Ibex Peak Intel® Management Engine

Firmware Bring Up Guide

November 2009

Revision 0.91

Intel Confidential

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

UNLESS OTHERWISE AGREED IN WRITING BY INTEL, THE INTEL PRODUCTS ARE NOT DESIGNED NOR INTENDED FOR ANY APPLICATION IN WHICH THE FAILURE OF THE INTEL PRODUCT COULD CREATE A SITUATION WHERE PERSONAL INJURY OR DEATH MAY OCCUR.

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

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

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

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

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

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

Code names featured are used internally within Intel to identify products that are in development and not yet publicly announced for release. Customers, licensees and other third parties are not authorized by Intel to use code names in advertising, promotion or marketing of any product or services and any such use of Intel's internal code names is at the sole risk of the user.

Intel and the Intel logo are trademarks of Intel Corporation in the U.S. and other countries.

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

Contents

Figures

Tables

Revision History

Revision Number	Description	Date
0.1	Initial Full SKU release	December 2008
0.2	• Updated FITc screen captures to reflect interface name changes. • Added PCH B0 Bring Up section. • Added Clock configuration information.	January 2009
0.3	• Updated QST section INI naming. • Fixed start of B0 Bring-up section which was referencing to A0 / A1.	January 2009
0.4	• Updated the Fast Read Frequency to 50Mhz • Added in the preliminary Configuration Tab section setting information.	February 2009
0.5	• Added new section for manual editing of Soft Strap values for A0 / A1 stepping images. • Added new ME Features section. • Moved previous Appendix B information into Appendix C • Added new Flash Configuration section in Appendix B	February 2009
0.6	• Added new Kit Dashboard Table 3-1 • Added additional information to the Configuration Parameters section outlining proper Desktop / Mobile WLAN Power Well Config settings	February 2009
0.61	• Added updated programming information to ICC Data section. • Added Braidwood specific strap information. • Changed several default values for FITc soft strap values.	March 2009
0.62	• Changes Strap 15 Configuration description to indicate that this setting is required in order for M3 power flows to function properly	March 2009
0.63	• Updated Kit Contents section with for Engineering Release	March 2009
0.64	• Removed A0 / A1 Bring-up section information • Updated Braidwood section. • Added Appendix E with Redfort Mobile CRB information on G3 and Virtual Battery options.	March 2009
0.65	• Clarified the ConfigFile.xml reference for the Clock Control parameters in Bring-up Process – All Platforms section. • Added new Appendix F for Basic Intel® AMT bring-up testing. • Moved Kit Dash Board to the of Quick Start and Kit Contents	March 2009

Revision Number	Description	Date
0.66	• Updated Clock Control information and moved High Impact Clock section • Added Intel® RPAT section information • Added additional information on CPU settings for the Mobile platform and updated the Virtual Battery section for better clarity.	April 2009
0.67	• Updated Strap 9 PCIe Port Configuration 2 section information for Desktop versus Mobile CRB configuration. • Updated default XML file information • Removed Intel® AT-d section information • Removed the Mobile CRB CPU setting section.	April 2009
0.68	• Updated CCG and MPG BIOS version numbers in the Kit Contents sections for Alpha1 Release • Updated Braidwood section.	April 2009
0.69	• Updated M3 Power Rail Availability option	April 2009
0.70	• Updated Kit Contents section	May 2009
0.71	• Added SKU Manager and Updated Feature Enable / Disable changes.	May 2009
0.72	• Removed DOS4GW.exe reference from Intel® QST section. It is not required for Ibex Peak	May 2009
0.73	• Updated Strap 10 and Strap 14 information for FITc changes for Braidwood. • Added updated Braidwood section content with FITc changes. • Updated Firmware Features section changes. • Updated Configuration section Screen Captures. • Removed Intel® AT-d section from Configuration section. • Removed Appendix G Features section. No longer needed with changes made in FITc. • Added Consumer SKU Sentry Peak section.	May 2009
0.74	• Moved the binary sections to the start of the Bring-up process. • Moved Platform SKU Selection immediately after the ME Region loading section and added notes to start of both sections on the order of loading steps. • Updated Intel® RPAT section information	May 2009
0.75	• Change to the build settings option in FITc added.	June 2009
0.76	• Added GPIO33 jumper information for Redfort Mobile CRB to the Mobile CRB Appendix E • Changed PM1 Default setting recommendation	June 2009

Revision Number	Description	Date
0.77	• Updated Configuration section with information on concerning EHCI parameters	July 2009
0.78	• Updated Strap 10 option information to include Net Debug Emergency enable option • Updated Braidwood enabling section with latest information. • Updated Appendix A Clocking section	July 2009
0.79	• Updated Consumer SKU changes from Sentry Peak to Intel® Identity Protection Technology	July 2009
0.80	• Updated Appendix E Manufacturing mode jumper setting information.	Aug 2009
0.81	• Update Feature information to remove PAVP 1.5 ship state disable option	Aug 2009
0.82	• Removed Braidwood related information from the guide • Updated Strap and Configuration section screen captures to reflect resent change to FITc • Updated Appendix C – C.4 with current feature enable / disable option changes. • Removed the P57 / PM57 SKU information from Appendix C – C.4	Aug 2009
0.83	• Updated Kit Contents Drivers section • Updated Basic Intel® AMT Bring-up steps section to reflect MEBx changes	Sept 2009
0.84	• Updated Appendix A with new entries for DCI clocking: PLLEN* – PLL Enable DIVEN* – Divider Enable OBEN – Output Buffer Enable DIVEN* – Divider Enable SSCCTL* – SSC Control	Sept 2009
0.85	• Updated PM1 default setting recommendation	Sept 2009
0.86	• Updated Intel® RPAT sections • Updated Intel® Identity Protection section	Oct 2009
0.87	• Updated Kit Contents section	Oct 2009
0.88	• Updated Section **4.2.1** and **4.2.7** with changes to the End of Manufacturing changes for FITc.	Nov 2009
0.89	• Updated CRB BIOS versions in Kit Contents section	Nov 2009
0.90	• Updated for AMT 6.1 Alpha release	Nov 2009
0.91	• Minor changes for clarification	Nov 2009

§

1 Introduction

1.1 Purpose and Scope of this Document

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

The bring up procedure primarily involves building an 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 Firmware region — Contains firmware for the Intel® Management Engine.
- **[optional]** GbE region — Contains firmware for Intel LAN solution

See *SPI Flash Programming Guide* and Appendix B – for more details on SPI Flash layout. Once the SPI flash image is built, it will be programmed to the target Ibex Peak 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 Firmware is operating as expected.

1.2 Related Documentation

82577 (Hanksville-M)

CDI:

http://www.intel.com/cd/edesign/library/asmo-na/eng/402854.htm

Document ID:-402854

Title:-Intel® 82577 Gigabit Ethernet PHY – (Hanksville-M -Beta1 Update SVK) Silicon Sample Kit – 27-Feb-2009

Abstract:-LAN Access Division (LAD) - Update to Beta1 kit that has updated NVM versions for use with Ibex Peak B0 and 82577 A2, ES2 samples. Has an updated version of Intel Boot Agent. Version V1.0C0073 TIC 180648,

VIP: 16954 - Intel® 82577 Gigabit Ethernet Controller (Hanksville-M SVK) - Beta1 Update - TIC 180648

82578 (Hanksville-D)

CDI:

http://www.intel.com/cd/edesign/library/asmo-na/eng/402853.htm

Document ID:-402853

Title:-Intel® 82578 Gigabit Ethernet PHY – (Hanksville-D Beta1 Update SVK) Silicon Sample Kit – 27-Feb-2009

Abstract:-LAN Access Division (LAD) - Update to Beta1 kit that has updated NVM versions for use with Ibex Peak B0 and 82578 C0, ES2 samples. Contains an updated version of Intel Boot Agent. Version V1.0C0073 TIC 180643.

