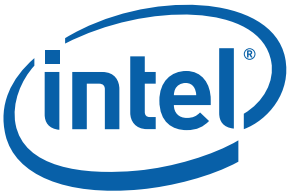


Intel® 8 Series Chipset Family - Intel® Management Engine Firmware 9.0

1.5MB Firmware Bring Up Guide

September 2013

Revision 1.0

Intel Confidential

Table of Contents

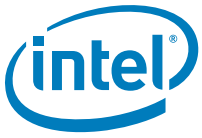
1 Introduction 7
1.1 Related Documentation 7
1.2 Intel® ME FW Features 7
1.3 Prerequisites 8
1.4 Acronyms and Definitions 8
1.4.1 General 8
1.4.2 Intel® Management Engine 9
1.4.3 System States and Power Management 10
1.5 Reference Documents 11
1.6 Format and Notation 11
1.7 Kit Contents 12
1.8 External Hardware Requirements for Bring Up 15

2 Image Creation: Flash Image Tool (FITC) 16
2.1 Start FITC and Set Up The Build Environment 16
2.2 Configure PCH Silicon Stepping 20
2.3 Set Up SPI Flash Regions 20
2.4 Set Up Descriptor and SPI Flash Device(s) 23
2.4.1 Set Up Soft-Straps 29
2.5 Configure PCH Silicon SKU 40
2.6 Intel®ME FW Feature Configuration 41
2.6.1 Firmware Features and Capabilities 41
2.6.2 Clock Control Parameters 48
2.7 Build SPI Flash Binary Image 55
2.7.1 Build SPI Flash Binary Image 55
2.7.2 Save Your Settings 55
2.7.3 Protect Saved Configuration XML File 56

3 Programming SPI Flash Devices and Checking Firmware Status 58
3.1 Flash Burner/Programmer 58
3.1.1 In-Circuit SPI Flash Programming for Mobile CRB 58
3.2 Flash Programming Tool (FPT) 59
3.2.1 FPT Windows* Version 60
3.3 Checking Intel® ME Firmware Status 60
3.4 Common Bring Up Issues and Troubleshooting Table 62

A Appendix — Flash Configurations 65

B Appendix — ICC SKU Support Matrix 68
B.0.1 ICC SKU Support Matrix 68



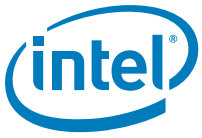
Figures

2-1 Build | Environment Variables 17
2-2 Build | Build Settings... 19
2-3 PCH Silicon Stepping Combo Box 20
2-4 SKU Manager Combo Box 40
2-5 Build | Build Image 55
2-6 Protecting FITC Configuration XML File 57
A-1 Configuration "A" — Desktop/Server/Workstation or Mobile 65
A-2 Configuration "B" — Mobile Only 66
A-3 Configuration "C" — Desktop/Server/Workstation Only 66
A-4 Configuration "D" — Mobile Only 67

Tables

1-1 Number Format Notation 11
1-2 Data Format Notation 11
1-3 Kit Contents 12
2-1 Flash Image | PDR Region 20
2-2 Flash Image | GbE Region 21
2-3 Flash Image | ME Region 22
2-4 Flash Image | BIOS Region 23
2-5 Flash Image | Descriptor Region 23
2-6 Flash Image | Descriptor Region | Descriptor Map 24
2-7 Flash Image | Descriptor Region | Component Section 25
2-8 Flash Image | Descriptor Region | Master Access Section | CPU/BIOS 26
2-9 Flash Image | Descriptor Region | Master Access Section | Manageability Engine (ME) 26
2-10 Flash Image | Descriptor Region | Master Access Section | GbE LAN 27
2-11 Flash Image | Descriptor Region | VSCC Table | W25Q64BV (example) 28
2-12 Flash Image | Descriptor Region | OEM Section 28
2-13 Flash Image | Descriptor Region | PCH Straps | PCH Strap 0 30
2-14 Flash Image | Descriptor Region | PCH Straps | PCH Strap 1 31
2-15 Flash Image | Descriptor Region | PCH Straps | PCH Strap 2 31
2-16 Flash Image | Descriptor Region | PCH Straps | PCH Strap 4 32
2-17 Flash Image | Descriptor Region | PCH Straps | PCH Strap 7 33
2-18 Flash Image | Descriptor Region | PCH Straps | PCH Strap 9 34
2-19 Flash Image | Descriptor Region | PCH Straps | PCH Strap 9 - Continued 35
2-20 Flash Image | Descriptor Region | PCH Straps | PCH Strap 10 36
2-21 Flash Image | Descriptor Region | PCH Straps | PCH Strap 11 37
2-22 Flash Image | Descriptor Region | PCH Straps | PCH Strap 15 38
2-23 Flash Image | Descriptor Region | PCH Straps | PCH Strap 17 39
2-24 Flash Image | Descriptor Region | PCH Straps | PCH Strap 17 39
2-25 Flash Image | ME Region | Configuration | ME 41
2-26 Flash Image | ME Region | Configuration | Features Supported 43

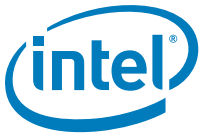
2-27 Flash Image | ME Region | Configuration | Intel® NFC Capabilities 44
2-28 Flash Image | ME Region | Configuration | Intel® Anti-Theft Technology 44
2-29 Flash Image | ME Region | Configuration | ME Debug Event Service 46
2-30 Flash Image | ME Region | Configuration | Setup and Configuration 47
2-31 Flash Image | ME Region | Configuration | Integrated Clock Controller..... 48
2-32 Flash Image | ME Region | Configuration | Integrated Clock Controller | ICC Profile 0 - Standard..... 49
2-33 Flash Image | ME Region | Configuration | Integrated Clock Controller | ICC Profile 0 - Standard | Power Management Settings 50
2-34 Flash Image | ME Region | Configuration | Integrated Clock Controller | ICC Profile 0 - Standard | PCI and Flex Clock Settings..... 51
2-35 Flash Image | ME Region | Configuration | Integrated Clock Controller | ICC Profile 0 - Standard | DMI and PCIe Clock Settings 52
2-36 Flash Image | ME Region | Configuration | Integrated Clock Controller | ICC Profile 0 - Standard | Clock Range Definition Records..... 53
2-37 Flash Image | ME Region | Configuration | Integrated Clock Controller | ICC Profile 0 - Standard | Clock Enables Masks 54
2-38 Flash Image | ME Region | Configuration | Integrated Clock Controller | ICC Profile 0 - Standard | Hardware Registers..... 55
3-1 Jumper Settings for Mobile CRB SPI Flash Programming..... 58
3-2 Common Bring Up Issues and Troubleshooting Table 62
..... 63
3-3 Feature Default Settings by Intel® 8 Series Chipset Family SKU (Desktop)..... 63
3-3 64
3-4 Feature Default Settings by Intel® 8 Series Chipset Family SKU (Mobile) 64
B-1 68



Revision History

Revision	Description	Date
1.0	Final Release: See change bars on the left side of the page.	September 2013

§ §



1 Introduction

This document covers the Intel® Management Engine Firmware (Intel® ME) 8.0 - 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 **Wellsburg SPI Programming Guide** and Appendix A. Once the SPI Flash image is built, it will be programmed to the target Intel® 8 Series Chipset Family 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.

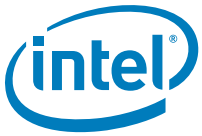
1.1 Related Documentation

CDI: Kit# 509296 - Intel® Ethernet Network Connections I217-LM - LAN Software Drivers -- LAN Access Division (LAD) - Version V10.0C00104 TIC: 272857. Alpha 2 Release providing support for our new Intel® Ethernet Connection I217-LM.

1.2 Intel® ME FW Features

This firmware release includes the following applications:

- Platform Clocks – Tune Intel® 8 Series Intel® C610 Chipset Family 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.



1.3 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 Intel® 8 Series Chipset Family based platform, this document will highlight any changes that must be imposed onto the bring up steps accordingly.

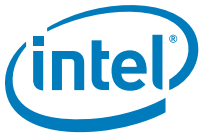
This document makes only the following limited assumptions regarding hardware:

- The platform is Intel® 8 Series Chipset Family based
- The platform is equipped with one or more SPI Flash devices with a total capacity sufficient for storing all relevant firmware images.

1.4 Acronyms and Definitions

1.4.1 General

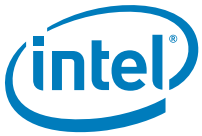
Acronym or Term	Definition
API	Application Programming Interface
ASCII	American Standard Code for Information Interchange
BIOS	Basic Input Output System
CPU	Central Processing Unit
DIMM	Dual In-line Memory Module
DLL	Dynamic Link Library
DMI	Direct Media Interface
EC	Embedded Controller
EEPROM	Electrically Erasable Programmable Read Only Memory
FDI	Flexible Display Interface
FW	Firmware
GbE	Gigabit Ethernet
HECI	Host Embedded Controller Interface (aka Intel® MEI)
IBV	Independent BIOS Vendor
ID	Identification
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)
IMSS	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



Acronym or Term	Definition
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
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
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

1.4.2 Intel® Management Engine

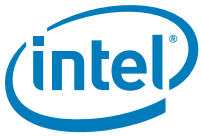
Acronym or Term	Definition
3PDS	3rd Party Data Storage
Agent	Software that runs on a client PC with OS running
Intel® AT	Intel® Anti-Theft Technology (Intel® AT)
End User	The person who uses the computer (either Desktop or Mobile). In corporate, the user usually does not have an administrator privileges.
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.



Acronym or Term	Definition
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 PCH
MECI	ME-VE Communication Interface
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 SOAP/XML 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

1.4.3 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.



1.5 Reference Documents

Document	Doc Number/ Location*
Shark Bay Desktop and Denlow-WS Platform - Design Guide - Rev. 1.0	486711 / IBL
Shark Bay Mobile Platform Design Guide	30600 / IBL
Intel® Management Engine (Intel® ME) and Embedded Controller Interaction for Shark Bay Platform	496741/ IBL
RS – Intel® Management Engine BIOS Writers Guide	493768 / IBL
[Maho Bay / Chief River / Carlow] Platforms - Intel® Management Engine (Intel® ME) 8.0 - 1.5 MB SKU Firmware for Intel® 8 Series Chipset- Compliancy and Testing Guide -Rev. 0.8	493797/ IBL

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

1.6 Format and Notation

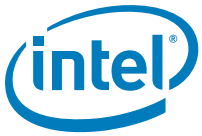
The formats and notations used within this document model are those typically used by BIOS vendors. This section describes the formatting and the notations that will be followed in this document.

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



1.7 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
1.5MB FW Getting Started Guide.pdf	This document provides an overview for using Intel® ME firmware.
Intel® 8 Series Chipset FamilyWellsburg 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]	
GRND13.R01.rom	BIOS image only for Intel CRB. This BIOS image works for both desktop and mobile CRBs. **For other Intel® 8 Series Chipset Family based platforms, a custom BIOS image will be required.**
[GbE]	
NAHUM6_CLARKSVILLE_DESKTOP_12.bin	Intel® LAN PHY firmware image. This image is for desktop platforms only.
NAHUM6_CLARKSVILLE_MOBILE_11.bin	Intel® LAN PHY firmware image. This image is for mobile platforms only.
[ME]	
ME9.0_1.5M_PreProduction.bin.bin	Intel® ME firmware image (**Non Production FW**) - supports **unfused Intel® 8 Series Chipset Family** PCH steppings: • Unfused WBG (Super SKU) **Note: For PAVP Testing**, you must match Production FW with Production Part and Non Production FW with Non Production Parts.
ME9.0_1.5M_Production.bin.bin	Intel® ME firmware image (**Production FW**) - supports **fused** and **unfused Intel® 8 Series Chipset Family** PCH steppings: • Unfused PPT ES0 (B0 Super SKU) • Fused PPT Pre-QS and QS **Note: For PAVP Testing**, you must match Production FW with Production Part and Non Production FW with Non Production Parts.
[Installers]	
Intel® ME SW Installation Guide.pdf	Intel®ME SW Installation Guide
[ME_SW]	
Setup.exe	Install executable (non-InstallShield) of Intel® ME Drivers for Windows* OS. See readme.txt for more information.
[ME_SW_IS]	
ME_SW_IS.zip	Zip containing InstallShield* files of Intel® ME Drivers for Windows* OS. See readme.txt in previous directory for more information.

