Error Filter	Critical	All	
	Logging Interface	Flash	Network	This option controls the output inteface for logging PDA messages: **Disabled** = Message logging disabled **Network** = Message logging sent over Wired LAN interface **SMBus** = Message logging sent over SMBus. **Flash** = Message logging sent to SPI flash. **PRAM** = Message logging sent to ME PRAM **SVT** = Message logging sent to SVT interface.
	Buffer Size	1	24	Default is **1**.
	Buffer Mode	Blocking	Buffered	**Note:** Delayed Flush is not supported. **Note:** Buffered mode should never be used when using SPI logging.
	Source IP Address	10.2.0.2	10.2.0.2	
	Destination IP Address	10.2.0.255	10.2.0.255	
	Destination MAC Address	0C FF 17 22 FF 2D	0C FF 17 22 FF 2D	This is the MAC address of the SUT.
	Slave Address Enable	false	true	
	Slave Address	0x00	0x56	Default is **0x56**.
	Event Filters	Filter Group 1: **0x00000001** Filter Group 76: **0x000000FE** **All other values set to**: **0x00000000**	**Basic** Filter Group 1: **0x00000001** Filter Group 5: **0x00000003** Filter Group 70: **0x00000001** **Advanced (Intel LAN)** Filter Group 1: **0x00000001** Filter Group 4: **0x000003F6** Filter Group 5: **0x00000003** Filter Group 70: **0x00000001** **Advanced (SMBus)** Filter Group 1: **0x00000001** Filter Group 4: **0x000003F6** Filter Group 5: **0x00000003** Filter Group 70: **0x00000001**	Event Filter Groups / Name of Event Filter Group 1 CheckPoint 4 Loader 5 Power Management 6 MPC 70 HECI 74 MBP 75 BIOS Debug 109 WLAN **Note:** To enable Filter groups **74** and **75** add a **1** value to enable group 109 a **0xffffffff** value.

Parameter	Value
Error Filter	Critical
Logging Interface	Flash
Buffer Size	1
Buffer Mode	Blocking
Source IP Address	10.2.0.2
Destination IP Address	10.2.0.255
Destination MAC Address	0C FF 17 22 FF 2D
Slave Address	0x00
Event Filters	Click To Edit

Basic Filter configuration:

Filter Group 1	0x00000001
Filter Group 5	0x00000003
Filter Group 6	0x000F0000
Filter Group 70	0x00000001

Advanced Filter configuration (LAN):

Filter Group 1	0x00000001
Filter Group 4	0x000003F6
Filter Group 5	0x00000003
Filter Group 6	0x000F0000
Filter Group 70	0x00000001

Advanced Filter configuration (SMBus):

Filter Group 1	0x00000001
Filter Group 4	0x000003F6
Filter Group 5	0x00000003
Filter Group 6	0x000F0000
Filter Group 70	0x00000001

Table 2-35. Flash Image | ME Region | Configuration | Setup and Configuration

Location	Parameter	CRB Set To	Settings for Any Platform
Follow navigation tree below: • Select **Flash Image | ME Region | Configuration | Setup and Configuration** • Set the parameters in the **Setup and Configuration** section as shown ME Features Supported Manageability Application Intel (R) NFC Capabilities Intel (R) Anti-Theft Technology Boot Guard Platform Trust RPMC ME Debug Event Service Setup and Configuration Integrated Clock Controller	**Yellow means custom settings may be required.**		
	ODM ID used by Intel(R) Services	0x00000000	These fields are used by Intel® Services. Intel® Identity Protection Technology (Intel® IPT) use ODM ID field only (for platform identification between the OEM and the ISBV).
	System Integrator ID used by Intel(R) Services	0x00000000	
	Reserved ID used by Intel(R) Services	0x00000000	
	MCTP static EIDs	0x920030	Defines the Intel® ME 8 bit MCTP endpoint IDs for Each SMBus segment. Only bits 0-7 are supported to be modified. Bits 8-23 must be left to 0x9200
	Permit Period Timer Resolution	Days	Treat as reserved.
	PKI DNS Suffix	Leave Blank	Treat as reserved.
	OEM Default Certificate Active	false	Treat as reserved.
	OEM Default Certificate Friendly Name	Leave Blank	Treat as reserved.
	OEM Default Certificate Stream	Leave Blank	Treat as reserved.
	OEM Customizable Certificate 1-3 Active	false	Treat as reserved.
	OEM Customizable Certificate 1-3 Friendly Name	Leave Blank	Treat as reserved.
	OEM Customizable Certificate 1-3 Stream	Leave Blank	Treat as reserved.
	Embedded Host Based Configuration	false	This option controls the behavior for Embedded Host Based Configuration. If set to '**true'** the Privacy / Security Level will be read-only and set to default. If the Privacy / Security Level is set to Non-Default this option will be read-only and set to **'false'**.

2.6.2 Clock Control Parameters

Table 2-36. Flash Image | ME Region | Configuration | Integrated Clock Controller

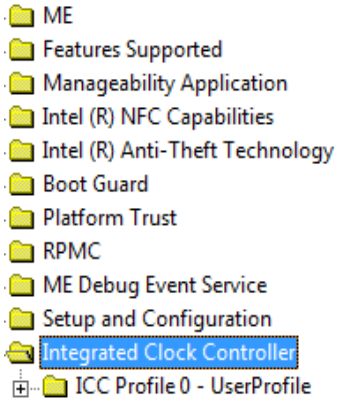
Location	Parameter	CRB Set To	Settings for Any Platform
Follow navigation tree below: • On the navigation tree to the left, select the **Flash Image | ME Region | Configuration | Intergrated Clock Controller.** 	***Note:*** Intel® ICCS settings from PCH Strap 10 are removed . These settings are moved to **Flash Image | ME Region | Configuration| Integrated Clock Controller.**		
	Default Profile Selection	ICC Profile 0 - Standard	This value is used to select default profile to be used by the final generated SPI Flash binary image by the target platform at boot time. This value is valid only if ICC Boot profile is selected by softstrap. SPI Flash binary images across multiple board designs are expected to contain the same block of clock control parameters. Selection is limited to the profiles defined under "Integrated Clock Controller" **up to maximum 16 profiles.** Profiles can be added by right clicking on "Integrated Clock Controller" and selecting "Add profile". The 'Record #' refers to profile created under the Configuration Tab, **Flash Image | ME Region | Configuration | Integrated Clock Controller**. Default boot profile for system is **ICC Profile 0 - Standard**.
	Profile Selection By SoftStrap/BIOS	SoftStrap	Specifies if the ICC Boot Profile is selected by Soft Strap or controlled by BIOS.
	Default Lock Enables Mask	0:Default	This parameter controls lock enable mask. it defines the integrated clock registers left accessible to OS after EOP. **Default** - Locks all but the registers used to adjust nominal clock frequency and spread settings. **All Locked -** Locks all clock adjustments after EOP message received. **All Unlocked** - Unlocks all clocks. This option is mainly used for debug purpose.