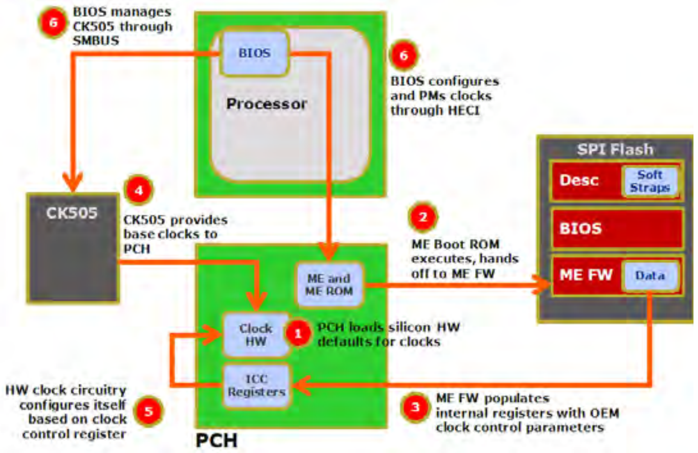
VIP: 16955 - Intel® 82578 Gigabit Ethernet Controller (Hanksville-D SVK) - Beta1 Update - TIC 180643and checks required to ensure that this boot process is successful, and that Intel® ME Firmware is operating as expected.

1.3 Intel® ME Firmware Features

This firmware release includes the following applications:

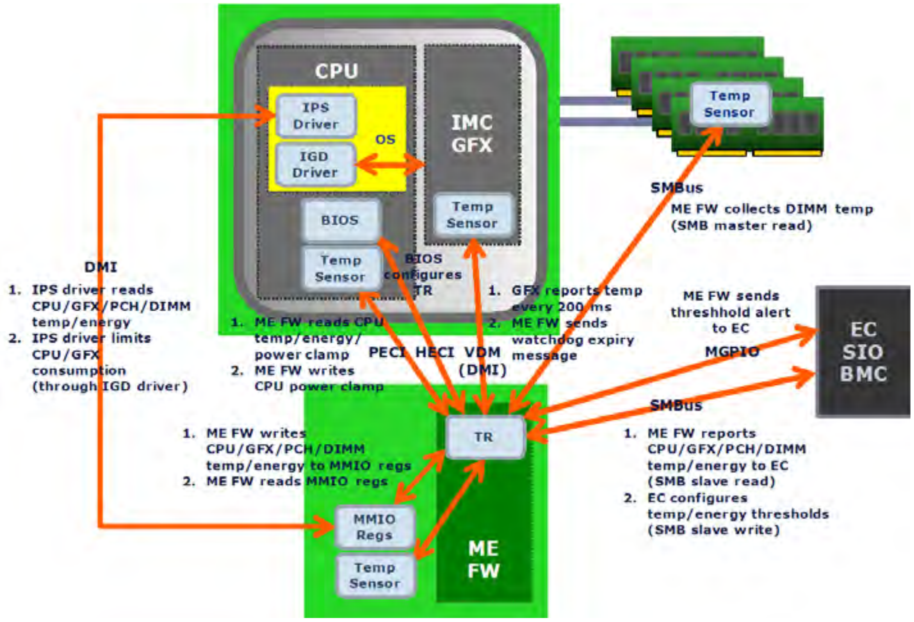
- Platform Clocks – Tune Ibex Peak clock silicon to the parameters of a specific board, configure clocks at run time, power manage clocks.
- **Benefit:** Allows extensive customizability and soft control of "first generation" clock solution and makes clocks available before CPU powers up.

Figure 1-1. Clock Initialization Process (Simplified)


6
BIOS manages CK505 through SMBUS
BIOS
Processor
6
BIOS configures and PMs clocks through HECI
SPI Flash
Desc
Soft Straps
BIOS
ME FW
Data
4
CK505 provides base clocks to PCH
CK505
2
ME Boot ROM executes, hands off to ME FW
ME and ME ROM
Clock HW
1
PCH loads silicon HW defaults for clocks
ICC Registers
HW clock circuitry configures itself based on clock control register
5
3
ME FW populates internal registers with OEM clock control parameters
PCH

- Silicon Workaround Capability – Intel ME firmware will have limited capabilities to perform targeted workarounds for silicon issues. **Benefit:** Allows Intel ME Firmware to address some issues that otherwise would require a new silicon stepping.

Figure 1-2. Thermal Reporting


CPU
IPS Driver
IGD Driver
OS
IMC GFX
BIOS
Temp Sensor
Temp Sensor
BIOS configures TR
DMI
1. IPS driver reads CPU/GFX/PCH/DIMM temp/energy
2. IPS driver limits CPU/GFX consumption (through IGD driver)
1. ME FW reads CPU temp/energy/ power clamp
2. ME FW writes CPU power clamp
PECI
HECI
VDM (DMI)
1. GFX reports temp every 200 ms
2. ME FW sends watchdog expiry message
Temp Sensor
SMBus
ME FW collects DIMM temp (SMB master read)
ME FW sends threshhold alert to EC
MGPIO
EC SIO BMC
SMBus
1. ME FW reports CPU/GFX/PCH/DIMM temp/energy to EC (SMB slave read)
2. EC configures temp/energy thresholds (SMB slave write)
1. ME FW writes CPU/GFX/PCH/DIMM temp/energy to MMIO regs
2. ME FW reads MMIO regs
TR
MMIO Regs
Temp Sensor
ME FW

- Thermal Reporting – ME Firmware reports thermal and power information available only on PECI to host accessible registers / Embedded Controller (EC) via SMBus. Benefit: Reporting is a requirement of performance-critical Intel® Intelligent Power Sharing feature. Allows third party PECI-capable temperature monitor value segment solutions.

1.4 Prerequisites

Before this document is read and utilized, it is essential that the reader first review the **Readme** and **Release Notes** documents included in the kit distribution. Notes documents included in the kit distribution.

This document is constructed so that the reader can run through the bring-up steps as given for the Intel CRB. However, in the case that bring up is being performed on a different Ibex Peak based platform, this document will highlight any changes that must be imposed onto the bring-up steps accordingly.

This document makes only the following assumptions for hardware:

- The platform is Ibex Peak based.
- The platform is equipped with one or more SPI flash devices with a total capacity large enough to contain the generated SPI flash image.

1.5 Acronyms and Definitions

1.5.1 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
EC	Embedded Controller
EEPROM	Electrically Erasable Programmable Read Only Memory
GbE	Gigabit Ethernet
HECI (deprecated)	Host Embedded Controller Interface
IBV	Independent BIOS Vendor
ID	Identification
Intel® ME	Intel® Management Engine
Intel® MEI	Intel® Management Engine Interface (renamed from HECI)
Intel® TPM	Intel® Trusted Platform Module
ISV	Independent Software Vendor
JTAG	Joint Test Action Group
KVM	Keyboard, Video, Mouse
LAN	Local Area Network
LED	Light Emitting Diode
NVM	Non Volatile Memory
NVRAM	Non-Volatile Random Access Memory
OOB	Out of Band
OS	Operating System
PAVP	Protected Video and Audio Path
PCI	Peripheral Component Interconnect
PCIe*	Peripheral Component Interconnect Express
PHY	Physical Layer
PRTC	Protected Real Time Clock
RNG	Random Number Generator
RSA	RSA is a public key encryption method.
RTC	Real Time Clock

Acronym or Term	Definition
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

1.5.2 Intel® Management Engine

Acronym or Term	Definition
3PDS	3rd Party Data Store
Agent	Software that runs on a client PC with OS running.
Intel® AT	Intel® Anti-Theft Technology. Intel® AT-p (previously known as TDT).
CBM	ME CBMs - Core Base Modules. Refer to Figure: Intel ME Firmware partitioning
CEM	ME CEMs - Core Extension Modules. Also called ME CS. Refer to Figure: Intel ME Firmware partitioning
Corwin Spring	See WoX
DT	Danbury Technology. Previous name for Intel® AT-d which is part of Intel® Anti-Theft Technology.
End User	The person who uses the computer (either Desktop or Mobile). In corporate, the user usually does not have an administrator privileges. The end user may not be aware to the fact that the platform is managed by Intel® AMT.
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 support 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® AMT Firmware	The Intel® AMT Firmware running on the embedded processor.
Intel® Management Engine Interface (Intel® MEI)	Interface between the Management Engine and the Host system.
Intel® MEI driver	Intel® AMT host driver that runs on the host and interfaces between ISV Agent and the AMT HW.