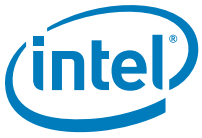


Table 1-3. Kit Contents (Sheet 2 of 3)

File or [Directory]	Content Description
[Tools]	
[ICC_Tools]	
Intel(R) ME Firmware Integrated Clock Control (ICC) Tools User Guide.pdf	ICC Tools User Guide
[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]	
Open Watcom Public License.pdf	Sybase Open Watcom Public License version 1.0 document.
System Tools User Guide.pdf	System Tools User Guide
Tools_Version.txt	Tools version information
[Flash Image Tool]	
fitc.exe	Flash Image Tool (FITC)
fitc.ini	Configuration file for FITC
fitctmpl.xml	FITC Tool XML file
newfiletmpl.xml	FITC Configuration XML file
vsccommn.bin	Binary containing the supported SPI parts
VSCCommn_bin Content.pdf	Documentation listing the SPI parts supported by vscccommn.bin
[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]	
fparts.txt	List of supported SPI Flash devices with specific Flash parameters
fptw64.exe	Flash Programming Tool (FPT) for Windows* (64-bit) OS
[FWUpdate]	

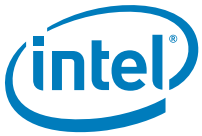


Table 1-3. Kit Contents (Sheet 3 of 3)

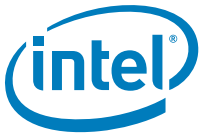
File or [Directory]	Content Description
[EFI]	
FWUpdLcl.efi	FW Update Tool (EFI version)
[Local-DOS]	
FWUpdLcl.exe	FW Update Tool (DOS version)
[Local-Win]	
FWUpdLcl.exe	FW Update Tool (Windows* version 32bit)
[Local-Win64]	
FWUpdLcl64.exe	FW Update Tool (Windows* version 64bit)
[MEInfo]	
[DOS]	
MEInfo.exe	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
VSCCommn_bin Content.pdf	Documentation listing the SPI parts supported by vscccommn.bin
[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
VSCCommn_bin Content.pdf	Documentation listing the SPI parts supported by vscccommn.bin
[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
VSCCommn_bin Content.pdf	Documentation listing the SPI parts supported by vscccommn.bin

1.8 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.

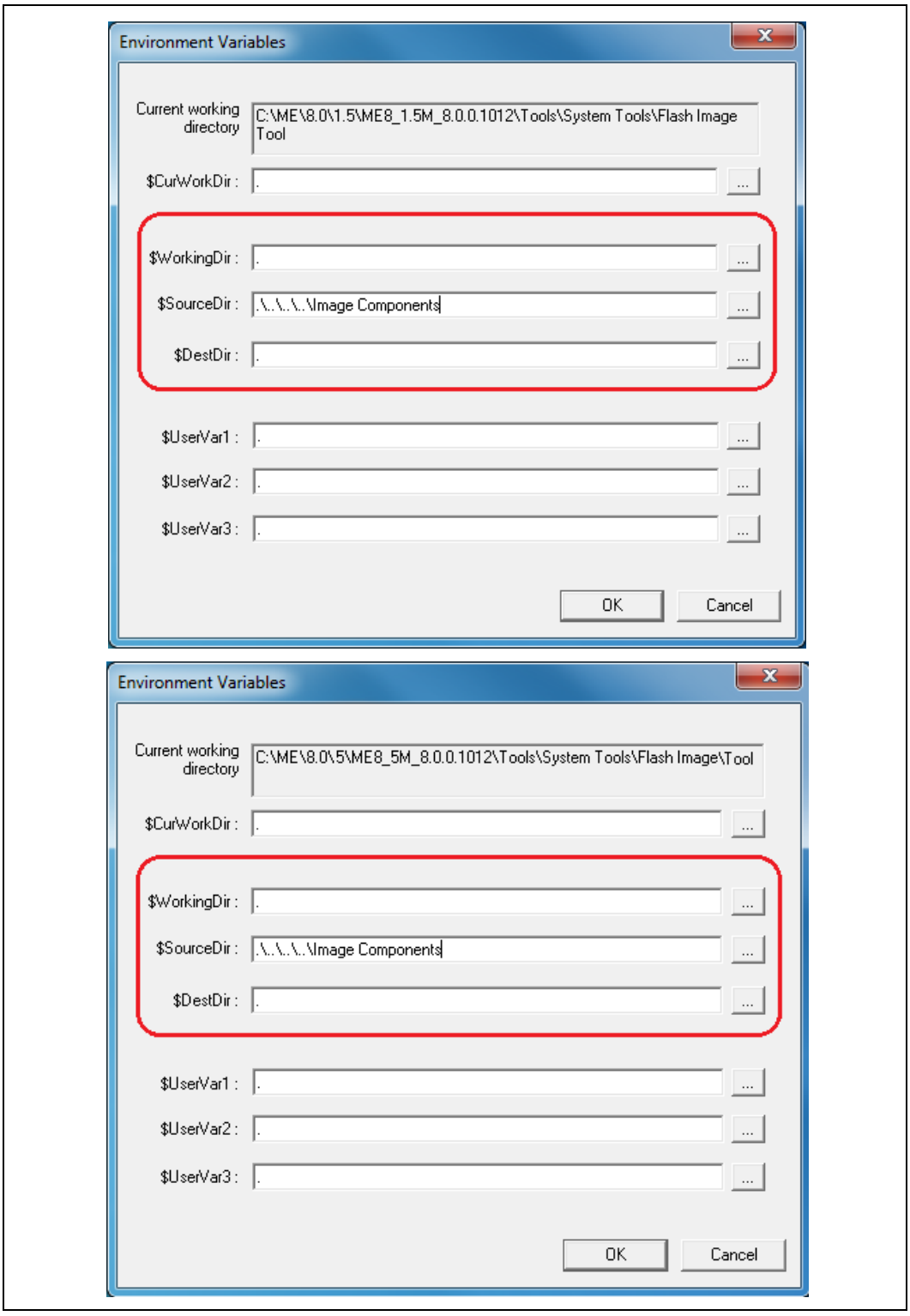
Note: The FITC Tool may be updated throughout the release cycles. As a general rule, please ensure you use the tools, images and other content from the same kit and refrain from using different version tools.

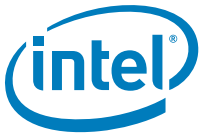
After this SPI Flash image is created, it will need to be burned onto the target platform's SPI Flash device(s). Section 3, "Programming SPI Flash Devices and Checking Firmware Status" later in this document provides steps to do this.

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 1.7). 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

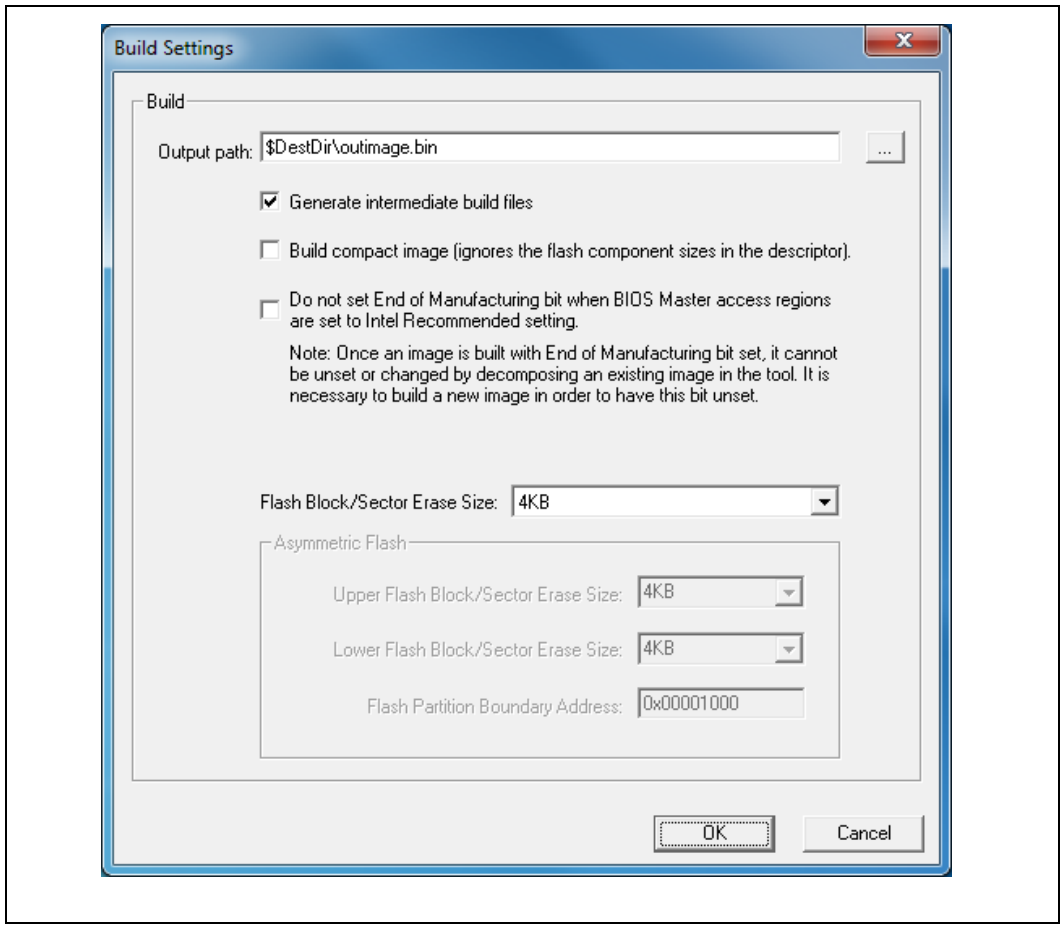




3. Click **OK** to apply your changes.

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. Change the **Flash Block/Sector Erase Size** as appropriate for your SPI flash part(s). Click **OK** to apply your changes.

Figure 2-2. Build | Build Settings...

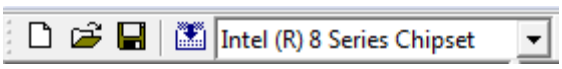


5. In the main menu select **File | Open...**. In the Open dialog that appears navigate to **[root]\Tools\System Tools\Flash Image Tool**. Click on **newfiletmpl.xml** and click **OK**.

2.2 Configure PCH Silicon Stepping

Leave the **PCH Silicon Stepping Combo Box** at its default value of **Intel® 8 Series Chipset**.

Figure 2-3. PCH Silicon Stepping Combo Box



2.3 Set Up SPI Flash Regions

Table 2-1. Flash Image | PDR Region

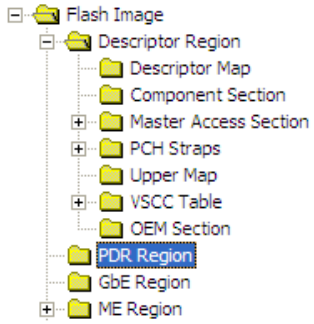
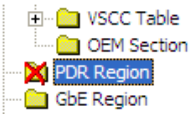
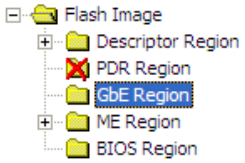
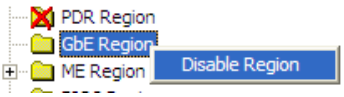
Location	Parameter	CRB Set To	Settings for Any Platform
Follow navigation tree below: • Select the Flash Image • Select **Flash Image | PDR Region** • Set the parameters in the **PDR Region** section as shown 	PDR Region Length	PDR Region is disabled	Displays Region size information when **Binary input 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	
	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	true	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**.			