Table 2-37. Flash Image | ME Region | Configuration | Integrated Clock Controller | ICC Profile 0 - Standard

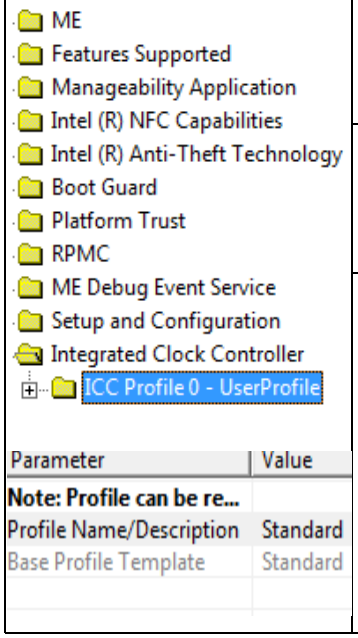
Location	Parameter	CRB Set To	Settings for Any Platform
Follow navigation tree below: • On the navigation tree to the left, select the **Flash Image | ME Region | Configuration | Intergrated Clock Controller |ICC Profile 0- Standard.** 	***Note:*** **FITC provides 2 pre- defined ICC profiles.** • **Standard:** This profile provides default settings for standard configuration, no adaptive clocking is allowed. Platform clocks output internal and external(CPU,PCIe,USB3 and SATA) are driven from MODDIV2**.** Default clock frequency is 100 MHz with 0.5%DownSpread. • **WiMax3G:** This profile provides Wimax friendly configuration. This profile will configure the platform based on the standard profile allowing adaptive clocking adjustment to reduce EMI interference. Defalut clock frequency is 99.8267MHz with spread percentage 0.288%-down spread. ***Note:*** In FITC, default profile is Standard. **To add other pre -defined profiles** ,right click on **Flash Image | ME Region | Configuration | Integrated Clock Controller | Add profile** and choose profile from drop down menu.		
	Profile Name/Description	Standard	This parameter allows user to customize profile name for for easy identification. By deafult it uses pre-defined profile name.
	Base Profile Template	Standard	This parameter indicates which pre-defined profile selected when profile was added.

Table 2-38. Flash Image | ME Region | Configuration | Integrated Clock Controller | ICC Profile 0 - Standard | Power Management Settings

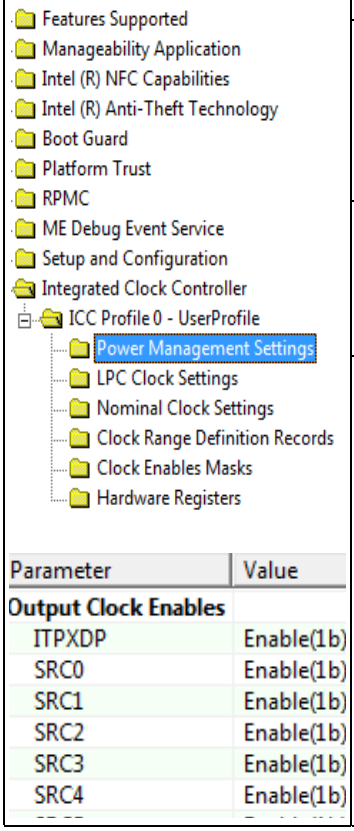
Location	Parameter	CRB Set To	Settings for Any Platform
Follow navigation tree below: • On the navigation tree to the left, select the **Flash Image | ME Region | Configuration | Intergrated Clock Controller| ICC Profile 0 - Standard| Power Management Settings**. 	Output Clock Enables	Keep defaults.	This parameter controls enabling /disabling of specific output clocks at boot time. These settings should match with platform hardware design. For CRB, recommend keeping defaults for bring up with Intel® ME FW.
	LPC Clock Power Management	Keep defaults.	This parameter controls enabling/disabling of CLKRUN support for CLKOUT_LPC clocks. For CRB, recommend keeping defaults for bring up with Intel® ME FW.
	CLKREQ# Associations	Keep defaults.	This parameter controls association of dynamic CLKREQ control with SRC(PCIe and CPU) clocks. For CRB, recommend keeping defaults for bring up with Intel® ME FW.
	Miscellaneous Power Settings	Keep defaults.	Dynamic Power Management of HDA PLL parameter controls enabling/disabling HD Audio clock source to dynamically bring this clock down to lower power state when hardware detects idle condition. This clock source is used for Gbe, TimeSync and Azalia. WarmRest Gating of CLKOUT_DP parameter controls enabling/disabling the output enable of the CLKOUT_DP signal during warm reset. Note: for WarmReset Gating of CLKOUT_DP parameter, keep default value.

Table 2-39. Flash Image | ME Region | Configuration | Integrated Clock Controller | ICC Profile 0 - Standard | LPC Clock Settings

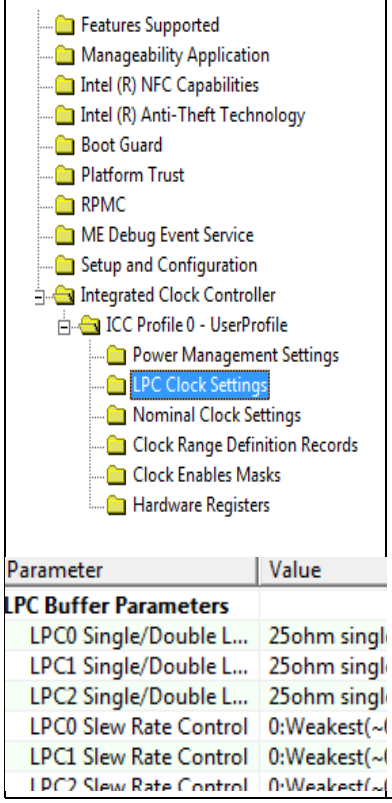
Location	Parameter	CRB Set To	Settings for Any Platform
Follow navigation tree below: • On the navigation tree to the left, select the **Flash Image | ME Region | Configuration | Intergrated Clock Controller| ICC Profile 0 - Standard|PC Clock Settings** •  	LPC Buffer Parameters	keep defaults	LPC[0:1] Slew Rate Control parameter controls slew rate for output clock CLKOUT_LPC[0:1]. LPC [0:2] Single/Double Load Series Register parameter allows to set programmable series resistance for output clock CLKOUT_LPC[0:2].