Acronym or Term	Definition
Intel® Quiet System Technology (Intel® QST)	Fan speed control architecture that allows multiple sensors to control a single fan as well as allow a single sensor control of multiple fans.
IT User	Information Technology User. Typically very technical and uses a management console to ensure multiple PCs on a network function.
LMS	Local Management Service, A SW application which runs on the host machine and provide a secured communication between the ISV agent and the Intel® Management Engine Firmware.
Intel® ME	Intel® Management Engine, The embedded processor residing in the chipset GMCH.
Intel® MEBx	Intel® Management Engine BIOS Extensions
MECI	ME-VE Communication Interface
NVM	Non-Volatile Memory. A type of memory that will retain its contents even if power is removed. In the Intel® AMT current implementation, this is achieved using a FLASH memory device.
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 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
IPT	Intel® Identity Protection Technology
System States	Operating System power states such as S0. See detailed definitions in system state section.
TDT	Theft Deterrence Technology. Previous name for AT-p, which is part of the Intel® Anti-Theft Technology.
UIM	User Identifiable Mark
Un-configured state	The state of the Intel® Management Engine Firmware when it leaves the OEM factory. At this stage the Intel® Management Engine Firmware is not functional and must be configured.
WoX	Wake on Event or Wake on VoIP. Also called Corwin Spring.

1.5.3 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. Host power state is S0.
M1	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 PCI-E* interface are unavailable to the host SW. **This power state is not available in Ibex Peak.**
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 PCI-E* interface are unavailable to the host SW. 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 shut down.
OS Hibernate	OS state where the OS state is saved on the hard drive.
S0	A system state where power is applied to all HW devices and system is running normally.
S1, S2, S3	A system state where the host CPU is not running however power is connected to the memory system (memory is in self refresh).
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 is still connected.
Shut Down	All power is off for the host machine however the power cord is still connected.
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	OS 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.

1.6 Reference Documents

Document	Doc Number / Location*
RS – Piketon/Kings Creek and Foxhollow – Platform Design Guide	IBL 376563
RS – Calpella – Platform Design Guide	IBL 398905
Calpella – ME-EC Specification	IBL 394791
Calpella – PCH-EC SMBus Protocol Specification	IBL 390730
RS – Piketon/Kings Creek and Foxhollow – BIOS Writer's Guide	*
Ibex Peak Platform Clocks – Debug and Test Guide	*
Ibex Peak Platform Clocks and Intel® Management Engine – Co-validation Guide	*
Ibex Peak Platform Intel® Management Engine – Hardware Debug and Test Guide	*

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

1.7 Number and Format

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

Data Type	Notation	Size
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

§

2 Intel® QST Image Generation

- **This section is only applicable if Intel® QST is to be configured on the target platform. If not, please skip this section and continue with the next section.**
- This section describes how to change the fan speed settings (Intel® QST settings), if default values are to be modified.
- INI files are provided in the kit with Intel-provided default values. If fan speed control values are to be modified, then change the default values provided in the INI files, before creating the Intel® QST image.

This section describes the creation of the Intel® QST binary image. This image will be integrated with the Intel ME firmware image along with the GbE and BIOS images using the Flash Image Tool to create the final flash image. The Intel® QST binary image is created using the Intel® QST Configuration tool. The Intel® QST Configuration tool takes in an INI (parameter initialization) file as input to create the Intel® QST binary image.

2.1 Intel® QST INI files

An INI file is used to create the Intel® QST binary image. The following table summarizes the location of the INI files:

INI File	Directory Location	Example
QstCfgATXIP.ini	“Unzipped_folder”\Tools\QST Tools\	C:\PCH_8M_6.0.0.xxxx\Tools\QST Tools\QstCfgATXIP.ini

2.2 Intel® QST Configuration Tool

The Intel® QST binary image can be created either using the DOS environment (as described in Section 2.2.1) or using Windows* environment (as described in section 2.2.2).

2.2.1 Intel® QST Configuration DOS Tool

The Intel® QST Configuration DOS Tool can be accessed under the following directory:

- “Unzipped_folder” Tools\QST Tools\
  (Example: C:\PCH_8M_6.0.0.xxxx\Tools\QST Tools\QstCfgD.exe)

Executing the following command at the DOS prompt generates the Intel® QST binary file:

- QstCfgD <INI File Pathname> [{-w|-o} <Binary File Pathname>]

Where:

INI File Pathname: Provides a pathname for the INI file

-w [Binary File Pathname]: Specifies that the payload is to be written to a file. If the file already exists, the tool will ask for confirmation before overwriting it.

-o [Binary File Pathname]: Specifies that the payload is to be written to a file. If the file already exists, it will be overwritten.

(Example: QstCfgD.exe QstCfgATXIP.ini -w QSTBinary.bin)

The Intel® QST binary image (Example: QSTBinary.bin) is created in the specified folder.

Note: For more details on this tool, refer to the document – 'Intel Quiet System Technology Configuration and Tuning Manual'. Please contact your Intel representative to get access to this document.

2.2.2 Intel® QST Configuration Windows* Tool

The Intel® QST Configuration Windows* tool is located in the following directory:

- "Unzipped_folder"\Tools\QST Tools\
  (Example: C:\PCH_8M_6.0.0.xxxx\Tools\QST Tools\QstCfg.exe)

Executing the following command at the Windows command prompt generates the Intel® QST binary file:

- QstCfg <INI File Pathname> [{-w|-o} <Binary File Pathname>]

Where:

INI File Pathname: Provides a pathname for the INI file

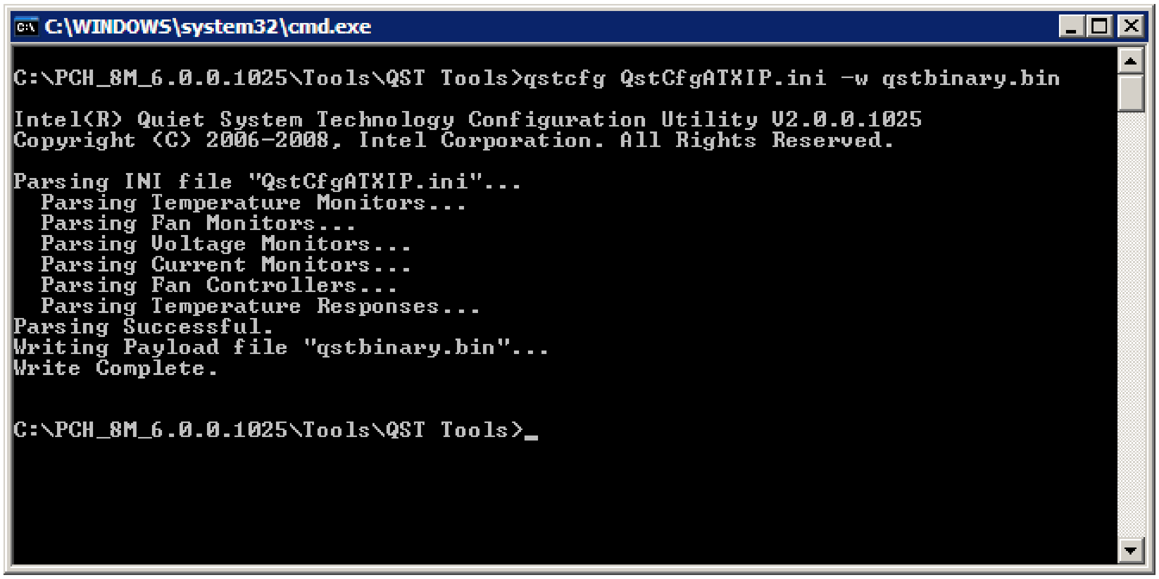
-w [Binary File Pathname]: Specifies that the payload is to be written to a file. If the file already exists, the tool will ask for confirmation before overwriting it.