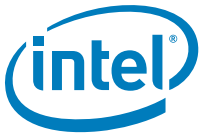
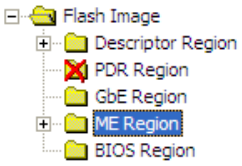


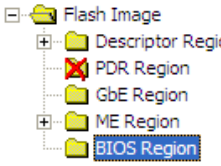
Table 2-3. Flash Image | ME Region

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	0x0082 TAYLOR	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 FWUpdlcl.

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

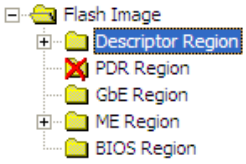
Location	Parameter	CRB Set To	Settings for Any Platform
Follow navigation tree below: • Select the **Flash Image** tab. Select **Flash Image | Descriptor Region** • Set the parameters in the **Descriptor Region** section as shown 	**Yellow means custom settings may be required, otherwise use CRB setting.**		
	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

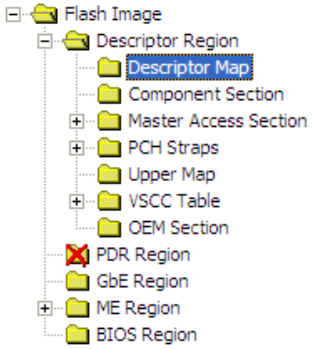
Location	Parameter	CRB Set To	Settings for Any Platform
Follow navigation tree below: • Select the **Flash Image** tab • Select **Flash Image | Descriptor Region | Descriptor Map** • Set the parameters in the **Descriptor Map** section as shown 	**Yellow means custom settings may be required, otherwise 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
	Component base address	0x03	Read Only, See SPI programming Guide for details.
	Number of PCH straps	20	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

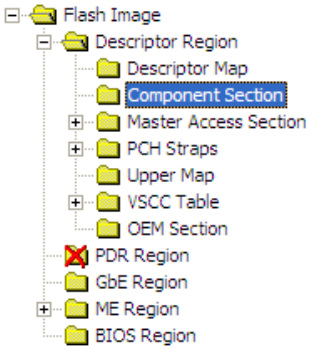
Location	Parameter	CRB Set To	Settings for Any Platform
Follow navigation tree below: • Select the **Flash Image** tab. Select F**lash Image | Descriptor Region | Component Section** • Set the parameters in the **Component Section** section as shown 	**Yellow means custom settings may be required, otherwise 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 PCH 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	
	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 *LPT SPI programming Guide* for more details.
	Invalid instruction 3	0	Opcode entered here will not be allowed by the PCH's SPI controller for HW sequencing. See *LPT SPI programming Guide* for more details. **0** = no instruction is specified
	Invalid instruction 2	0	
	Invalid instruction 1	0	
	Invalid instruction 0	0	
	Invalid instruction 7	0	
	Invalid instruction 6	0	
	Invalid instruction 5	0	
	Invalid instruction 4	0	

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

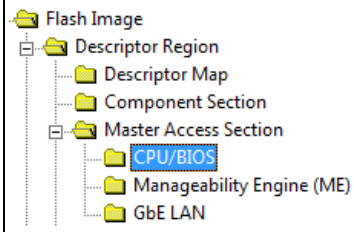
Location	Parameter	CRB Set To	Settings for Any Platform
Follow navigation tree below: • Select the **Flash Image** tab • Select **Flash Image | Descriptor Region | Master Access Section | CPU/BIOS** • Set the parameters in the **CPU/BIOS** section as shown 	**Yellow means custom settings may be required.**		
	PCI Bus ID	0	
	PCI Device ID	0	
	PCI Function ID	0	
	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 **0x1B** = Production with access to PDR **0xFF (default)** = Non-production/debug platform
	Write Access	0xFF	Controls write access by BIOS. Structure is identical to **Read access** parameter. **0x0A** = Production platform **0x1A** = Production with access to PDR **0xFF (default)** = Non-production/debug platform

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

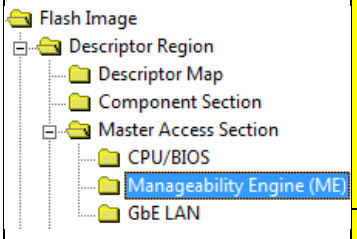
Location	Parameter	CRB Set To	Settings for target platform
Follow navigation tree below: • Select the **Flash Image** tab • Select **Flash Image | Descriptor Region | Master Access Section | Manageability Engine (ME)** • Set the parameters in the **Manageability Engine (ME)** section as shown 	**Yellow means custom settings may be required.**		
	PCI Bus ID	0	
	PCI Device ID	0	
	PCI Function ID	0	
	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

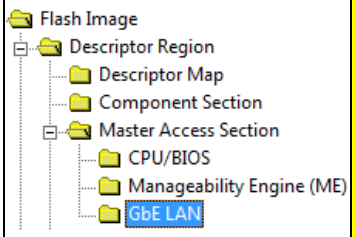
Location	Parameter	CRB Set To	Settings for Any Platform
Follow navigation tree below: • Select the **Flash Image** tab • Select **Flash Image | Descriptor Region | Master Access Section | GbE LAN** • Set the parameters in the **GbE LAN** section as shown 	**Yellow means custom settings may be required.**		
	PCI Bus ID	1	1
	PCI Device ID	3	3
	PCI Function ID	0	0
	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)

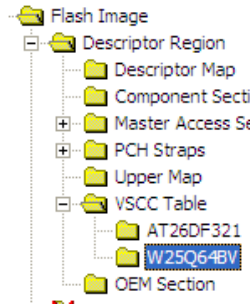
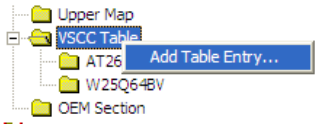
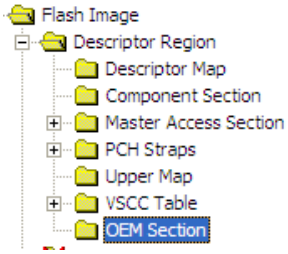
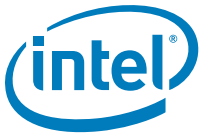
Location	Parameter	CRB Set To	Settings for Any Platform
Follow navigation tree below: • Select **Flash Image | Descriptor Region | VSCC Table |** • Set the parameters for the Atmel 4-MB SPI part in the **W25Q64BV** section as shown  • Right click VSSC Table to add a Flash entry. 	**Yellow means custom 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 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® *LPT SPI programming Guide* describes the 32-bit VSCC register value. Default is **0x00**.
	Device ID 0	Intel® CRBs use **0x40**	Use values obtained by using Vendor Serial Flash datasheet and Intel® *LPT SPI programming Guide* Default is **0x00**.
	Device ID 1	Intel® CRBs use **0x17**	Use values obtained by using Vendor Serial Flash datasheet and Intel® *LPT SPI programming Guide* Default is **0x00**.

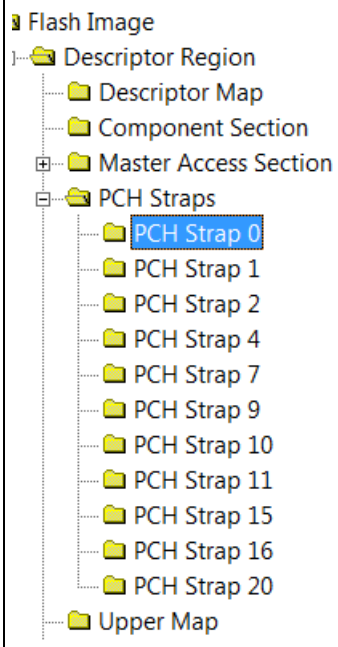
Table 2-12. Flash Image | Descriptor Region | OEM Section

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

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** = Only required if target platform has Intel wired LAN and PCH GP12 is used as LAN_PHYPC for Intel LAN. **GPIO12 default is General Purpose (GP) output** = PCH GP12 is used as General Purpose Input/Output (GPIO) pin. Must be **General Purpose output** if using Third-party LAN and no Intel wired LAN is present. **Note:** Please consult with the target hardware designer to determine this setting.
	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	Mobile and Desktop CRB uses **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.

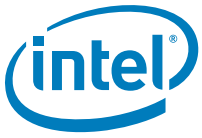


Table 2-14. Flash Image | Descriptor Region | PCH Straps | PCH Strap 1

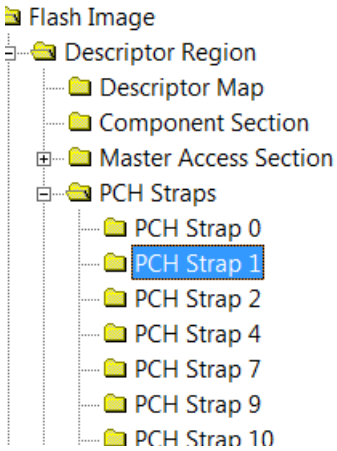
Location	Parameter	CRB Set To	Settings for Any Platform
Follow navigation tree below: • Select the **Flash Image** tab • Select **Flash Image | Descriptor Region | PCH Straps | PCH Strap 1** • Set the parameters in the **PCH Strap 1** section as shown 	**Yellow means custom settings may be required.**		
	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 2-15. Flash Image | Descriptor Region | PCH Straps | PCH Strap 2

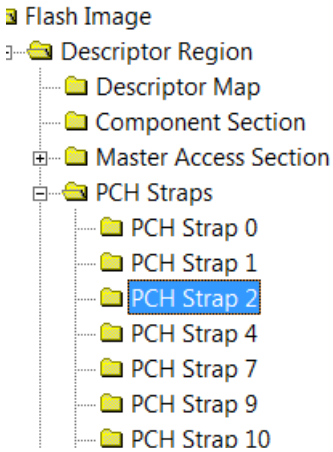
Location	Parameter	CRB Set To	Settings for Any Platform
Follow navigation tree below: • Select the **Flash Image** tab • Select **Flash Image | Descriptor Region | PCH Straps | PCH Strap 2** • Set the parameters in the **PCH Strap 2** section as shown 	**Yellow means custom settings may be required.**		
	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 2-16. Flash Image | Descriptor Region | PCH Straps | PCH Strap 4

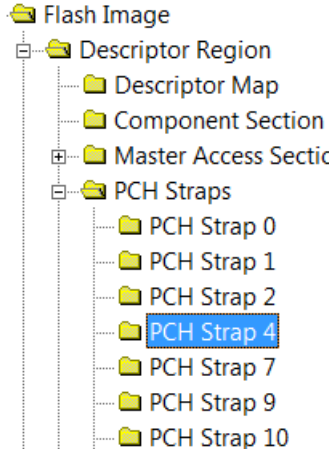
Location	Parameter	CRB Set To	Settings for Any Platform
Follow navigation tree below: • Select the **Flash Image** tab • Select **Flash Image | Descriptor Region | PCH Straps | PCH Strap 4** • Set the parameters in the **PCH Strap 4** 	**Yellow means custom settings may be required.**		
	GbE PHY SMBus 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
	SATA Port 5 PCIe Port 2 Mode	Statically assigned to SATA Port 5	If this soft strap is set to "11" then GPIO49 native mode is SATA5_PCIE2#, otherwise the native mode is SATA5GP. This soft strap only has effect if it is allowed by the "SATA Port 5 PCIe Port 2 Mode" fuse. **00 :** Statically assigned to SATA Port 5 **01 :** Statically assigned to PCIe Port 2 **11 :** Assigned based on the native mode of GPIO49 pin. If the native GPIO49 pin is a „1", then it is assigned to SATA Port 5, else it is assigned to PCIe Port 2.