Table 2-40. Flash Image | ME Region | Configuration | Integrated Clock Controller | ICC Profile 0 - Standard | Nominal Clock Settings

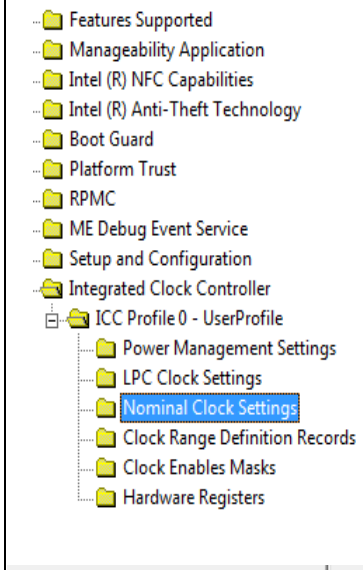
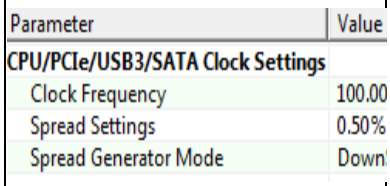
Location	Parameter	CRB Set To	Settings for Any Platform
Follow navigation tree below: • On the navigation tree to the left, select the **Flash Image | ME Region | Configuration | Intergrated Clock Controller| ICC Profile 0 - Standard|Nominal Clock Settings.**   	CPU/PCIe/USB3/SATA Clock Settings	Keep defaults	This parameter controls clock frequency and spread setting for MODDIV2 clock. For CRB, recommend keeping defaults for bring up with Intel® ME FW.

Table 2-41. Flash Image | ME Region | Configuration | Integrated Clock Controller | ICC Profile 0 - Standard | Clock Range Definition Records

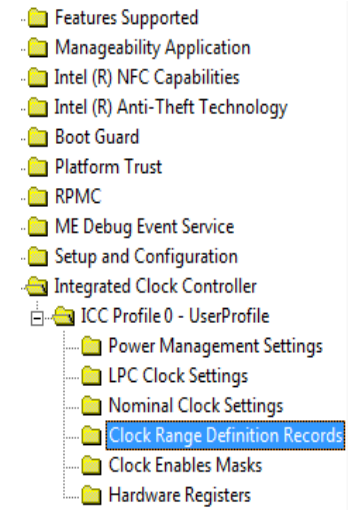
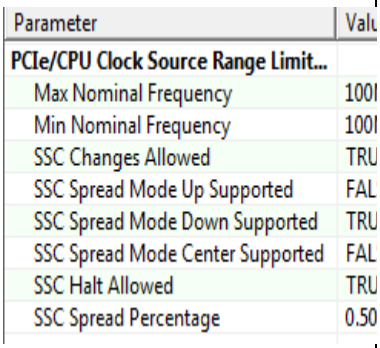
Location	Parameter	CRB Set To	Settings for Any Platform
Follow navigation tree below: • On the navigation tree to the left, select the **Flash Image | ME Region | Configuration | Intergrated Clock Controller| ICC Profile 0 - Standard|Clock Range Definition Record.** ***Note:*** Max Nominal Frequency refers to maximum divider value which corresponds to minimum frequency output value. Min Nominal Frequency refers to minimum divider value which corresponds to maximum frequency output value.   	PCIe/CPU Clock Source Range Limit(MODDIV2)	Keep defaults	This parameter controls Max nominal and Min nominal frequency as well as Max spread % range for MODDIV2.

Table 2-42. Flash Image | ME Region | Configuration | Integrated Clock Controller | ICC Profile 0 - Standard | Clock Enables Masks

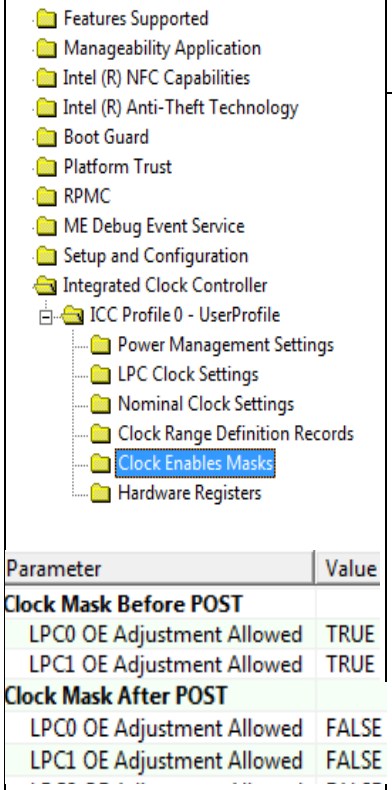
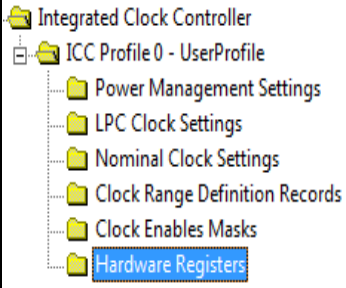
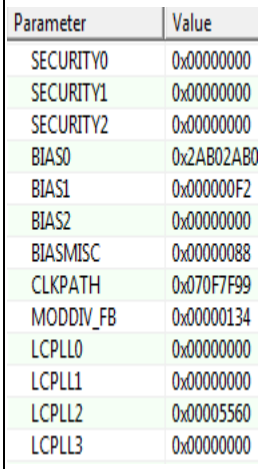
Location	Parameter	CRB Set To	Settings for Any Platform
Follow navigation tree below: • On the navigation tree to the left, select the **Flash Image | ME Region | Configuration | Intergrated Clock Controller| ICC Profile 0 - Standard|Clock Enables Masks** •  	Clock Mask Before POST	keep defaults	This parameter allows which clocks can be turned On/Off using HECI command before POST. Mask determining which clock output enables can be modified through the SET_CLOCK_ENABLES interface prior to End-Of-POST. Typically prior to EOP, all OE adjustments should be allowed by the BIOS. Disabling OE adjustment prior to EOP will prevent BIOS from runtime enabling/disabling the clock.
	Clock Mask After POST	keep defaults	This parameter allows which clocks can be turned On/Off using HECI command after POST. Mask determining which clock output enables can be modified through the SET_CLOCK_ENABLES interface after to End-Of-POST. Typically after to EOP, only clocks associated with slotted devices should remain enabled. All others will be disabled, so that no runtime adjustments are allowed.