-o [Binary File Pathname]: Specifies that the payload is to be written to a file. If the file already exists, it will be overwritten.

(Example: QstCfg.exe QstCfgATXIP.ini -w QSTBinary.bin)

The Intel® QST binary image (Example: QSTBinary.bin) is created in the specified folder.

Figure 2-1. Snapshot of executing the Intel® QST Windows Configuration Tool



```
C:\PCH_8M_6.0.0.1025\Tools\QST Tools>qstcfg QstCfgATXIP.ini -w qstbinary.bin

Intel(R) Quiet System Technology Configuration Utility V2.0.0.1025
Copyright (C) 2006-2008, Intel Corporation. All Rights Reserved.

Parsing INI file "QstCfgATXIP.ini"...
  Parsing Temperature Monitors...
  Parsing Fan Monitors...
  Parsing Voltage Monitors...
  Parsing Current Monitors...
  Parsing Fan Controllers...
  Parsing Temperature Responses...
Parsing Successful.
Writing Payload file "qstbinary.bin"...
Write Complete.


C:\PCH_8M_6.0.0.1025\Tools\QST Tools>_
```

- For more details on this tool, refer to the document – ‘*Intel® Quiet System Technology Configuration and Tuning Manual’.* Please contact your Intel representative for access to this document.
- The Intel® QST Configuration GUI Tool (QSTCT_GUI.exe), also included in this distribution, can be used to create the Intel® QST binary image in Windows* environment. See the document ‘*Intel® Quiet System Technology Configuration and Tuning Manual*’ for a description of the GUI tool.
- Downloading of Microsoft VC runtime libraries is required for the Intel® QST Configuration GUI tool to work under Microsoft* Windows* 2000 Operating System. For more details, please refer to the document ‘ReleaseNote.pdf’ (Download from the same source as the kit is downloaded from)

§

3 Quick Start and Kit Contents

Table 3-1. Kit Dashboard

Component	Description	
ME Firmware Kit	This kit is intended for initial IBV / OEM integration and basic testing with Full firmware core for Ibex Peak based platforms.	
Firmware Core	□ Uses Ignition Firmware core (no UMA) ☑ Uses Full Firmware core (uses UMA)	
Supported Manageability Power States	☑ S0/M0 ☑ S3/M3 ☑ S4/M3	☑ S5/M3 ☑ Sx/Moff
Supported processors	Desktop (Quad Core) ☑ Lynnfield LGA1156 SFF QS Desktop (Dual Core) ☑ Clarkdale LGA1156 QS	Mobile (Quad Core) ☑ Clarksfield rPGA QS Mobile (Dual Core) ☑ Arrandale rPGA QS
Supported PCHs	Desktop ☑ Ibex Peak ES3 (B1, QLLS) ☑ Ibex Peak ES3 (B2, QLLS) ☑ Ibex Peak ES3 (B3, QLLS)	Mobile/SFF ☑ Ibex Peak ES3 (B1, Qxxx) ☑ Ibex Peak ES3 (B2, Qxxx) ☑ Ibex Peak ES3 (B3, Qxxx)
Supported Intel LAN PHYs	Desktop ☑ 82578DM (Hanksville-D) ES1/ES2 (C0 , QLMJ)	Mobile ☑ 82577LM (Hanksville-M) ES1/ES2 (A2, QLDT)
Tools	☑ Flash Image Tool (FITc) ☑ Flash Programming Tool (FPT, FPTW) ☑ MEInfo ☑ ConfigurationServer ☑ QST Tools	☑ MEManuf ☑ UpdParam ☑ FSTDOS ☑ FWUpdate

3.1 Quick Start

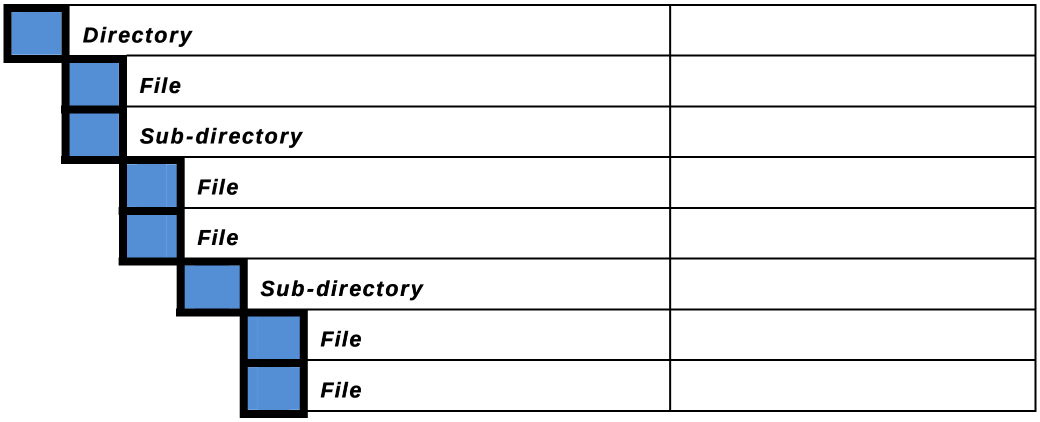
The Intel ME Firmware bring-up process involves the following steps:

1. Download the Intel ME Firmware kit and inspect its contents (see Section **3.2**, page **26**)
2. Create SPI flash binary image using Flash Image Tool (**4.2**, page **37**)
3. Program the SPI binary image into the target platform's SPI device(s) using Flash Image Tool, or a flash programmer (see Section **4.4**, page **80**), or using firmware update methodology.

   [Remove power from the target system. Clear CMOS by removing the CMOS battery after power has completely cleared the target system. Reapply power to the target system, and press the power button.]
4. Verify that system clocks are operating as expected (see *Ibex Peak Platform Clocks – Debug and Test Guide*).