Table 2-17. Flash Image | Descriptor Region | PCH Straps | PCH Strap 7

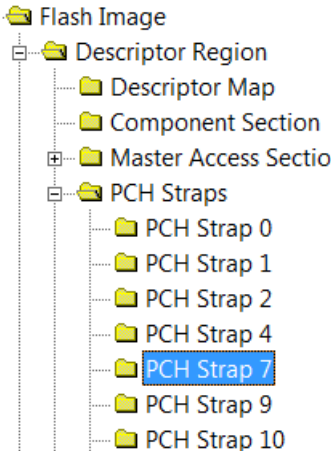
Location	Parameter	CRB Set To	Settings for Any Platform
Follow navigation tree below: • Select the **Flash Image** tab. • Select **Flash Image | Descriptor Region | PCH Straps | PCH Strap 7** • Set the parameters in the **PCH Strap 7** 	Intel® ME SMBus Subsystem Vendor & Device ID for ASF2	0x00000000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

Table 2-18. Flash Image | Descriptor Region | PCH Straps | PCH Strap 9

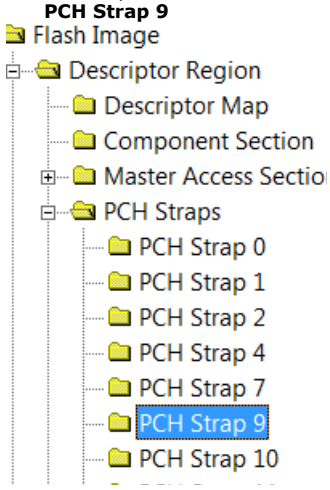
Location	Parameter	CRB Set To	Settings for Any Platform
Follow navigation tree below: • Select the **Flash Image** tab • Select **Flash Image | Descriptor Region | PCH Straps | PCH Strap 9** • Set the parameters in the **PCH Strap 9** 	**Yellow means custom settings may be required.**		
	TEMP_ALERT# or SML1ALERT# Select	TEMP_ALERT#	Treat as reserved.
	Subtractive Decode Agent Enable	true	**true** = A PCI Bridge chip is connected to the PCH **false (default)** = A PCI Bridge chip is not connected to the PCH ***Note:*** Please consult the target hardware designer to determine this setting
	Intel® PHY Over PCI Express Enable	true	**true (default)** = Intel LAN is present **false** = Third-party LAN is present
	Intel® PHY PCIe Port Select	**Desktop** set to 010:Port 3 **Mobile** set to 101:Port 6	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 1 **001** = Port 2 **010** = Port 3 **011** = Port 4 **100** = Port 5 **101** = Port 6 **110** = Port 7 **111** = Port 8
	DMI Lane Reversal	false	***Note:*** Please consult the target hardware designer to determine this setting When using Small Form Factor CRB platforms set this value to '**true**'.
	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 2	00: 4x1 Ports 5-8 (x1)	***Note:*** Please consult the target hardware designer to determine this setting
	PCIe Port Configuration 1	00: 4x1 Ports 1-4 (x1)	***Note:*** Please consult the target hardware designer to determine this setting

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

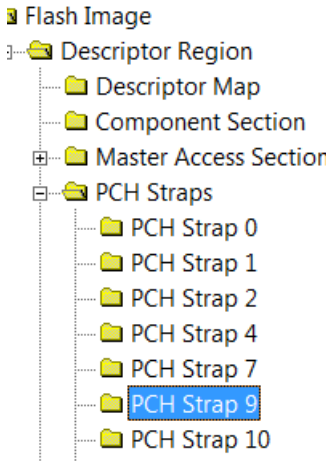
Location	Parameter	CRB Set To	Settings for Any Platform
Follow navigation tree below: • Select the **Flash Image** tab • Select **Flash Image | Descriptor Region | PCH Straps | PCH Strap 9** • Set the parameters in the **PCH Strap 9** 	**Yellow means custom settings may be required.**		
	USB3 Port 2 PCIe Port 1 Mode	**Desktop** set to PCIe Lane 1 is statically assigned to USB3 Port 2 **Mobile** set to PCIe Lane 2 is statically assigned to PCI Express (or GbE)	This soft strap set the dafault value of the USB3 PCI Express Port 1 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 2 Reserved. Autodetect of USB3/PCIe is no supported PCIe Lane 1 is dynamically assigned to PCI Express or USB3 Port 2 based on the ExpressCard USB3# select pin on GPIO71
	USB3 Port 3 PCIe Port 2 Mode	**Desktop** set to PCIe Lane 2 is statically assigned to USB3 Port 3 **Mobile** set to 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 2 is statically assigned to PCI Express (or GbE) PCIe Lane 2 is statically assigned to USB3 Port 3 Reserved. Autodetect of USB3/PCIe is no supported PCIe Lane 2 is dynamically assigned to PCI Express or USB3 Port 3
	SATA Port 4 PCIe Port 1 Mode	Statically assigned to SATA Port 4	If this soft strap is set to 'Assigned based on the native mode of GPIO16 pin.' then the GPIO16 native mode is SATA4_PCIE1# otherwise native mode is SATA4GP: Statically assigned to SATA Port 4 Statically assigned to PCIe Port 1 Assigned based on the native mode of GPIO16 pin. **Note:** This soft strap only has effect if it is allowed by the 'SATA Port 4 PCIe Port 1 Mode' fuse.

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

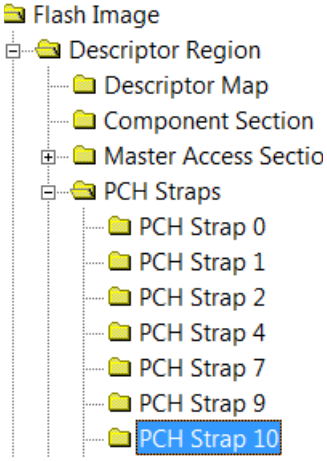
Location	Parameter	CRB Set To	Settings for Any Platform
Follow navigation tree below: • Select the **Flash Image** tab • Select **Flash Image | Descriptor Region | PCH Straps | PCH Strap 10** • Set the parameters in the **PCH Strap 10** section as shown 	**Yellow means custom settings may be required.**		
	Note: ICC settings from PCH Strap 10 is removed and are moved to **Flash Image | ME Region | Configuration| Integrated Clock Controller.**		
	ME boot from Flash	false (grayed out)	**false (default)** = No ME Region binary loaded, or ME Region binary does not contain ME ROM bypass image **Note: On B0 and later PCH stepping parts this setting should be set to 'false'**
	Reserved	false	This value must be set to '**false**'
	ME Debug SMBus Emergency Mode Enable	Disables ME Debug SMBus Emergency Mode	**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 PCH pin CL_RST1#. **true** = ME reset assert/de-assert can be observed on PCH pin CL_RST1# **false** = CL_RST1# usage is available as per *Intel® C610 Series Chipset Family 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.

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

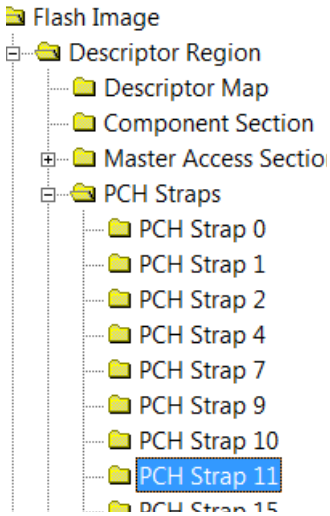
Location	Parameter	CRB Set To	Settings for Any Platform
Follow navigation tree below: • Select the **Flash Image** tab • Select **Flash Image | Descriptor Region | PCH Straps | PCH Strap 11** • Set the parameters in the **PCH Strap 11** section as shown 	**Yellow means custom settings may be required.**		
	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 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 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 15

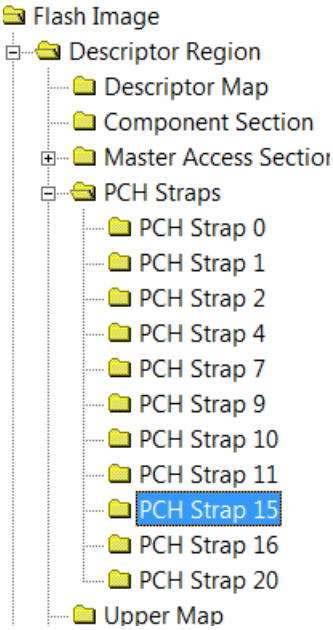
Location	Parameter	CRB Set To	Settings for Any Platform
Follow navigation tree below: • Select the **Flash Image** tab • Select **Flash Image | Descriptor Region | PCH Straps | PCH Strap 15** • Set the parameters in the **PCH Strap 15** section as shown 	**Yellow means custom settings may be required.**		
	PCIe Power Stable Timer Enable	t205b timer is disabled	This strap controls the behavior of the t205b timer. t205b timer is disabled PCH will count 99ms from PWROK assertion before PLTRST# is de-asserted ***Note:*** See *Intel® 8 Series/C220 series Chipset Family EDS* for details
	SLP_LAN#/GPIO29 Select	false	**true =** Enables GPIO29 and disables SLP_LAN# functionality. **false** =Set to false to use have GPIO behave as SLP_LAN#. ***Note:*** This field is read only if Intel integrated LAN is disabled. See Table 2-2.
	t1001 Timing	1 ms	This setting controls t1001 timing from CPUWRGD assertion to SUS_STAT#. **1ms (default)** **30us** **5ms** **2ms** ***Note:*** See *Intel® 8 Series/C220 series Chipset Family 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 *Intel® 8 Series/C220 series Chipset Family EDS* for details
	Intel®Integrated LAN Enable		Treat as reserved. This field is read only. and is via the GbE parameter
	Deep Sx Platform	false	Treat as reserved. This field is read only and is set via PCH Strap 10

Table 2-23. Flash Image | Descriptor Region | PCH Straps | PCH Strap 17

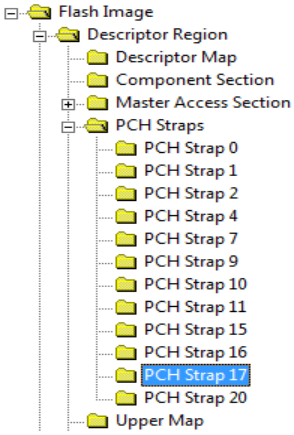
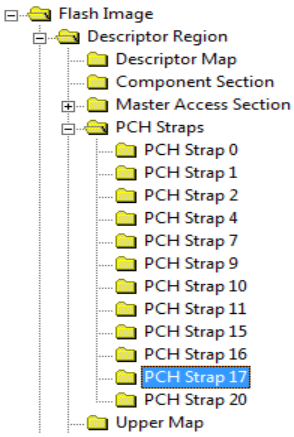
Location	Parameter	CRB Set To	Settings for Any Platform
Follow navigation tree below: • Select **Flash Image | Descriptor Region | PCH Straps | PCH Strap 17** • Set the parameters in the **PCH Strap 17** section as shown 	**Yellow means custom settings may be required.**		
	BTM/FCIM Select	Full Clock Integrated Mode	If PCH clock boot mode is specified by soft strap then this parameter specifies whether the PCH clocks boot in Full Clock Integrated Mode (FCIM) or Buffer Through Mode (BTM). **NOTE:** Buffer Through Mode (BTM) is **NOT** POR mode supported by **Intel® 8 Series Chipset Family** and it will not be validated by Intel.

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 PCH clock boot mode is specified by soft strap then this parameter specifies whether the PCH clocks boot in Full Clock Integrated Mode (FCIM) or Buffer Through Mode (BTM).