Table 2-43. Flash Image | ME Region | Configuration | Integrated Clock Controller | ICC Profile 0 - Standard | Hardware Registers

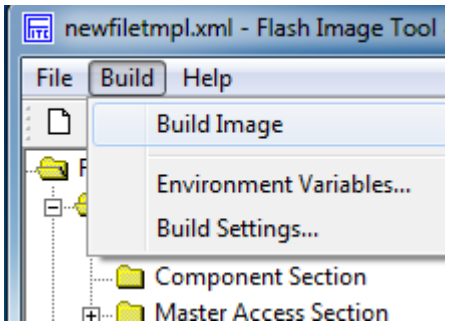
Location	Parameter	CRB Set To	Settings for Any Platform
Follow navigation tree below: • On the navigation tree to the left, select the **Flash Image	ME Region	Configuration	Intergrated Clock Controller	ICC Profile 0 - Standard	Hardware Registers.** 		Keep Defaults	This section displays all ICC registers. Values are programed based on parameters selected using pre-defined ICC profile. If any parameter is changed from its default value , Hardware register specific to that parameter will be highlighted to yellow. **Note:** Do not modify any Hardware registers.

2.7 Build SPI Flash Binary Image

2.7.1 Build SPI Flash Binary Image

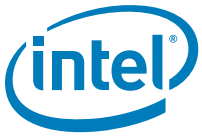
In the main menu select **Build | Build Image**. The image will be saved in the directory specified by **$DestDir** parameter and will be named **outimage.bin**, unless the default **Output Directory** in **Build | Build Settings** was changed (see Section 2.1).

Figure 2-5. Build | Build Image



2.7.2 Save Your Settings

In the main menu select **File | Save As...**. Select a name and location for the XML file that contains all the settings configured thus far. It is recommended that you save this file in your **[root)]\Tools\System Tools\Flash Image Tool** directory for easy access.



Assuming that the custom settings file was saved as **customfile.xml** to the FITC directory (**[root)]\Tools\System Tools\Flash Image Tool**), then these settings could be loaded in the FITC GUI itself using the main menu option **File | Load…**.

Note: Previous platform generations of the FITC tool required multiple configuration files to be edited and saved. For this generation, only one configuration file **(customfile.xml)** is required.

This custom settings file could also be used to generate an SPI Flash binary image using the command line, with a command of the form:

```
fitc.exe [xml_file] [/o <file>] /b
```

Example usage: > fitc.exe newfiletmpl.xml /o .\temp.bin /b

where:

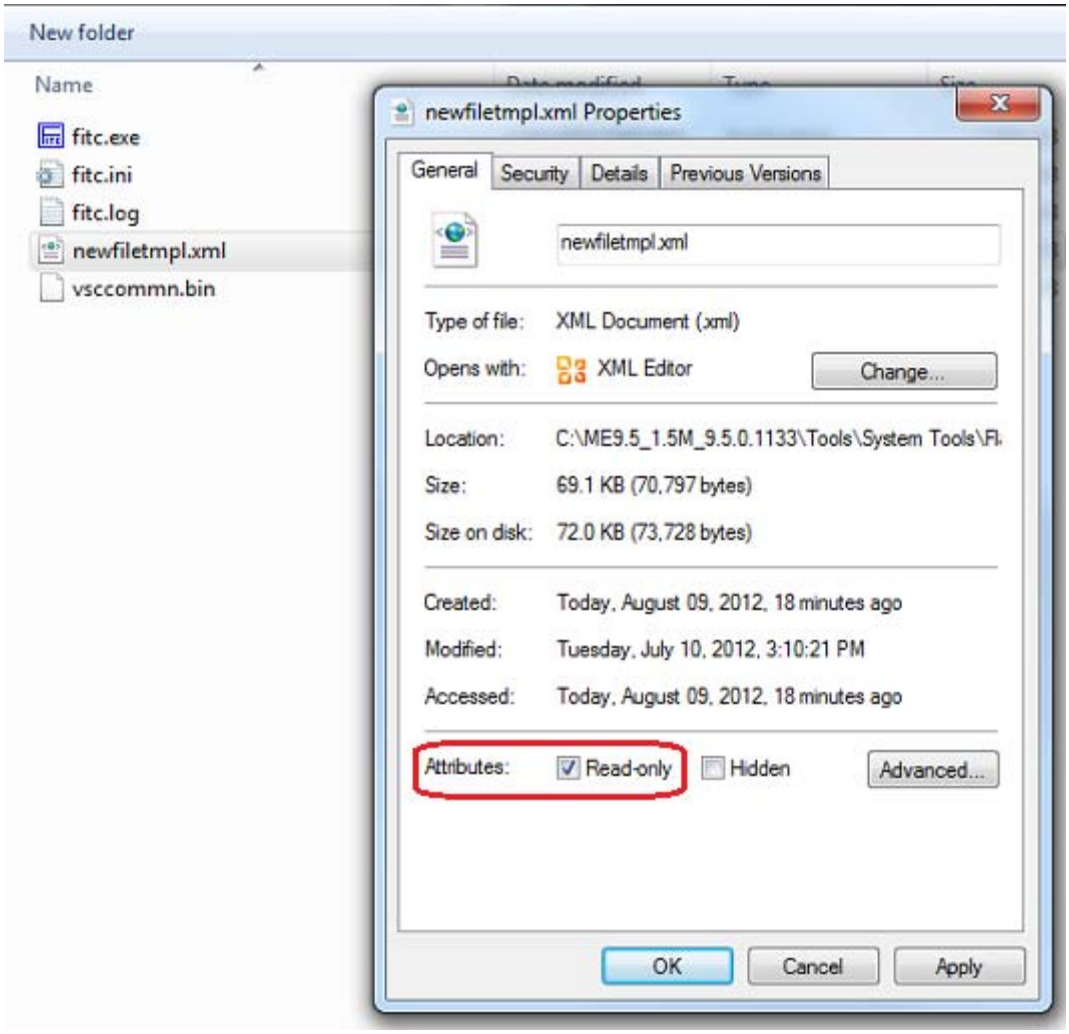
- **<xml_file>** — The XML configuration file saved when configuring FITC.
- **/o <file>** — The path and filename where the image will be saved. This command overrides the 'Output path' in the XML file.
- **/b** — Automatically builds the Flash image. The FIT GUI will not be displayed when this flag is set, since FIT will run in auto-build mode. Error messages will be displayed by FITC, if necessary.