3.2 Kit Contents

The Intel ME Firmware kit can be downloaded from VIP (https://platformsw.intel.com/). The contents of this kit are provided in this section. The contents are organized within the example framework shown below:



The kit is distributed as a ZIP archive. Extract the archive, keeping its directory structure intact. The root folder of the extracted archive will be referred to as "(root)". In some of the examples shown in this document, **(root)** is **C:\temp\ME_Kit**. The Intel ME Firmware kit contains the following files:

(root)	Location of extracted archive contents.
FW Bring Up Guide.pdf	This document.
PCH_SPI_Programming_Guide.pdf	How to program SPI device parameters, VSCC tables, descriptor region details. This document's contents are integrated with the Firmware Bring Up Guide.
Intel MEBx_Users_Guide_for_Intel AMT_6_0.pdf	MEBx Users guide.
Intel(R)AMT_6_0_OEM_WebUI_Guide.pdf	WebUI OEM Users guide.
Drivers	MEI / LMS_SOL Drivers
readme.txt	This explains the differences between the installer packages
ME_IS	InstallShield - MEI / LMS_SOL Drivers with IMSS.
ME_IS.zip	
SetupSE.exe	
ME _IS_NO_IMSS	InstallShield - MEI / LMS_SOL Drivers without IMSS.
ME_IS_NO_IMSS.zip	
MEI_SOL _Installer	MEI / LMS_SOL Drivers with IMSS.
Drivers	
MEI	
heci.cat	
HECI.inf	
HECI.sys	
HECIx64.sys	
SOL	
mesrl.cat	
mesrl.inf	
mesrle.cat	
mesrle.inf	
IMSS	
AMT_COM_InterfaceLib.dll	
AMT_SW_GUI.dll	

PrivacyIconClient.exe	
PrivacyIconClient.exe.config	
readme.txt	
Intel Control Center	
SetupICC.exe	
Lang	MEI / LMS_SOL Setup Localized Languages.
LMS	
LMS.exe	
NTService_license.txt	
MEWMIProv	
MeProv.dll	
StatusStrings.dll	
xerces-c_2_7.dll	
ME	
CreateMENamespace.bat	
ME_Schema.mof	
register.mof	
remove.mof	
removeMEnamespace.bat	
wmi_build.mof	
cim_schema	
MEMofs	
NAC_PP	
Configuration Guide for Intel AMT Posture Data.pdf	
IntelAMTPP.dll	
IntelAMTPP.inf	
Readme.txt	
UNS	
DTMessageLib.dll	
DTMessageLib_X64.dll	
gSOAP_license.txt	
IntelAMTUNS.config	

openSSL_license.txt	
readme.txt	
StatusStrings.dll	
UNS.exe	
xerces_LICENSE.txt	
xerces-c_2_7.dll	
x64	
DIFxAPI.dll	
Drv64.exe	
MEcp64.exe	
MEI_SOL _Installer_NO_IMSS	InstallShield - MEI / LMS_SOL Drivers without IMSS.
Drivers	
MEI	
heci.cat	
HECI.inf	
HECI.sys	
HECIx64.sys	
SOL	
mesrl.cat	
mesrl.inf	
mesrle.cat	
mesrle.inf	
Intel Control Center	
SetupICC.exe	
Lang	
LMS	
LMS.exe	
NTService_license.txt	
MEWMIProv	
MeProv.dll	
StatusStrings.dll	
xerces-c_2_7.dll	

ME	
CreateMENamespace.bat	
ME_Schema.mof	
register.mof	
remove.mof	
removeMEnamespace.bat	
wmi_build.mof	
cim_schema	
MEMofs	
NAC_PP	
Configuration Guide for Intel AMT Posture Data.pdf	
IntelAMTPP.dll	
IntelAMTPP.inf	
Readme.txt	
UNS	
DTMessageLib.dll	
DTMessageLib_X64.dll	
gSOAP_license.txt	
IntelAMTUNS.config	
openSSL_license.txt	
readme.txt	
StatusStrings.dll	
UNS.exe	
xerces_LICENSE.txt	
xerces-c_2_7.dll	
x64	
DIFxAPI.dll	
Drv64.exe	
MEcp64.exe	
NVM Image	
BIOS	

cgibx165_rst9_5.rom - Piketon – Desktop CRB BIOS ***MPG083.rom - Calpella – MPG Mobile CRB BIOS***	BIOS firmware binary. Can only be used with the Intel CRB. For other Ibex Peak based platforms, a custom BIOS firmware binary will be required.
Firmware	
PCH_8M_DT_PreProduction.BIN –Desktop Full firmware binary ***PCH_8M_DT_UPD_PreProduction.BIN –Desktop Update binary for use with FWUpdLcl*** ***PCH_8M_MB_PreProduction.BIN –Mobile Full firmware binary*** ***PCH_8M_MB_UPD_PreProduction.BIN – Mobile Update binary for use with FWUpdLcl***	ME firmware binaries and update files. To be used on any Ibex Peak based platform.
GbE ***82577 GbE NVM Readme.doc*** ***82578 GbE NVM Readme.doc***	Intel LAN PHY firmware binary. Use with desktop, server, or workstation Ibex Peak based platforms.
82577 (Mobile)	
LAN Switch	
82577LM_A3_IBEXPEAK_B2B3_LAN_SWITCH_VER0PTC1.bin - Mobile Gbe firmware ***82577LM_A3_IBEXPEAK_B2B3_LAN_SWITCH_VER0PTC1.txt***	
Non LAN Switch	
82577LM_A3_IBEXPEAK_B2B3_NON_LAN_SWITCH_VER0PTC3.bin - Mobile Gbe firmware ***82577LM_A3_IBEXPEAK_B2B3_NON_LAN_SWITCH_VER0PTC3.txt***	
82578 (Desktop)	
82578DM (Corporate)	
82578DM_C0_IBEXPEAK_B2B3_VER0PTC2.bin – Desktop GbE firmware ***82578DM_C0_IBEXPEAK_B2B3_VER0PTC2.txt***	
ME_BIOS_Extension	
mebx_launch_6.0.3.0019.bin	
mebx_main_6.0.3.0019.bin	
Tools	

AMT Tools	
AMTConfiguration	
ConfigurationServer.exe	
gSOAP_license.txt	
libeay32.dll	
msvcr71.dll	
nokia_openssl_contribution_license.txt	
openSSL_license.txt	
ssleay32.dll	
CertGenerator	
ClientSecScripts	
OpenSSL	
SecConfig	
SecScripts	
ConfigScripts	
create_usb_file.bat	
default.conf.xml	
getcfg.bat	
provend.bat	
psk.repository.xml	
PskGenerator.exe	
USBFile.exe	
yesno.exe	
Unprovision	
gSOAP_license.txt	
StatusStrings.dll	
xerces-c_2_7.dll	
WsmanOnly	
StatusStrings.dll	
xerces-c_2_7.dll	
ZTCLocalAgent	
StatusStrings.dll	

ZTCLocalAgent.exe	
FSTDOS	
FSTDOS.exe	
QST	Refer to the **IBX QST Tool User Guide.pdf** for further details on the tools / usage in this folder.
IBX QST Tool User Guide.pdf	
QstCfg.exe	
QstCfgATXIP.ini	
QstCfgD.exe	
QstComm.dll	
QstComm.lib	
QstConfigurationWizard.msi	
QstCply.exe	
QSTCT_GUI.exe	
QstCtrl.exe	
QstINI.exe	
QstINID.exe	
QstInst.dll	
QstInst.lib	
QstLog.exe	
QstStat.exe	
QstStatD.exe	
QstTuningWizard.msi	
Include	
QstCfg.h	
QstCmd.h	
QstComm.h	
QstInst.h	
typedef.h	
MaxPower	
System Tools	
System Tools User Guide.pdf	

Tools_Version.txt	This file provides the tool versions for manufacturing tools contained in the kits.
Flash Image Tool	Refer to the **System Tools User Guide.pdf** for further details on the tools / usage in this folder.
fitc.exe	
vsccommn.bin	
fitc.ini	
fitctmpl.xml	
newfiletmpl.xml	Default FIT configuration XML file.
Flash Programming Tool	Refer to the **System Tools User Guide.pdf** for further details on the tools / usage in this folder.
License.rtf	
DOS	
fparts.txt	Database of supported SPI flash devices.
fpt.exe	Flash Programming Tool binary for DOS.
fptcfg.ini	
vsccommn.bin	
Windows	
fparts.txt	Database of supported SPI flash devices.
fptcfg.ini	
fptw.exe	Flash Programming Tool binary for 32-bit Windows operating systems.
sseidrvdll32e.DLL	
ssepmxdll32e.DLL	
ssepmxdrv.SYS	
vsccommn.bin	
FWUpdate	Refer to the **System Tools User Guide.pdf** for further details on the tools / usage in this folder.
Local-DOS	
FWUpdLcl.exe	
Local-Win	