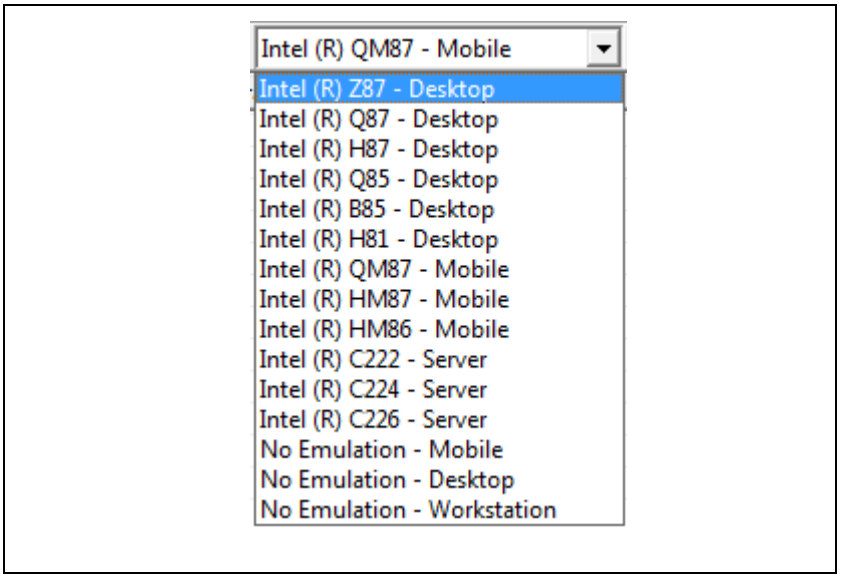
2.5 Configure PCH Silicon SKU

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:

- Intel® 8 Series Chipset family
  - — Intel® Z87 Express Chipset
  - — Intel® Z85 Express Chipset
  - — Intel® H87 Express Chipset
  - — Intel® H81 Express Chipset
  - — Mobile Intel® HM87 Express Chipset
  - — Mobile Intel® HM86 Express Chipset

Figure 2-4. SKU Manager Combo Box



When a PCH SKU is selected in FITC, Super SKU PCH silicon will then behave as if it were the selected Production SKU PCH silicon from Intel®ME FW perspective. The SKU Manager selection option has no effect on Production SKU PCH 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 PCH. If there are issues with drivers, host software, or BIOS that do not recognize the PCH, then select the appropriate SKU with Super SKU DID.

Note: P67 must use a discrete graphics solution. Undesired behavior such as failure to boot may result if using integrated graphics.

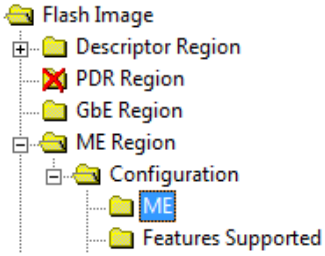
Note: Sections of FITC other than the **Features Supported** folder under **Flash Image ME| Region| Configuration** will not reflect what is disabled for the selected PCH silicon SKU and/or ME FW binary.

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).

2.6.1 Firmware Features and Capabilities

Table 2-25. 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:*** This field is read only if Power package 2 supported is enabled. ***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.

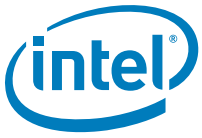
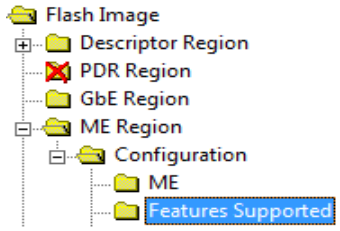


Table 2-25. Flash Image | ME Region | Configuration | ME (Sheet 2 of 2)

Location	Parameter	CRB Set To	Settings for Any Platform
	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.
	Processor Emulation	No Emulation	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 MEBx FW update option will be visible to end users. **'true'** - The 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
	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.
	Enable hash file creation	true	This enables the creation of an external hash file of the ME Region.
	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.

Table 2-26. 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 PCH SKU selected by PCH 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	
	Service Advertisement and Discovery Permanently disabled[1]	No	
	Intel® Manageability Application Enable/ Disable	Disabled	Disabled (not supported on 1.5MB FW)
Note: The Feature supported settings shown above are an example.			

Notes:

1. Services Advertisement & Discovery was previously refered to as mDNS.

Since 1.5MB FW does not support "Manageability Application" the following settings **Flash Image | ME Region | Configuration | Manageability Application**, are not applicable.

Table 2-27. Flash Image | ME Region | Configuration | Intel® NFC Capabilities

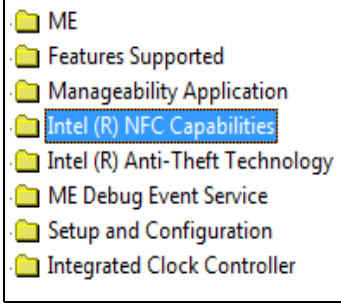
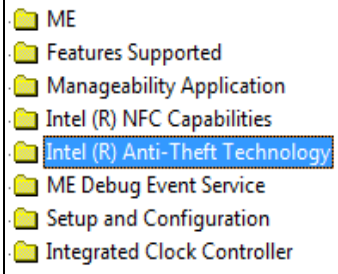
Location	Parameter	CRB Set To	Settings for Any Platform
Follow navigation tree below: • Select **Flash Image | ME Region | Configuration | Intel® NFC Capabilities** Set the parameters in the **Intel® NFC Capabilities** section as shown 	**Yellow means custom settings may be required.**		
	Near Field Communication Enabled	false	This parameter controls whether or not NFC is enabled on the platform. **true -** NFC Enabled **false -** NFC Disabled
	SMBus Address	0x5E-Intel	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	GPIO57	This parameter determines the GPIO used as IRQ line between the PCH (Intel ME FW) and the NFC module. You should set the GPIO based on the HW design of the platform. Options are: GPIO57 or GPIO74

Table 2-28. 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 	**Yellow means custom settings may be required.**		
	Allow Unsigned Assert Stolen	false	Treat as reserved.
	Intel(R) Anti-Theft BIOS Recovery Timer	Disabled	This timer will enable a 30 minute window to allow a firmware/BIOS reflash before the system is powered down.
	Flash Protection Override Policy Hard	**Allowed When AT Not Provisioned**	This option determines if the ME will enter a disabled state to allow full SPI device re-flashing when the manufacturing override jumper (HMFPRO) is set. **Always Allowed** - Full SPI re-flash will always be allowed regardless of Intel®AT enrollment state. **Allowed When AT Not Provisioned** - Full SPI re-flash allowed if Intel®AT has not been enrolled.
	Flash Protection Override Policy Soft	**Allowed When AT Not Provisioned**	This option determines if the ME will enter a disabled state via BIOS based MEI messages and allow ME only region re-flash. **Always Allowed** - Intel®ME region re-flash will always be allowed regardless of Intel®AT enrollment state. **Allowed When AT Not Provisioned** - Intel®ME region re-flash allowed if Intel®AT has not been enrolled.

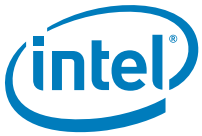
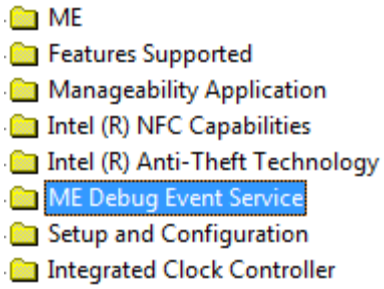
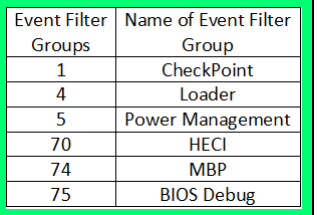


Table 2-29. Flash Image | ME Region | Configuration | ME Debug Event Service

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 - Network	false	true	Set to **true** only for platforms with Intel LAN.
	Logging Interface - SMBus	false	false	Can be set to **true** for platforms with no Intel LAN. May also be set to **true** if ME Debug logging through SMBus is desired.
	Logging Interface - Flash	true	false	**Note:** This should only be used with the Critcal filter setting options from the first column (**ME Debug Enabled SPI Logging**).
	Logging Interface - PRAM	false	false	
	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 6: **0x000F0000** Filter Group 70: **0x00000001** **Advanced (Intel LAN)** Filter Group 1: **0x00000001** Filter Group 4: **0x000003F6** Filter Group 5: **0x00000003** Filter Group 6: **0x000F0000** Filter Group 70: **0x00000001** **Advanced (SMBus)** Filter Group 1: **0x00000001** Filter Group 4: **0x000003F6** Filter Group 5: **0x00000003** Filter Group 6: **0x000F0000** Filter Group 70: **0x00000001**	 **Note:** To enable Filter groups **74** and **75** add a **1** value.

Parameter	Value
Error Filter	All
Logging Interface - Network	false
Logging Interface - SMBus	true
Logging Interface - Flash	false
Logging Interface - PRAM	false
Buffer Size	24
Buffer Mode	Buffered
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 Enable	true
Slave Address	0x56
Event Filters	Click To Edit

Basic Filter configuration:

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

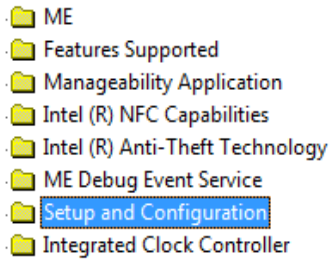
Advanced Filter configuration (LAN):

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 2-30. 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 	**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 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.

2.6.2 Clock Control Parameters

Table 2-31. Flash Image | ME Region | Configuration | Integrated Clock Controller

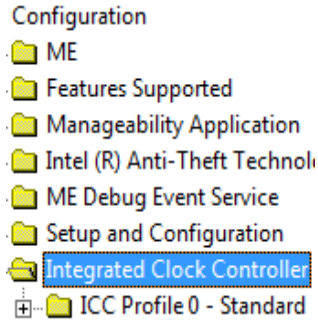
Location	Parameter	CRB Set To	Settings for Any Platform
Follow navigation tree below: • On the navigation tree to the left, select the **Flash Image | ME Region | Configuration | Intergrated Clock Controller.** 	***Note:*** ICC settings from PCH Strap 10 is removed and are moved to **Flash Image | ME Region | Configuration| Integrated Clock Controller.**		
	Default Profile Selection	ICC Profile 0 - Standard	Specifies which clock control parameter set is to be used by the final generated SPI Flash binary image by the target platform at boot time. 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 BCLK & PCIe 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 2-32. Flash Image | ME Region | Configuration | Integrated Clock Controller | ICC Profile 0 - Standard

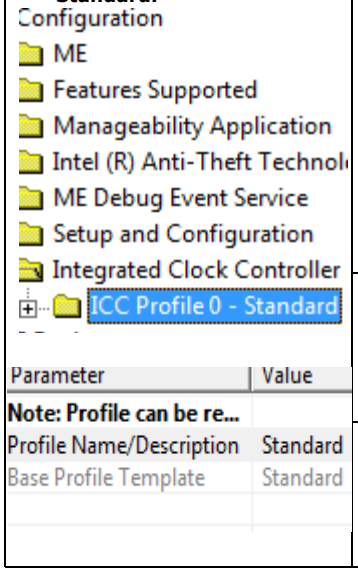
Location	Parameter	CRB Set To	Settings for Any Platform
Follow navigation tree below: • On the navigation tree to the left, select the **Flash Image | ME Region | Configuration | Intergrated Clock Controller |ICC Profile 0- Standard.** 	***Note:*** **FITC provides 4 pre- defined ICC profiles.** • **Standard:** This profile provides default settings for standard configuration, no overclocking or adaptive clocking is allowed. Platform clocks output internal and external are driven from MODDIV3. **MODDIV2 is turned off for power saving.** Default clock frequency is 100 MHz with 0.5%DownSpread. • **WiMax:** 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. Clock frequency is 99.8267MHz with spread percentage 0.26%-down spread. • **3G:** This profile provides 3G friendly configuration. MODDIV2 and MODDIV3 is turned on. Clock frequency for MODDIV2 is 98.8558MHz with 0.5% DownSpread. Clock frequency for MODDIV3 is 99.8267MHz with spread percentage 0.26%DownSpread. • **Overclocking**: This profile provides overclocking friendly configuration. clock frequency for MODDIV2 and MODDIV3 is 100 MHz with 0.5%DownSpread. This profile is used to perform BCLK/DMI overclocking using MODDIV2. ***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. 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 2-33. Flash Image | ME Region | Configuration | Integrated Clock Controller | ICC Profile 0 - Standard | Power Management Settings