2.7.3 Protect Saved Configuration XML File

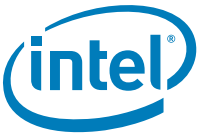
To avoid custom-configured values from ever overwritten when loading new binaries files (ie: when loading binaries into BIOS, GbE and ME regions in FITC) do the following (see Figure 2-6):

- After building the SPI Flash binary image and saving your configuration, close Flash Image Tool
- Right-click on the saved FITC configuration XML file (**customfile.xml**) and select **Properties**
- Check the **Read-Only** checkbox and click **OK**

Figure 2-6. Protecting FITC Configuration XML File



§ §



3 Programming SPI Flash Devices and Checking Firmware Status

Now that the Flash image file has been created, it can be programmed into the SPI Flash device(s) of the target machine. For platforms that don't boot, a Flash Chip Programmer will be required. For platforms that can boot to DOS or Windows*, the Flash Programming Tool (FPT) can be used.

3.1 Flash Burner/Programmer

The specific use of a Flash burner/programmer is beyond the scope of this document. Here are some general steps that may be followed:

1. Navigate to your **Output Directory** (as specified in Section 2.7.2) where your generated SPI Flash image(s) are saved. It is assumed that this image file is named **outimage.bin**.

   If two total SPI Flash devices were specified during the build process, then additional image files will be saved, one for each SPI Flash device. These files are assumed to be named **outimage(1).bin** and **outimage(2).bin**.
2. Utilize a Flash burner/programmer to program the image(s). For multiple SPI Flash devices, the images are numbered sequentially to correspond to the first and second SPI Flash device accordingly.

3.1.1 In-Circuit SPI Flash Programming for Mobile CRB

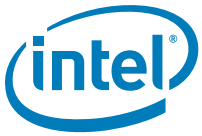
Mobile CRBs have the SPI Flash devices soldered down. As a result, to program the SPI Flash for mobile CRBs, follow these steps:

1. Leave mobile CRB powered off.
2. Connect Flash Programmer (such as DediProg SF100) header to connector **J8E1** which is labelled **"SPI PROG"**. Make sure to line up pin 1 on the header.
3. Change the jumpers to the **"Programming SPI-0"** mode as shown in Table 3-1 below.

Table 3-1. Jumper Settings for Mobile CRB SPI Flash Programming

Mode	J8C4	J8C5	J8D1
Programming SPI-0	1-2	1-2	1-2
Programming SPI-1	1-2	1-2	2-3
Normal Operation	1-X	1-X	1-X

4. Program the first image [outimage(1).bin] to the CRB.
5. Following Table 3-1, change the jumpers to the **"Programming SPI-1"** mode.
6. Program the second image [outimage(2).bin] to the CRB.
7. Once programming is complete, disconnect the Flash Programmer header. The CRB is now ready for power on.



3.2 Flash Programming Tool (FPT)

FPT can be used to substitute for a Flash burner/programmer, provided the system is capable of booting to a DOS or Windows* OS.

Note: FPT will automatically disable the Intel® ME prior to flashing the image to the platform.

FPT DOS Version

The DOS versions supported by FPT are: DOS, Free DOS, and DRMK DOS. Use the following steps to program the SPI Flash devices,

1. Copy all the files in the "(root)\Tools\System Tools\Flash Programming Tool\DOS" directory to the root directory of a bootable USB key.
2. Navigate to your **Output Directory** (as specified in Section 2.7.2) where your generated SPI Flash image(s) are saved. It is assumed that this image file is named **outimage.bin**. Copy this image file to the root directory of the USB key.
3. Boot the target system to DOS and change to the root directory of the bootable USB key. At the DOS prompt type:

```
fpt.exe /i
```

   The system should respond with the number of SPI Flash devices available. For example:

```
--- Flash Devices Found ---
W25Q64BV ID:0xEF4017 Size: 8192KB (65536Kb)
W25Q64BV ID:0xEF4017 Size: 8192KB (65536Kb)
```

   Note: If the SPI Flash device does not currently contain a descriptor it may report only a single device.

4. Program the SPI Flash image to the Flash device(s) by issuing the following command at the prompt:

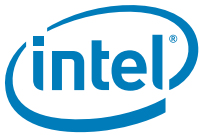
```
fpt.exe /f outimage.bin
```

   If the programming was successful, then the following message will be shown.

```
FPT Operation Passed
```

   If the programming was **NOT** successful, then repeat this step to try again. If programming problems persist, then check the SPI Flash devices and platform hardware.

5. Execute a platform global reset using FPT -greset. Next go to Section 3.3 to check the Intel® ME Firmware status.



3.2.1 FPT Windows* Version

The Windows* OS versions supported by FPT are: Windows* PE, Windows* XP SP2, Windows* Vista and Windows* 7. There are two versions of FPT for Windows*: a 32-bit version and a 64-bit version. Most Windows* OS, Windows* XP, Vista and Windows* 7 (32-bit or 64-bit) can use Windows* version of FPT. However, Windows* OS which do not support 32 bit compatible mode (Win PE 64-bit) **must use** FPT Windows* 64-bit version due to compatibility issues.

Use the following steps to program the SPI Flash devices,

1. Navigate to your **Output Directory** (as specified in Section 2.7.2) where your generated SPI Flash image(s) are saved. It is assumed that this image file is named **outimage.bin**. Copy this image file to FPT directory located at "(root) \Tools\System Tools\Flash Programming Tool\Windows".
2. Boot the target system to Windows* and open a Command Prompt window. In this window, change to the FPT directory and at the prompt type:

```
fptw.exe /i
```

   The system should respond with the number of SPI Flash devices available. For example:

```
--- Flash Devices Found ---
W25Q64BV ID:0xEF4017 Size: 8192KB (65536Kb)
W25Q64BV ID:0xEF4017 Size: 8192KB (65536Kb)
```

   Note: If the SPI Flash device does not currently contain a descriptor it may report only a single device.

3. Program the SPI Flash image to the Flash device(s) by issuing the following command at the prompt:

```
fptw.exe /f outimage.bin
```

   If the programming was successful, then the following message will be shown.

```
FPT Operation Passed
```

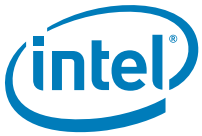
   If the programming was **NOT** successful, then repeat this step to try again. If programming problems persist, then check the SPI Flash devices and platform hardware.

4. Power down the platform with a G3 power cycle (ensure all power is disconnected from the system). Next go to Section 3.3 to check the Intel® ME Firmware status.

3.3 Checking Intel® ME Firmware Status

Use the following steps to check the platform health and Intel® ME FW status,

1. Copy the file **MEInfo.exe** in the "(root)\Tools\System Tools\MEInfo\DOS" directory to the root directory of a bootable USB key.