FWUpdLcl.exe	
gSOAP_license.txt	
xerces-c_2_7.dll	
MEInfo	Refer to the **System Tools User Guide.pdf** for further details on the tools / usage in this folder.
DOS	
MEInfo.exe	
Windows	
MEInfoWin.exe	
sseIdrvdll32e.dll	
ssePmxdll32e.dll	
ssepmxdrv.sys	
MEManuf	Refer to the **System Tools User Guide.pdf** for further details on the tools / usage in this folder.
DOS	
AUTOEXEC.BAT	
MEManuf.exe	
vsccommn.bin	
Windows	
MEManufWin.exe	
sseIdrvdll32e.dll	
ssePmxdll32e.dll	
ssepmxdrv.sys	
vsccommn.bin	
UpdParam	Refer to the **System Tools User Guide.pdf** for further details on the tools / usage in this folder.
UpdParam.exe	

§

4 Bring Up Process — All Platforms

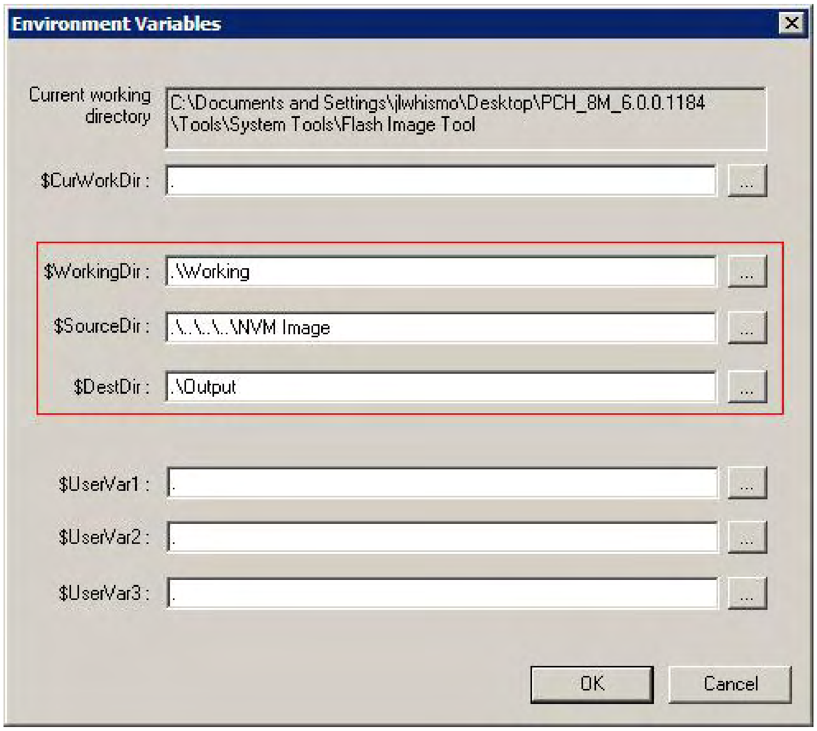
4.1 Bring Up Process

4.2 Assemble the SPI Flash Binary Image

Flash Image Tool will be used to generate the SPI flash binary image. Use the steps shown in following sections.

4.2.1 Set Up the Build Environment

1. Invoke Flash Image Tool. Using Explorer*, navigate to **(root)\Tools\System Tools\Flash Image Tool**. Ensure that FIT's directory contents are intact (see Section **3.2**, page **26**). 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)** is "**.**". **Source Directory** is where FIT will look to find binary images during the image creation process. **Destination Directory** is where FIT will save the SPI flash binary image. Click **OK** to apply your changes.



Current working directory: C:\Documents and Settings\jlwhismo\Desktop\PCH_8M_6.0.0.1184 \Tools\System Tools\Flash Image Tool

$CurWorkDir : .

$WorkingDir : .\Working

$SourceDir : .\..\..\..\NVM Image

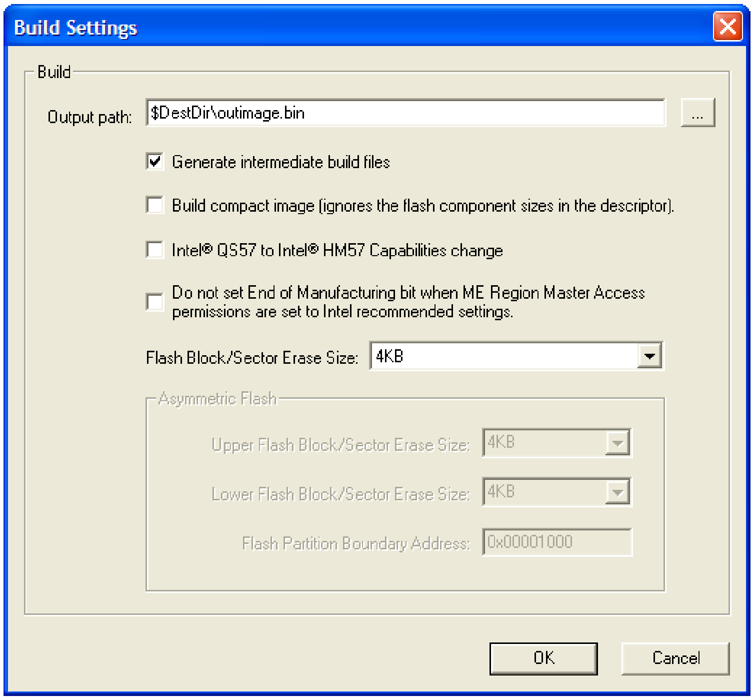
$DestDir : .\Output

$UserVar1 : .

$UserVar2 : .

$UserVar3 : .

3. 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).



Build

Output path: $DestDir\outimage.bin

☑ Generate intermediate build files

☐ Build compact image (ignores the flash component sizes in the descriptor).

☐ Intel® QS57 to Intel® HM57 Capabilities change

☐ Do not set End of Manufacturing bit when ME Region Master Access permissions are set to Intel recommended settings.

Flash Block/Sector Erase Size: 4KB

Asymmetric Flash

Upper Flash Block/Sector Erase Size: 4KB

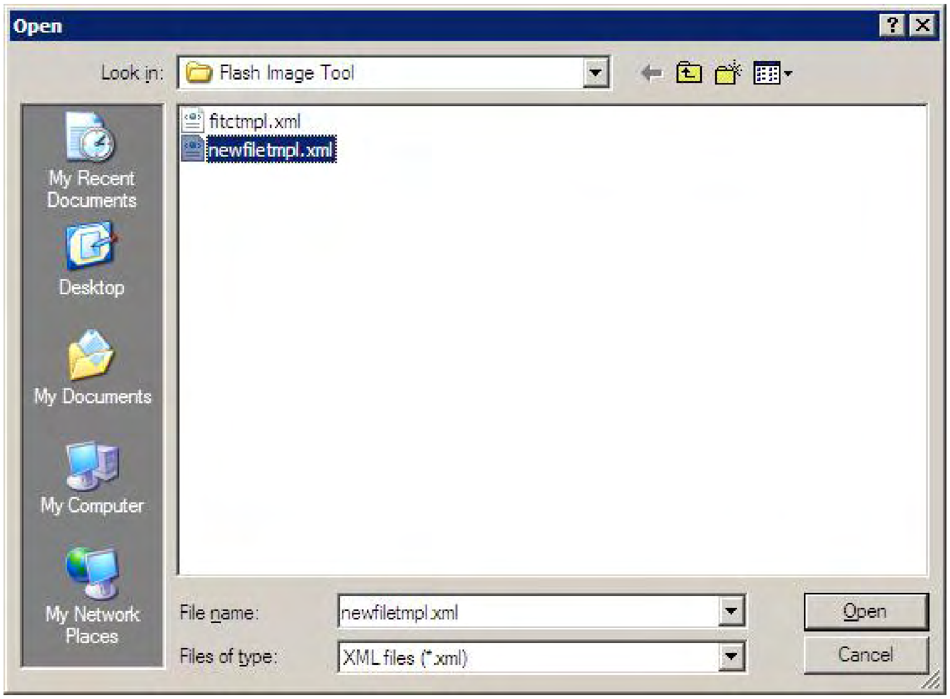
Lower Flash Block/Sector Erase Size: 4KB

Flash Partition Boundary Address: 0x00001000

Note: Leave selection box “Do not set End of Manufacturing Bit when ME Region Master Access Permissions are set to Intel Recommend” unchecked Unless it is explicitly desired not to close End of Manufacturing, when descriptor permissions are set to production values. Intel strongly recommends that the Global Lock Bit / End of Manufacturing bit is set on all production platforms.