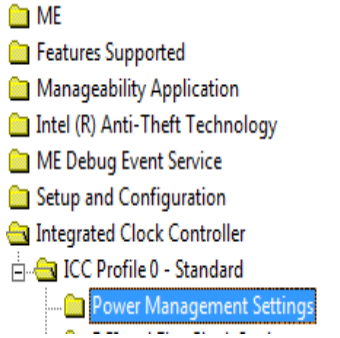
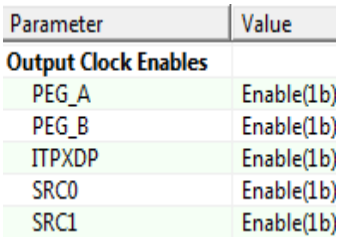
Location	Parameter	CRB Set To	Settings for Any Platform
Follow navigation tree below: • On the navigation tree to the left, select the **Flash Image | ME Region | Configuration | Intergrated Clock Controller| ICC Profile 0 - Standard| Power Management Settings**.  	Output Clock Enables	Keep defaults.	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.
	PCI Clock Power Management	Keep defaults.	This parameter controls enabling/disabling of CLKRUN support for PCI clocks. note: for Mobile platforms, it is recommended to enable CLKRUN for power saving. for Loopback PCI clock signal CLKRUN must be disabled.
	CLKREQ# Associations	Keep defaults.	This parameter controls association of dynamic CLKRQ# control with SRC(PCIe) clocks. For CRB, recommend keeping defaults for bring up with Intel® ME FW.
	Miscellaneous Power Settings	Keep defaults.	Dynamic Power Management of 96MHZ parameter controls enabling/disabling 96MHZ clock source to dynamically bring this clock down to lower power state when hardware detects idle condition. This clock source is used for 48/24Mhz flex clock, GbeTimeSync,Azalia,USB2.0 and xHCI Frame Timer. WarmRest Gating of CLKOUT_DPNS parameter controls enabling/disabling the output enable of the CLKOUT_DPNS signal during warm reset. Note: for WarmReset Gating of CLKOUT_DPNS parameter, keep default value.

Table 2-34. Flash Image | ME Region | Configuration | Integrated Clock Controller | ICC Profile 0 - Standard | PCI and Flex Clock Settings

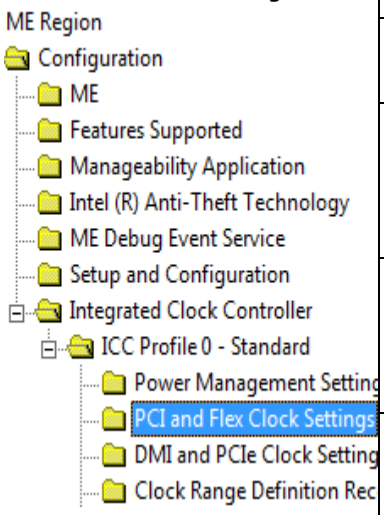
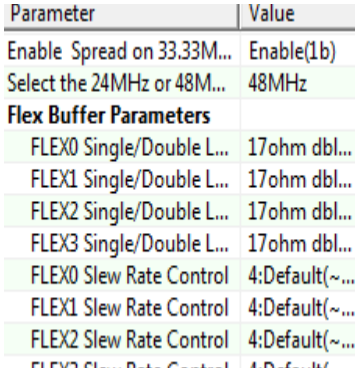
Location	Parameter	CRB Set To	Settings for Any Platform
Follow navigation tree below: • On the navigation tree to the left, select the **Flash Image | ME Region | Configuration | Intergrated Clock Controller| ICC Profile 0 - Standard|PCI and Flex Clock Settings.**  			
	Enable Spread on 33.33Mz Clock	Enable(1b)	This parameter allows to enable/disable spread spectrum support for 33MHz clock output.
	Select the 24MHz or 48MHz Clock Source	48MHz	This parameter allows output clock CLKOUT_FLEX of 24MHz or 48 MHz.
	Flex Buffer Parameters	Keep defaults	This parameter controls double/single load series resistance and slew rate for FLEX clocks. For CRB, recommend keeping defaults for bring up with Intel® ME FW.
	PCI Buffer Parameters	Keep defaults	This parameter controls double/single load series resistance and slew rate for 33MHz clocks. for CRB, recommend keeping defaults for bring up with Intel® ME FW.
	Flex Clock Source Selection	Keep defaults	This parameter controls muxing to select sources for Flex Clock outputs. Supported frequencies for Flex Clock Source are 33.33MHz, 14.31818MHz and 24/48MHz. For CRB, recommend keeping defaults for bring up with Intel® ME FW.

Table 2-35. Flash Image | ME Region | Configuration | Integrated Clock Controller | ICC Profile 0 - Standard | DMI and PCIe Clock Settings

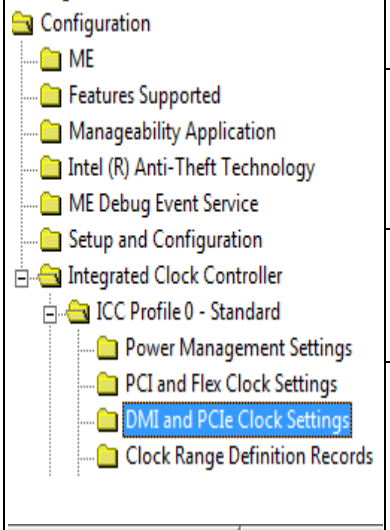
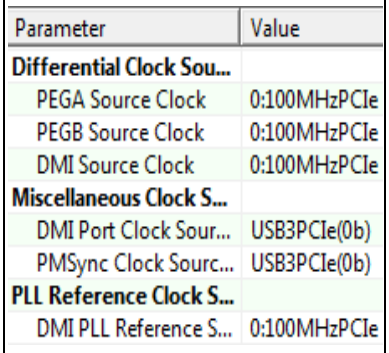
Location	Parameter	CRB Set To	Settings for Any Platform
Follow navigation tree below: • On the navigation tree to the left, select the **Flash Image | ME Region | Configuration | Intergrated Clock Controller| ICC Profile 0 - Standard|DMI and PCIe Clock Settings.** •  	Differential Clock Source Selection	keep defaults	This parameter controls source Clock selection for external clocks like PEGA, PEGB and DMI. **note:** Recommended to use default value based on pre-defined profile selection.
	Miscellaneous Clock Source Selection	keep defaults	This parameter controls source for internal DMI clock. **note:** Recommended to use default value based on pre-defined profile selection.
	PLL Reference Clock Source Selection	keep defaults	This parameter controls reference clock selection for PLL. **note:** Recommended to use default value based on pre-defined profile selection.
	DMI Clock Settings	keep defaults	This parameter controls enabling/ disabling DMI clock source. **note:** Recommended to use default value based on pre-defined profile selection.
	PCIe Clock Settings	keep defaults	This parameter controls enabling/ disabling PCIe clock source. **note:** Recommended to use default value based on pre-defined profile selection.

Table 2-36. Flash Image | ME Region | Configuration | Integrated Clock Controller | ICC Profile 0 - Standard | Clock Range Definition Records

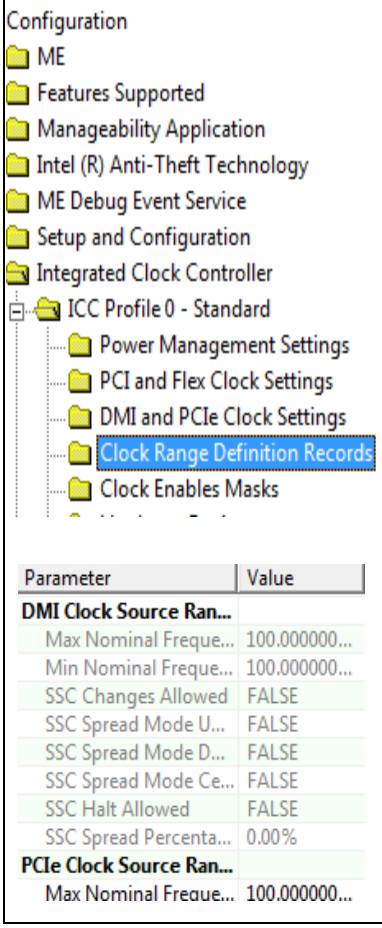
Location	Parameter	CRB Set To	Settings for Any Platform
Follow navigation tree below: • On the navigation tree to the left, select the **Flash Image | ME Region | Configuration | Intergrated Clock Controller| ICC Profile 0 - Standard|Clock Range Definition Record.** ***Note:*** Max Nominal Frequency 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.  	DMI Clock Source Range Limit(MODDIV2)	Keep defaults	This parameter controls Max nominal and Min nominal frequency as well as Max spread % range for MODDIV2. **Note:** Based on pre-defined ICC profile used, This option may not be available.
	PCIe Clock Source Range Limit(MODDIV3)	Keep defaults	This parameter controls Max nominal and Min nominal frequency as well as Max spread % range for MODDIV3.

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

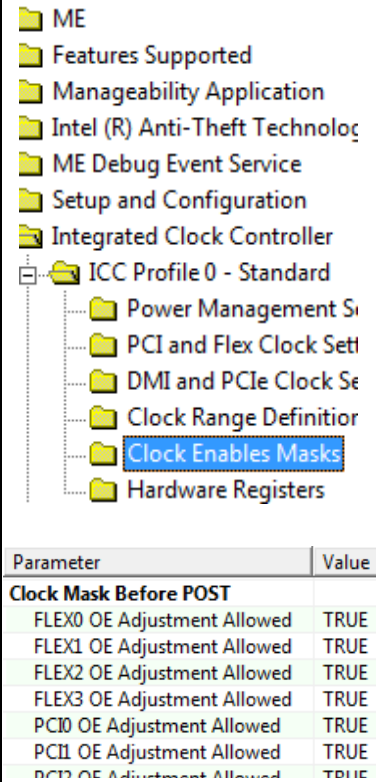
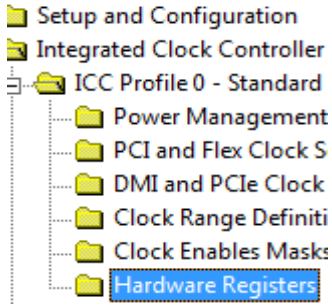
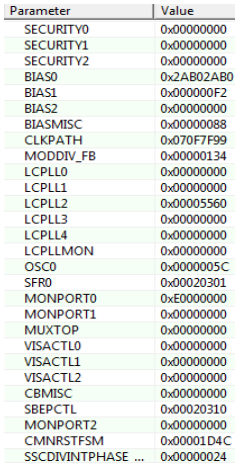
Location	Parameter	CRB Set To	Settings for Any Platform
Follow navigation tree below: • On the navigation tree to the left, select the **Flash Image | ME Region | Configuration | Intergrated Clock Controller| ICC Profile 0 - Standard|Clock Enables Masks** •  	Clock Mask Before POST	keep defaults	This 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 2-38. Flash Image | ME Region | Configuration | Integrated Clock Controller | ICC Profile 0 - Standard | Hardware Registers

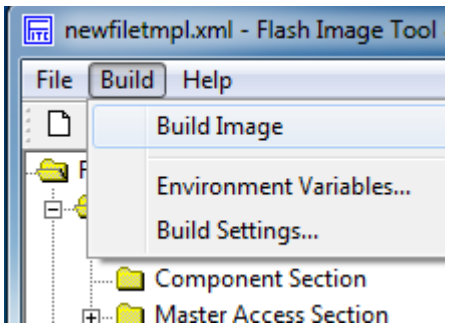
Location	Parameter	CRB Set To	Settings for Any Platform
Follow navigation tree below: • On the navigation tree to the left, select the **Flash Image	ME Region	Configuration	Intergrated Clock Controller	ICC Profile 0 - Standard	Hardware Registers.** 		Keep Defaults	This section displays all ICC registers. 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

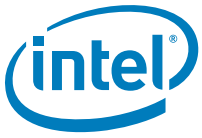
In the main menu select **Build | Build Image**. The image will be saved in the directory specified by **$DestDir** parameter and will be named **outimage.bin**, unless the default **Output Directory** in **Build | Build Settings** was changed (see Section 2.1).