2. Boot the target system and use F2 or Del to enter the BIOS setup menu. Load default values for BIOS (on Intel® CRBs press F3 to load default values). Save and reboot (on Intel® CRBs press F4 and select Yes).
3. Boot the target system to DOS and change to the root directory of the bootable USB key. At the DOS prompt type:

```
MEInfo.exe
```

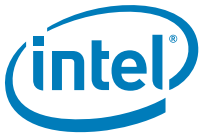
The system should respond with a message similar to below.

```
Intel(R) MEInfo Version: 10.0.0.xxxx
Copyright(C) 2005 - 2011, Intel Corporation. All rights reserved.

Intel(R) Manageability and Security Application code versions:

BIOS Version:                          ACRVMBY1.86C.0035.B00.1103131018
MEBx Version:                          10.0.0.xx
Gbe Version:                           1.3
VendorID:                              8086
PCH Version:                           600000
FW Version:                            10.0.0.xxxx

FW Capabilities:                       0x0DFE5C67

    Intel(R) Active Management Technology - PRESENT/ENABLED
    Intel(R) Anti-Theft Technology - PRESENT/ENABLED
    Intel(R) Capability Licensing Service - PRESENT/ENABLED
    Protect Audio Video Path - PRESENT/ENABLED
    Intel(R) ME Dynamic Application Loader - PRESENT/ENABLED

Intel(R) AMT State:                    Enabled
CPU Upgrade State:                     Upgrade Capable
Cryptography Support:                  Enabled
Last ME reset reason:                  Power up
Local FWUpdate:                        Enabled
BIOS and GbE Config Lock:              Enabled
Host Read Access to ME:                Enabled
Host Write Access to ME:               Enabled
SPI Flash ID #1:                       EF4017
SPI Flash ID VSCC #1:                  20052005
BIOS boot State:                       Post Boot
OEM Id:                                00000000-0000-0000-0000-000000000000
```

As in the above example if there are NO errors shown, then

- your platform's health is good
- Intel® ME FW has successfully initialized
- Intel® ME FW is operating normally

Note: This section is only intended to show how to use the MEInfo.exe tool for checking firmware status. For full usage and capabilities of the MEInfo.exe tool, please see the System Tools User Guide.



3.4 Common Bring Up Issues and Troubleshooting Table

Table 3-2. Common Bring Up Issues and Troubleshooting Table

Problem / Issue	Solution / Workaround
System does not boot to DOS	By default, the system will boot to EFI Shell. To boot to DOS, 1. Enter BIOS menu, then go to the 'Boot' screen 2. Change 'Boot Option #1' to be your USB key (ensure USB key is formatted to be DOS bootable) 3. Press 'F4' to save settings and reboot
Hear 3 beeps when platform powers on	Possible device is disconnected or device not found, check • platform power and MCP fan power connectors • DIMM memory modules • USB devices (keyboard, mouse, USB key) may be plugged into inactive USB port • missing/incorrect jumpers • missing MCP
No display on monitor	Ensure 1.5MB FW SKU supports integrated graphics. Try external graphics card.
USB device not detected or does not work	USB device may be plugged into inactive USB port
System does not boot (Post Code 00)	Incorrect Flash image – possible reasons: • wrong FW selected during Flash image build process • wrong Flash size selected Re-build image with correct settings and re-flash using Flash burner.

§ §

4 Intel® ME Firmware Features - Details and Settings

4.1 Deep Sx Settings

This chapter covers configuration settings for the Mainstream - Mobile Platform I/O based Desktop and Mobile CRB platforms Deep Sx operation.

Table 4-1. Deep Sx Settings for Desktop CRB

Desktop boards	Option	Settings
DeepSx Enabled		
FITC Strap 10	DeepSx	True
BIOS	Advanced -> PCH-IO Configuration-> DeepSx Power Policies	Enabled in S5 or Enabled in S4-S5
DeepSx Disabled		
FITC Strap 10	DeepSx	True
BIOS	Advanced -> PCH-IO Configuration-> DeepSx Power Policies	Disabled

Table 4-2. Deep Sx Settings for Mobile CRB

Mobile boards	Option	Settings
DeepSx Enabled		
FITC Strap 10	DeepSx	True
BIOS	Advanced -> PCH-IO Configuration-> DeepSx Power Policies	Enabled in S5/Battery or Enabled in S4-S5/Battery
DeepSx Disabled		
FITC Strap 10	DeepSx	True
BIOS	Advanced -> PCH-IO Configuration-> DeepSx Power Policies	Disabled

A Appendix — Flash Configurations

This chapter covers only the basic information needed for clock control parameter programming. For a more detailed treatment of Mainstream - Mobile Family clocks, see *Broadwell PCH-LP Clocks* and *Intel® Management Engine — Platform Compliancy Guide for ME Hardware*.

Figure A-1. Configuration "A"

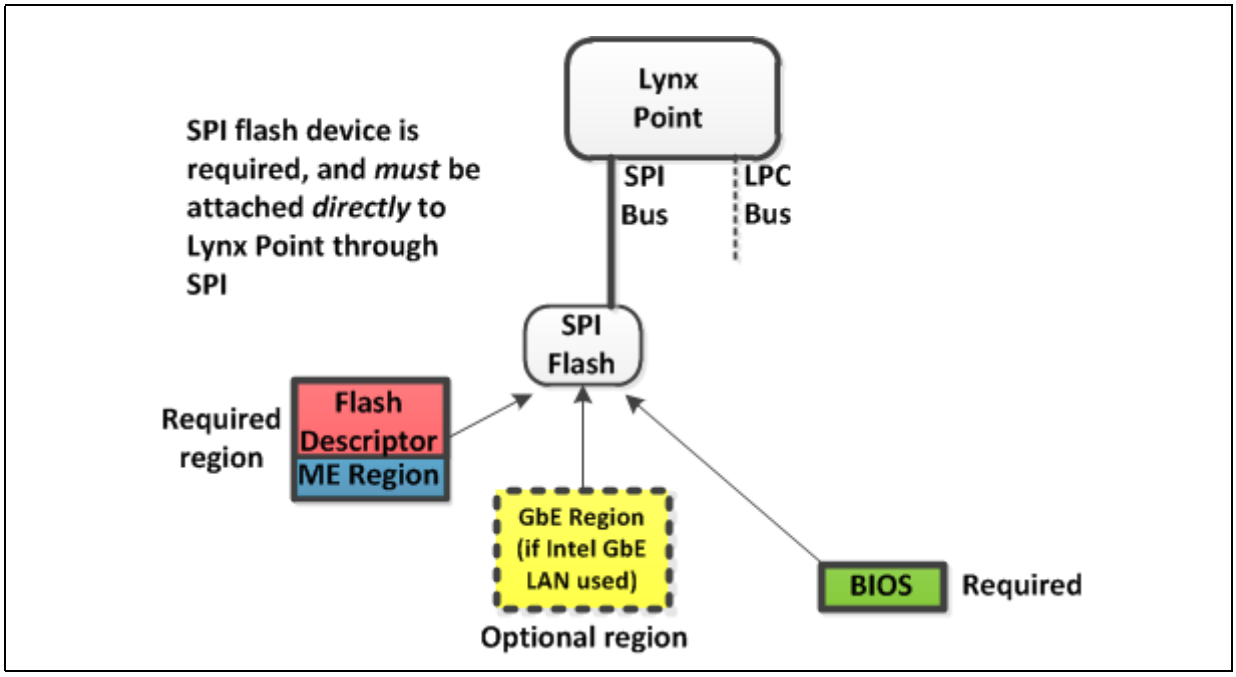


Figure A-2. Configuration “B”