Load the Default Settings XML File

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**.



File name: newfiletmpl.xml

Files of type: XML files (*.xml)

4.2.2 FITc Selection for CRB

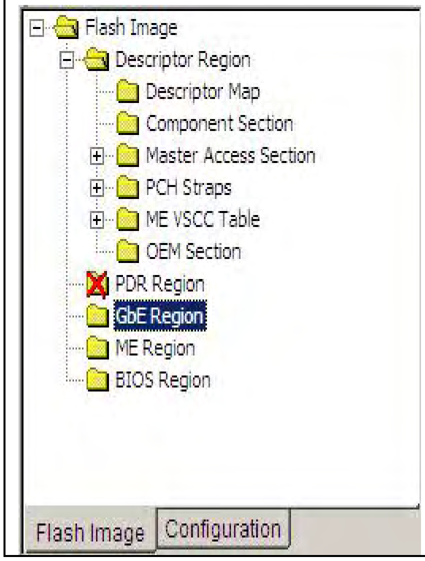
To build images for CRBs make the following selection in FITc as shown below.

4.2.3 Set Up GbE LAN PHY Firmware Region

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

Default parameter value can be used for all platform designs.
Default parameter value cannot be used. Change this value based on guidelines provided.
Parameter is read only.

1. On the navigation tree to the left, select the **Flash Image** tab. Select **Flash Image | GbE Region**. Set the parameters in the **GbE Region** section as shown in the table below.

Location	Parameter	Default	Comments
 Flash Image Descriptor Region Descriptor Map Component Section Master Access Section PCH Straps ME VSCC Table OEM Section PDR Region GbE Region ME Region BIOS Region Flash Image Configuration	GbE LAN region length	0h	
	Binary input file		Navigate to your **Source Directory** (as specified in Section **0**, page **38**) and switch to the **GbE** subdirectory. Choose the desktop or mobile Intel GbE LAN Firmware binary image.
	Major Version	0	Displays major revision value for Intel LAN GbE Firmware version when **Binary input file** is specified.
	Minor Version	0	Displays minor revision value for Intel LAN GbE Firmware version when **Binary input file** is specified.
	Image ID	0	Displays image ID value for Intel LAN GbE Firmware version when **Binary input file** is specified.

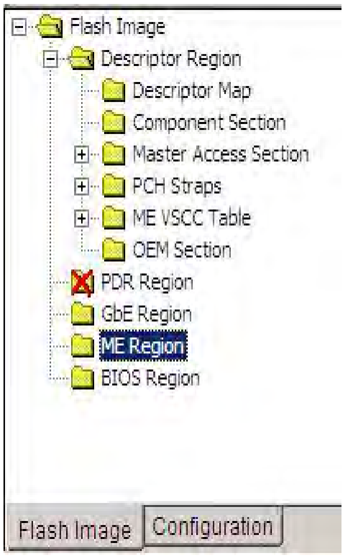
4.2.4 Set Up Intel® ME Firmware Region

Note: Selecting the Platform SKU needs to be done after the ME region has been loaded to ensure that the proper firmware settings are loaded into FITc.

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

Default parameter value can be used for all platform designs.
Default parameter value cannot be used. Change this value based on guidelines provided.
Parameter is read only.

1. On the navigation tree to the left, select the **Flash Image** tab. Select **Flash Image | ME Region**. Set the parameters in the **ME Region** section as shown in the table below.

Location	Parameter	Default	Comments
 Flash Image Descriptor Region Descriptor Map Component Section Master Access Section PCH Straps ME VSCC Table OEM Section PDR Region GbE Region ME Region BIOS Region Flash Image Configuration	Binary input file		Navigate to your **Source Directory** (as specified in Section **0**, page **38**) and switch to the **Firmware** subdirectory. Choose the Intel ME Firmware binary image. **Note:** Loading an Intel ME Firmware binary image unlocks the **ME Boot from Flash** parameter in **Flash Image | Descriptor Region | PCH Straps | PCH Strap 10** (see page **54**).
	Intel® QST config file		Enable QST navigate to the directory location where the qstbinary.bin file was created (as shown in Section **2**) **Note:** If this file is not installed QST will not be available on the platform.
	Permit file		Adds the Permit Data to the Datastore.
	* Partition Rom Bypass Enabled		Not technically a parameter. This information panel appears when an Intel ME Firmware image enables ME boot directly from flash.
	Major Version	0	Displays major revision value for Intel ME Firmware version when **Binary input file** is specified.
	Minor Version	0	Displays minor revision value for Intel ME Firmware version when **Binary input file** is specified.
	Image ID	0	Displays Intel ME Firmware image ID when **Binary input file** is specified.

Location	Parameter	Default	Comments
	Hotfix Version	0	Displays hotfix value for Intel ME Firmware version when **Binary input file** is specified.
	Build Version	0	Displays build value for Intel ME Firmware version when **Binary input file** is specified.

4.2.5 Selecting Platform SKU

Note: Selecting the Platform SKU needs to be done after the ME region has been loaded to ensure that the proper firmware settings are loaded into FITc.

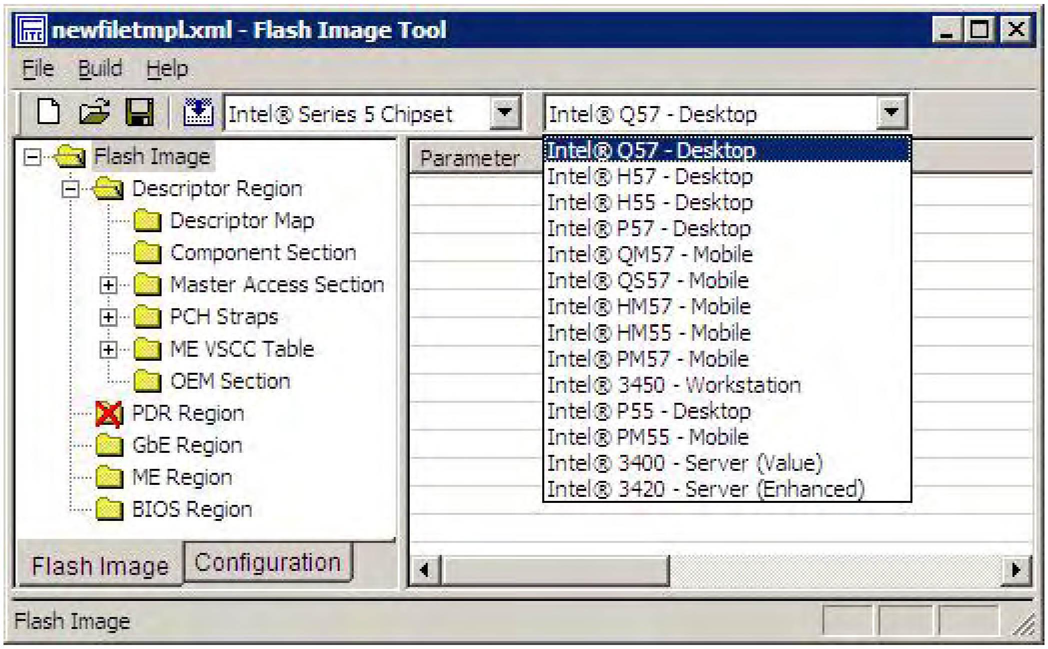
Use the SKU Manager drop down box to select the appropriate platform type for your specific chipset.