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:

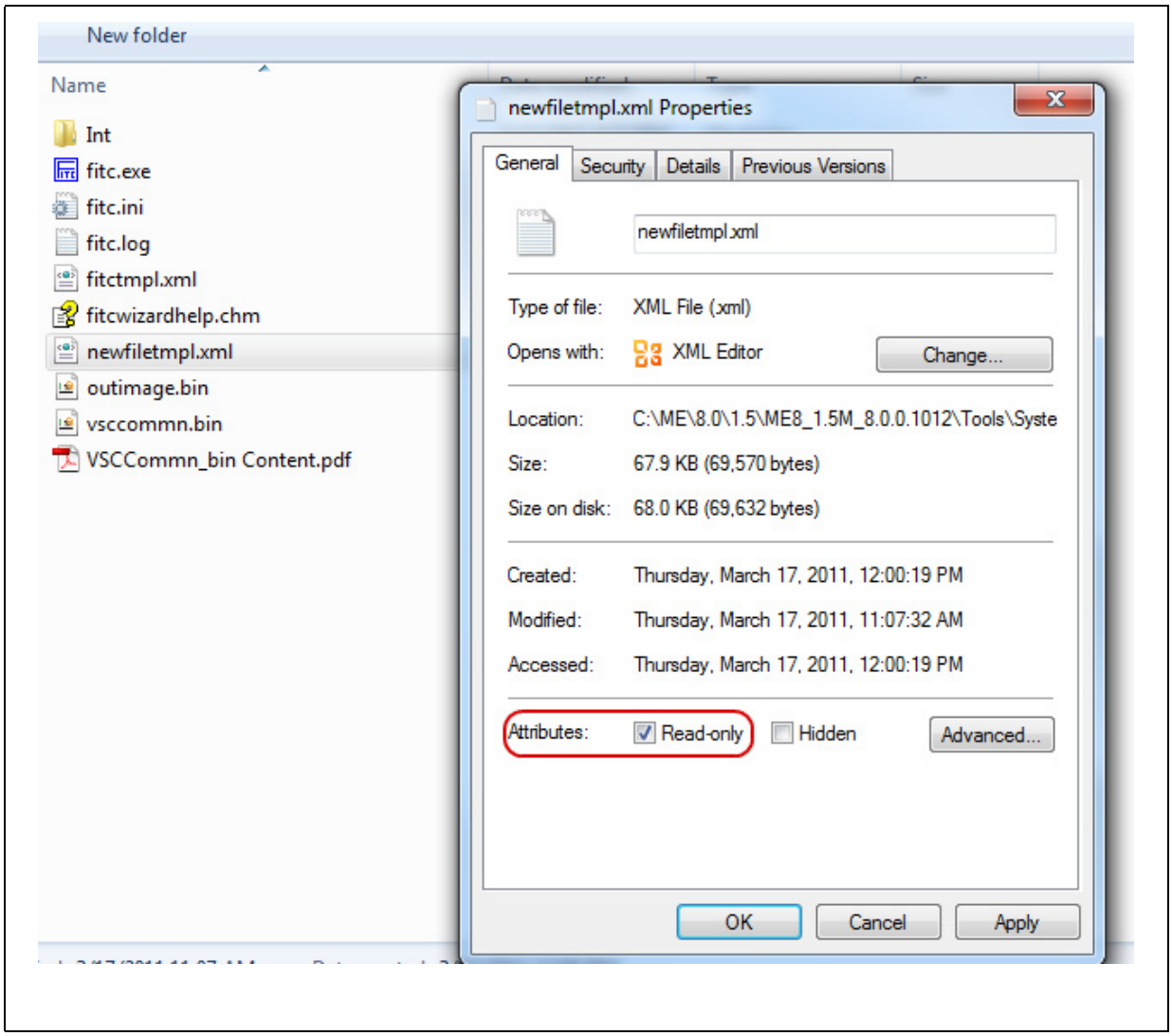
- **<xml_file>** — The XML configuration file saved when configuring FITC.
- **/o <file>** — The path and filename where the image will be saved. This command overrides the 'Output path' in the XML file.
- **/b** — Automatically builds the Flash image. The FIT GUI will not be displayed when this flag 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

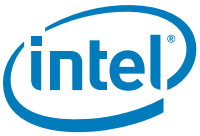
To avoid custom-configured values from ever overwritten when loading new binaries files (ie: when loading binaries into BIOS, GbE and ME regions in FITC) do the following (see Figure 2-6):

- 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. However, the following general steps may be followed:

1. Navigate to your **Output Directory** (as specified in Section 2.1) 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

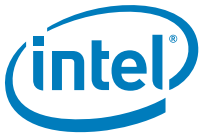
Mobile CRBs have the SPI Flash devices soldered down. As a result, to program the SPI Flash for mobile CRBs, follow these steps:

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 2.1) 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:

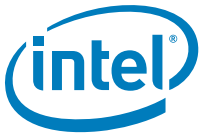
```
fpt.exe /f outimage.bin
```

   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 2.1) 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
```

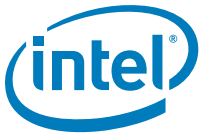
   If the programming was **NOT** successful, then repeat this step to try again. If programming problems persist, then check the SPI Flash devices and platform hardware.

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 stop at 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
```