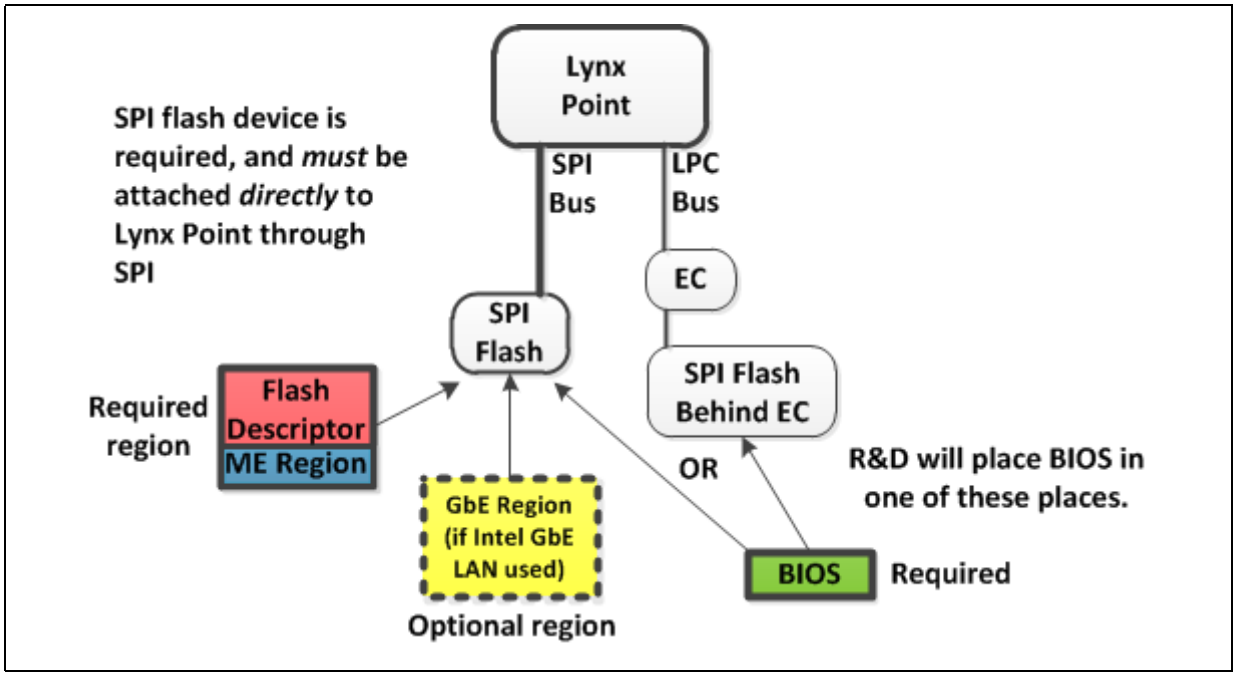
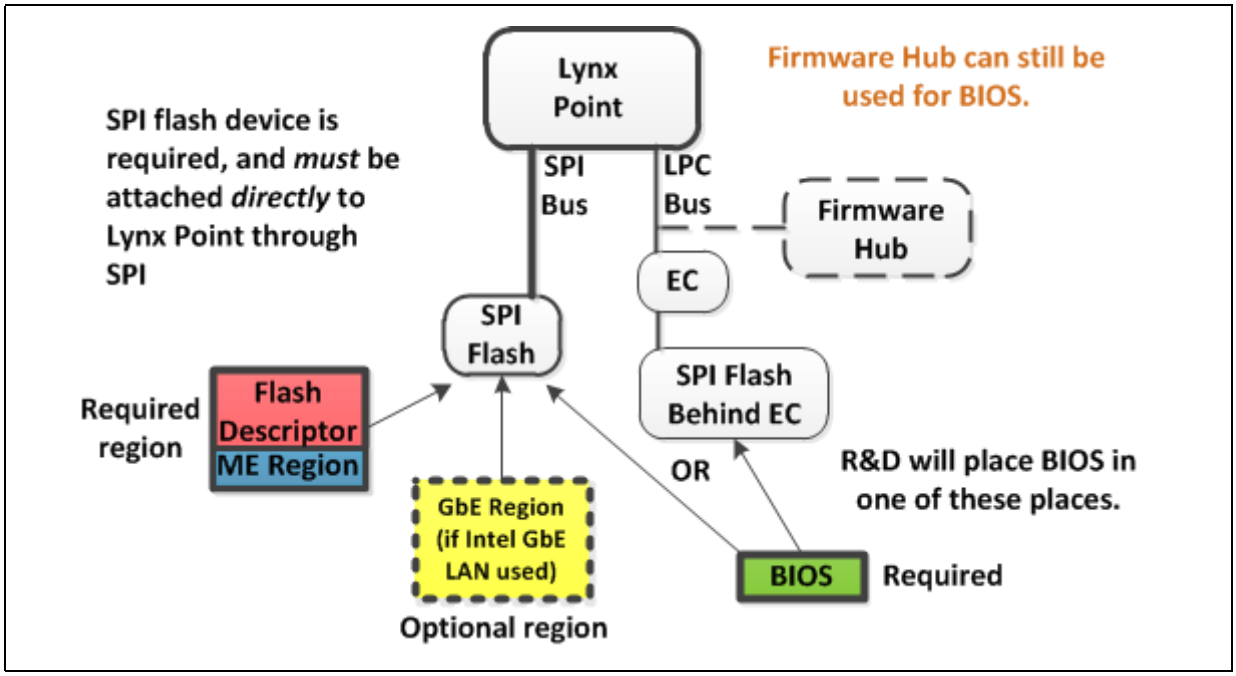


Figure A-3. Configuration “D”



§ §

B Appendix — Intel® ICCS SKU Support Matrix

Note: Please refer to Broadwell PCH-LP Platform Controller Hub (PCH) External Design Specification (EDS) for details about Broadwell PCH-LP Chipset Full Clock Integration Mode Architecture and Intel®ME FW clock control parameters.

For more information on validating and checking compliancy for MCP clocks, see *Broadwell PCH-LP Intel® Management Engine — Compliancy Guide.*

B.1 Intel® ICCS SKU Support Matrix

The following table describes features, clock range (maximum and minimum), spread mode supported by Broadwell Platform I/O Chipset MCP SKU. The Intel® ICCS SKU is divided into 2 categories; Basic and enhanced.

Table B-1. Intel® ICCS SKU Matrix

PCH SKU	Basic	Enhanced
Base		**x**
Premium		**x**
Performance		**x**
Features Supported	Display Clock Bending	Display Clock Bending Adaptive Clocking (Wimax Friendly Clocking)
Pre-Defined ICC profile supported.	Standard	Standard WiMax3G
Clock Range Supported	**MODDIV2** [Min-Max]=100MHz.	**MODDIV2** [Min - Max] = 99.5392 - 100 MHz.
Spread Mode and Max Spread % Supported	Lynx Point PCH HW supports Down Spread mode with Max Spread % = 0.5%	

Min = Clock Div Max (minimum allowed frequency)

Max = Clock Div Min (maximum allowed frequency)

C Appendix — Boot Guard Configuration

C.1 Boot Guard Profiles

The following table describes the profiles available for Boot Guard Configuration.

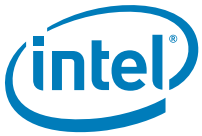
Table C-1. Profile Description

Index	Profile Name	F	V	M	ENF	PBE	Description
0	**Boot Guard Profile - No_FVME**	0	0	0	00	0	This configuration will invoke Boot Guard during boot with neither Verification nor Measurement. For platforms with all the required Boot Guard components but do not wish to enable Boot Guard boot block verification protection.
1	**Boot Guard VE**	0	1	0	01	1	When Verification is desired but if verification fails the platform will continue to boot with the unverified IBB for a short period, to allow remediation.
2	**Boot Guard VME**	0	1	1	01	1	When Verification and Measured are desired and the asset protection is provided by both TPM protection and a timed remediation period.
3	**Boot Guard VM**	0	1	1	00	1	When Verification and Measured are desired and the asset protection is provided by TPM protection.
4	**Boot Guard FVE**	1	1	0	11	1	Strict Verification enforcement.
5	**Boot Guard FVME**	1	1	1	11	1	Strict Verification and Measured enforcement. Prevents unverified IBB from running.

C.2 Enforement Policies

Table C-2. Enforcement Policy Description

Error Enforcement Policy (ENF)	Enforcement Mode Name	Description
0	**Unrestricted Mode**	Infinite time before shutdown – don't shutdown the platform, let everything run normally.
1	**Remediation Mode**	**30 minutes** before shutdown – enough time to remediate the system, e.g. update BIOS or other data on flash via host tools.
2	**Reserved**	
3	**Restricted Mode**	**0 minutes** before shutdown – instant shutdown policy.



C.3 OEM Profile Parameters

Table C-3. Profile Parameters Description

Parameter	Description	Settings
Force Boot Guard ACM Enabled (F)	Force Boot Guard Boot determines if the platform starts the Force Boot Guard Boot timer. If it successfully starts it indicates success. When the Force Boot Guard timer stops, it starts the Protect Bios Environment timer, if indicated by the boot policy restrictions. Anchor ACM then jumps to the Initial Boot Block(IBB) with the Force Boot Guard Boot time stopped and the Protect BIOS enable timer running.	**false** - Allow the CPU to jump to the legacy reset vector if the Boot Guard Module cannot be successfully loaded. (default) **true -** Force the Boot Guard ACM to execute.
Verified Boot Enabled (V)	Boot Guard cryptographically verifies the platform Initial Boot Block (IBB) using the boot policy key. On successful verification, Boot Guard executes Initial Boot Block (IBB) using the boot policy key. If the verification fails, Anchor signals or enters Remediation.	**false** - Platform does not perform verified boot (default) **true** - Platform performs verified boot
Measured Boot Enabled (M)	Boot Guard measures the Initial Boot Block (IBB) into the TPM. Boot Guard perform no verification that the IBB is correct or from the platform manufacturer. The Haswell implementation of Boot Guard will support measurements into TPM or Intel's Platform Trust Technology.	**false** - Platform does not perform measured boot (default) **true** - Platform performs measured boot
Protect Bios Environment Enabled (PBE)	Platform manufacturer may want Initial boot block to be protected between verification/ measurement and execution from attacks on buses and non-CPU components. Boot Guard accomplishes this by allowing the initial boot block to be verified and executed in LLC in NEM if PBE is enabled.	**false** - Take no actions to control the environment during execution of the BIOS components (default) **true** - Takes actions to control the environment during the execution of the BIOS components.
Error Enforcement Policy (ENF)	Boot Guard invokes the Enforcement Policy when a fatal error is encountered. The action taken by ENF is determined by the OEM set persistent policies. Like, • Allowing platform to continue to boot • Immediate Shutdown • Shutdown with Timeout intervals When the ENF logic is invoked, PTT or TPM also disconnects.	See Section C-2 for details.

D Appendix — Intel® Platform Trust Technology

D.1 Intel® Platform Trust Technology

The following table describes the platform configurations supported by Intel® Platform Trust Technology.

Note: Intel® Platform Trust Technology does not support the full TPM functionality requirements and should not be used for Intel® vPro based platforms.

Table D-1. Intel® Platform Trust Technology Configuration table

Configuration	ME Region -> Configuration -> Platform Trust -> Enable Intel® Platform Trust Technology	ME Region -> Configuration -> Features Supported -> Intel® Platform Trust Technology Enable / Disable	PCH Strap 10 -> Intel® Platform Trust Technology Permanent Disable	Description
Intel® PTT Permanently Disabled in HW via FPF	**Disabled**	**N/A**	**N/A**	After the End of Manufacturing command, this setting will permenatly set into the FPFs contained in the MCP. If disabled, the specific MCP can never be enabled for Intel® PTT.
Intel® PTT Permanently disabled in base firmware image	**Enabled**	**N/A**	**Yes**	This setting allows Intel® PTT to disabled without disabling the MCP FPFs. This is the recommended option to permanently disable Intel® PTT on a platform.
Intel® PTT ship state disabled in base firmware image	**Enabled**	**Disabled**	**No**	Intel® PTT initially shipped in disabled mode, can be enabled by BIOS command.
Intel® PTT enabled	**Enabled**	**Enabled**	**No**	Recommended setting for Windows*8 Connected Standby platforms and Intel® SBA platforms. Intel® PTT can be disabled by BIOS command