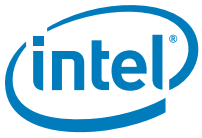
The system should respond with a message similar to below.

```
Intel(R) MEInfo Version: 9.0.0.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:                          9.0.0.xx
Gbe Version:                           1.3
VendorID:                              8086
PCH Version:                           600000
FW Version:                            9.0.0.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.

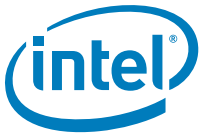


3.4 Common Bring Up Issues and Troubleshooting Table

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 CPU fan power connectors • DIMM memory modules • USB devices (keyboard, mouse, USB key) may be plugged into inactive USB port • missing/incorrect jumpers • missing CPU or PCH
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.

§ §

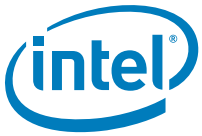


All parameters in this section are color-coded as per the key below.

The parameter can be changed
The parameter is read only and cannot be changed

Table 3-3. Feature Default Settings by Intel® 8 Series Chipset Family SKU (Desktop)

9 Series	Feature	Default Value
Intel® H87 - Desktop	Enable Intel® Standard Manageability; Disable Intel® AMT	Yes
	Managability Application Permanently Disabled?	No
	PAVP Permanently Disabled?	No
	TLS Permanently Disabled?	No
	Intel® Anti-Theft Technology Permanently Disabled?	No
	Intel® ME Network Services Permanently Disabled?	No
	mDNS Proxy Permanently Disabled?	Yes
	Intel® Manageability Application Enable / Disable	Enabled
Intel® Z87 - Desktop	Enable Intel® Standard Manageability; Disable Intel® AMT	Yes
	Managability Application Permanently Disabled?	Yes
	PAVP Permanently Disabled?	No
	TLS Permanently Disabled?	Yes
	Intel® Anti-Theft Technology Permanently Disabled?	No
	Intel® ME Network Services Permanently Disabled?	No
	mDNS Proxy Permanently Disabled?	Yes
	Intel® Manageability Application Enable / Disable	Disabled
Intel® Z85 - Desktop	Enable Intel® Standard Manageability; Disable Intel® AMT	Yes
	Managability Application Permanently Disabled?	Yes
	PAVP Permanently Disabled?	No
	TLS Permanently Disabled?	Yes
	Intel® Anti-Theft Technology Permanently Disabled?	No
	Intel® ME Network Services Permanently Disabled?	No
	mDNS Proxy Permanently Disabled?	Yes
	Intel® Manageability Application Enable / Disable	Disabled
Intel® H81 - Desktop	Enable Intel® Standard Manageability; Disable Intel® AMT	Yes
	Managability Application Permanently Disabled?	Yes
	PAVP Permanently Disabled?	No
	TLS Permanently Disabled?	Yes
	Intel® Anti-Theft Technology Permanently Disabled?	No
	Intel® ME Network Services Permanently Disabled?	No
	mDNS Proxy Permanently Disabled?	Yes
	Intel® Manageability Application Enable / Disable	Disabled



All parameters in this section are color-coded as per the key below.

The parameter can be changed
The parameter is read only and cannot be changed

Table 3-4. Feature Default Settings by Intel® 8 Series Chipset Family SKU (Mobile)

9 Series	Feature	Default Value
Mobile Intel® HM87 Express Chipset	Enable Intel® Standard Manageability; Disable Intel® AMT	Yes
	Managability Application Permanently Disabled?	No
	PAVP Permanently Disabled?	No
	TLS Permanently Disabled?	No
	Intel® Anti-Theft Technology Permanently Disabled?	No
	Intel® ME Network Services Permanently Disabled?	No
	mDNS Proxy Permanently Disabled?	Yes
	Intel® Manageability Application Enable / Disable	Enabled
Mobile Intel® HM86 Express Chipset	Enable Intel® Standard Manageability; Disable Intel® AMT	Yes
	Managability Application Permanently Disabled?	No
	PAVP Permanently Disabled?	No
	TLS Permanently Disabled?	No
	Intel® Anti-Theft Technology Permanently Disabled?	No
	Intel® ME Network Services Permanently Disabled?	No
	mDNS Proxy Permanently Disabled?	Yes
	Intel® Manageability Application Enable / Disable	Enabled

§ §

A Appendix — Flash Configurations

This chapter covers only the basic information needed for clock control parameter programming. For a more detailed treatment of Cougar Point clocks, see Intel® 8 Series Chipsethmmm Family *Platform Clocks* and *Intel® Management Engine — Platform Compliancy Guide for ME Hardware*.

Figure A-1. Configuration "A" — Desktop/Server/Workstation or Mobile

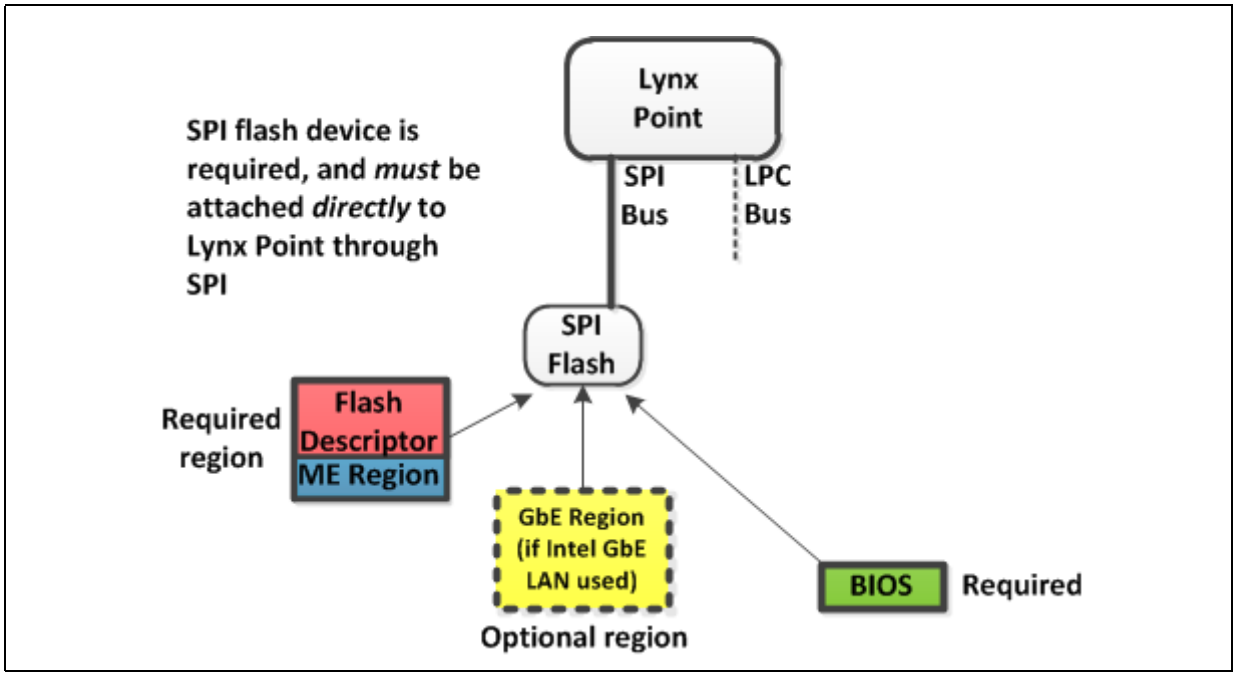


Figure A-2. Configuration "B" — Mobile Only

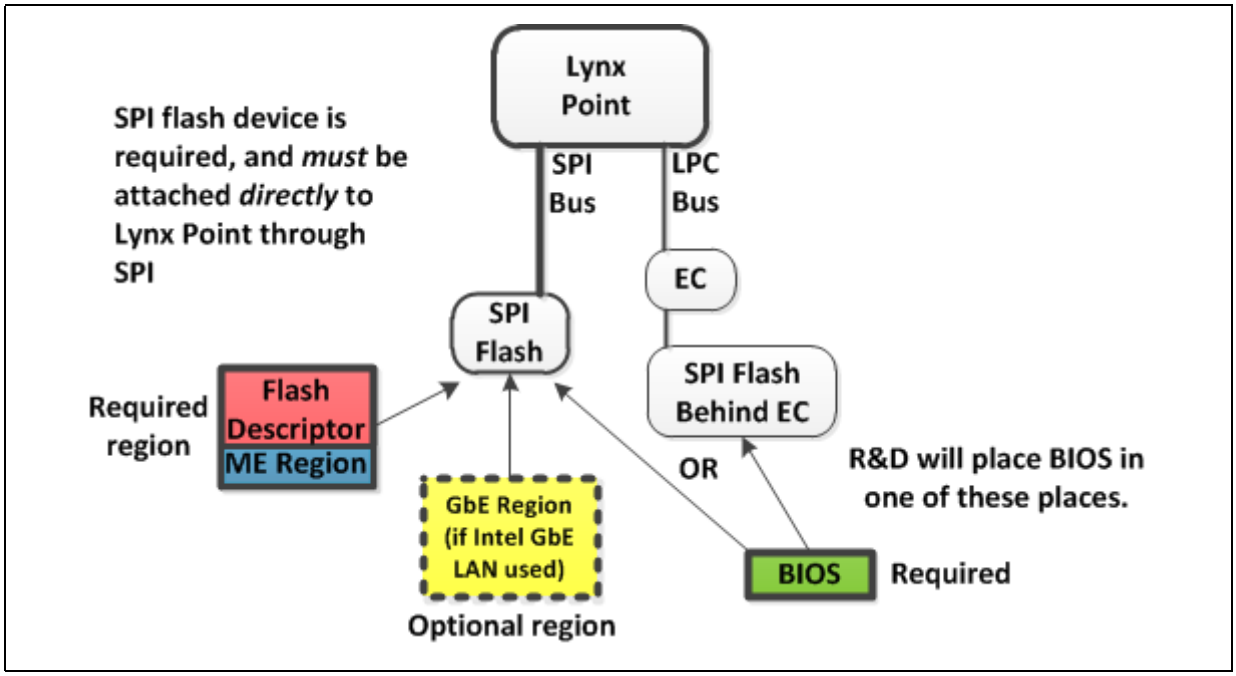


Figure A-3. Configuration "C" — Desktop/Server/Workstation Only

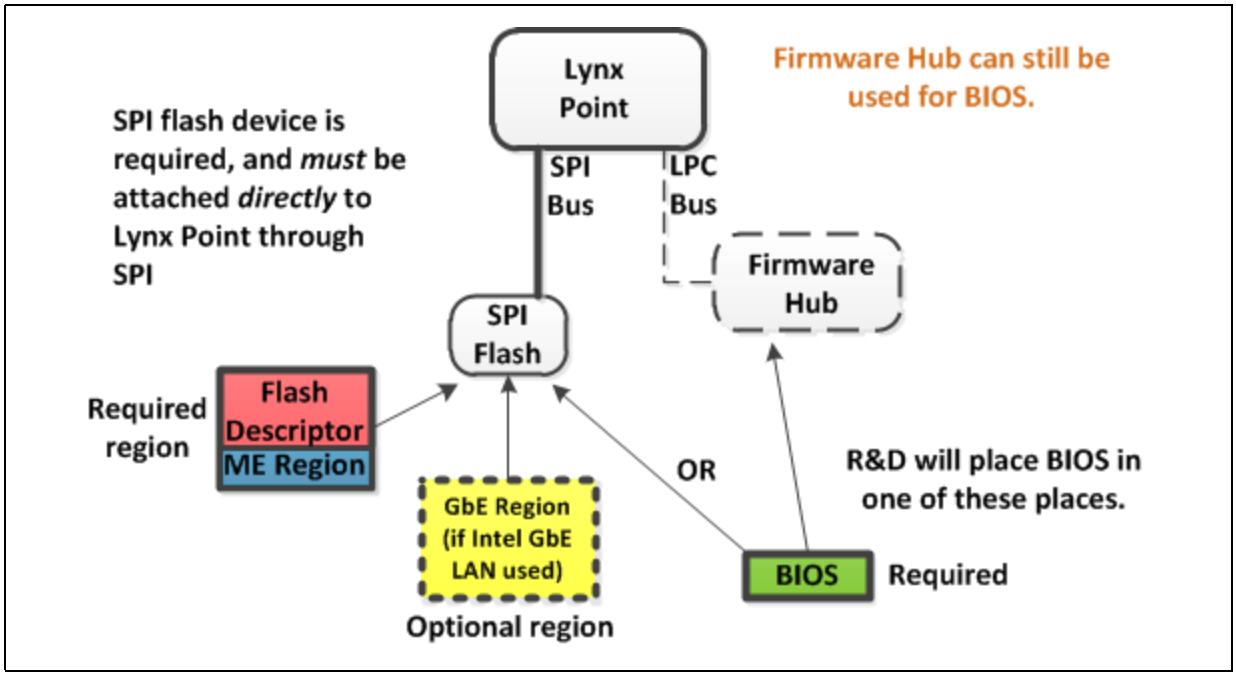
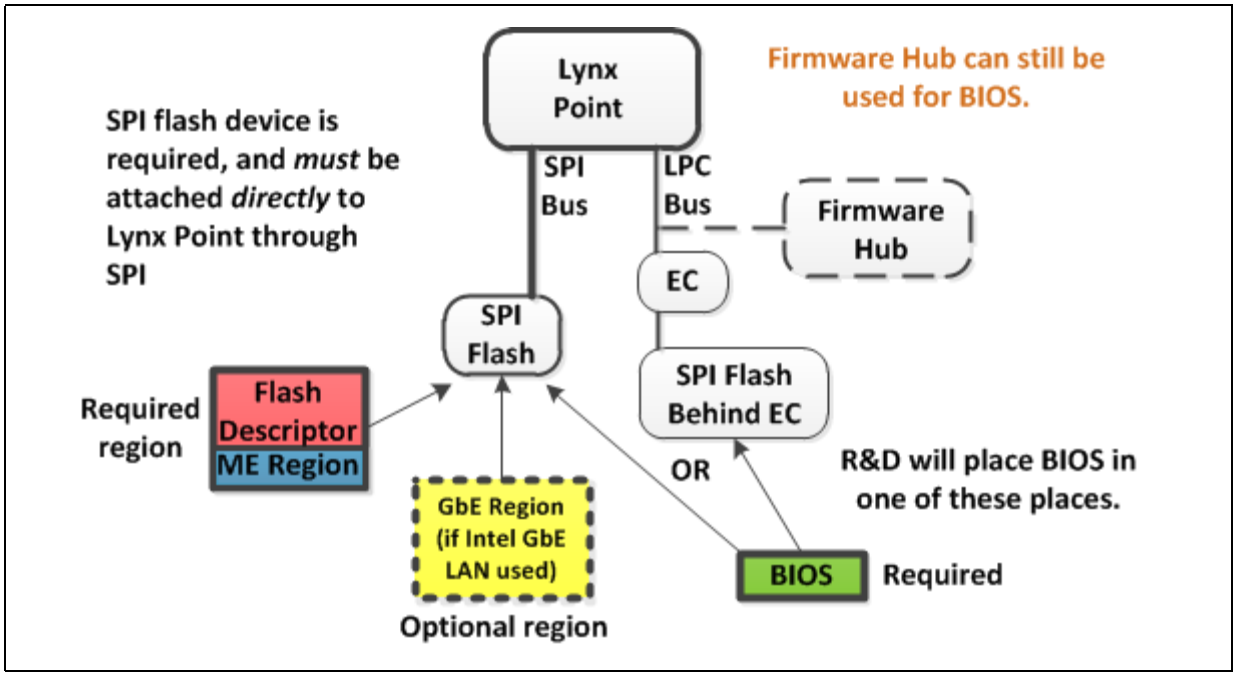


Figure A-4. Configuration "D" — Mobile Only



§ §

B Appendix — ICC SKU Support Matrix

Note: Please refer to Intel® 8 Series Chipset Family Platform Controller Hub (PCH) External Design Specification (EDS) for detail about Intel® 8 Series Intel® 8 Series Chipset Family Full Clock Integration Mode Architecture and Intel®ME FW clock control parameters.

For more information on validating and checking compliancy for PCH clocks, see Intel® 8 Series Intel® 8 Series Chipset Family *Intel® Management Engine — Compliancy Guide.*

B.0.1 ICC SKU Support Matrix

The following table describes features, clock range (maximum and minimum), spread mode supported by Intel® 8 Series Intel® 8 Series Chipset Family PCH SKU. The ICC SKU is divided into 3 categories; Basic, enhanced, and Extreme.

Table B-1.

PCH SKU	Basic	Enhanced	Extreme
Q87		**X**	
Q85		**X**	
B85		**X**	
H87		**X**	
Z87			**X**
Z85			**X**
H81		**X**	
QM87			**X**
HM87			**X**
HM86	**X**		
C222		**X**	
C224		**X**	
C226		**X**	
Features Supported	Display Clock Bending	Display Clock Bending Adaptive Clocking (Wimax Friendly Clocking)	Display Clock Bending Adaptive Clocking (Wimax Friendly Clocking) CPU BCLK Overclocking

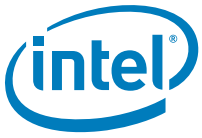


Table B-1.

PCH SKU	Basic	Enhanced	Extreme
Pre-Defined ICC profile supported.	Standard	Standard WiMax 3G	Standard WiMax 3G Overclocking
Clock Range Supported	**1. MODDIV2** will be turned off. **2. MODDIV3** * [Min-Max]=100MHz.	**1. MODDIV2** [Min - Max] = 98.4055 - 100 MHz. **2. MODDIV3** * [Min - Max] = 99.5392-100 MHz .	**1. MODIV2** [Min - Max] = 99.5463-800 MHz **2. MODDIV3** * **[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)

* MODDIV3 range limits are specified based on PCIe specifications.