This new feature allows testing how firmware behaves with SKU'd HW using Super-SKU Ibex Peak.

– Certain features only work with particular SKUs of firmware.
(For example Intel® AMT only works with corporate SKUs)

– When a SKU is selected in FITc the Super SKU Ibex Peak will then behaves as if it were the selected SKU silicon.

The SKU Manager Selection option has no effect on Production Silicon



Note: The Features Supported and other Configuration tabs in FITc will show the appropriate changes to the firmware features under '**Configuration / Features Supported**' according to the SKU selected.

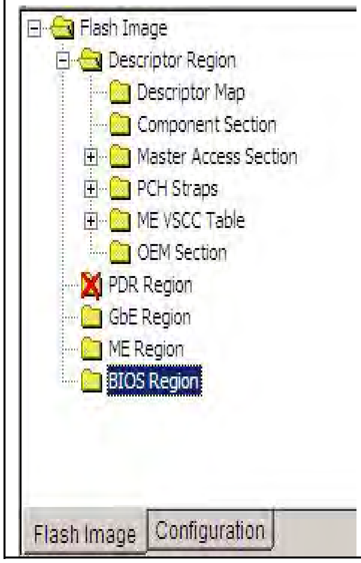
Note: For the 8MB firmware kit the only valid SKU choices are Intel® Q57, H57, H55, QM57, QS57, Intel 3450, HM57 and HM55.

4.2.6 Set Up BIOS Region

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

Default parameter value can be used for all platform designs.
Default parameter value cannot be used. Change this value based on guidelines provided.
Parameter is read only.

1. On the navigation tree to the left, select the **Flash Image** tab. Select **Flash Image | BIOS Region**.

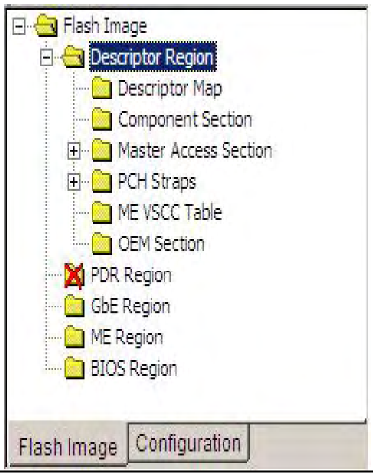
Location	Parameter	Default	Comments
	BIOS Revision		Displays BIOS revision information when **Binary input file** is specified.
	BIOS region length	0h	See Table Below.
	Binary input file		For the Intel CRB navigate to your **Source Directory** (as specified in Section Section **0**, page **38**) and switch to the **BIOS** subdirectory. Choose the desktop or mobile BIOS binary image. See Section **3** page **25**. For all other platforms point this parameter to the appropriate BIOS image.

4.2.7 Set Up Descriptor and SPI Flash Device(s)

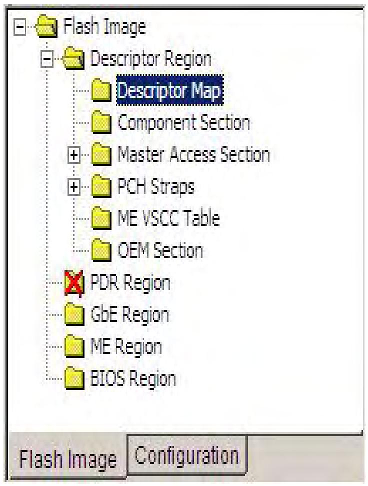
All parameters in this section are color-coded as per the key below.

Default parameter value can be used for all platform designs.
Default parameter value cannot be used. Change this value based on guidelines provided.
Parameter is read only.

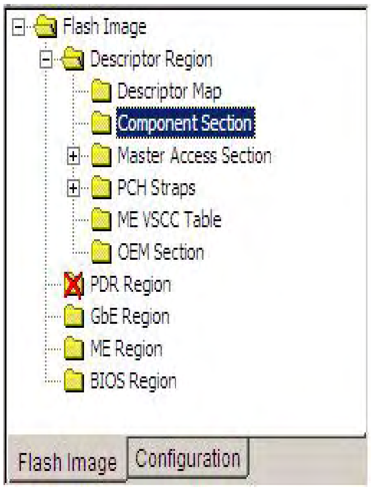
1. On the navigation tree to the left, select the **Flash Image** tab. Select **Flash Image | Descriptor Region**. Set the parameters in the **Descriptor Region** section as shown in the table below.

Location	Parameter	Default	Comments
 Flash Image Descriptor Region Descriptor Map Component Section Master Access Section PCH Straps ME VSCC Table OEM Section PDR Region GbE Region ME Region BIOS Region Flash Image Configuration	Descriptor region length	0h	Leave this at zero. Allows FIT to auto-size the descriptor region length.

2. On the navigation tree to the left, select the **Flash Image** tab. Select **Flash Image | Descriptor Region | Descriptor Map**. Set the parameters in the **Descriptor Map** section as shown in the table below.

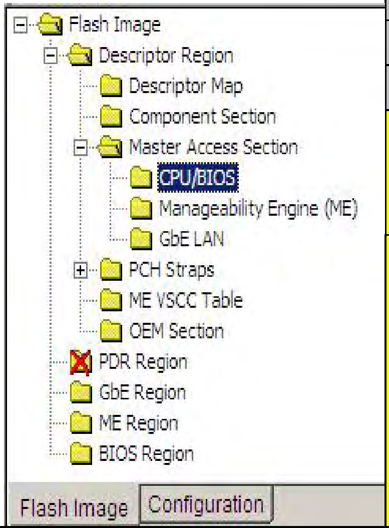
Location	Parameter	Default	Comments
 Flash Image Descriptor Region Descriptor Map Component Section Master Access Section PCH Straps ME VSCC Table OEM Section PDR Region GbE Region ME Region BIOS Region Flash Image Configuration	Region base address	4h	Flash region base address (FRBA).
	Number of flash components	2	Number of SPI flash devices on the platform. Normally set to **1** or **2**. **0** = Build ME region only.
	Component base address	2h	
	Number of PCH straps	16	
	PCH straps base address	10h	
	Number of Masters	2	
	Master base address	6h	
	Number of PROC straps	0	
	MCH straps base address	20h	

3. On the navigation tree to the left, select the **Flash Image** tab. Select **Flash Image | Descriptor Region | Component Section**. Set the parameters in the **Component Section** as shown in the table below.

Location	Parameter	Default	Comments
 Flash Image Descriptor Region Descriptor Map Component Section Master Access Section PCH Straps ME VSCC Table OEM Section PDR Region GbE Region ME Region BIOS Region Flash Image Configuration	Read ID and Read Status clock frequency	33MHz	Lowest common frequency of all SPI flash parts on the platform.
	Write and erase clock frequency	33MHz	Lowest common frequency of all SPI flash parts on the platform.
	Fast read clock frequency	33MHz	Lowest common frequency of all SPI flash parts on the platform.
	Fast read support	true	
	Read clock frequency	20MHz	
	Flash component 2 density	4MB	Size of second SPI flash part on the platform.
	Flash component 1 density	4MB	Size of first SPI flash part on the platform.
	Invalid instruction 3	0	
	Invalid instruction 2	0	
	Invalid instruction 1	0	
	Invalid instruction 0	0	

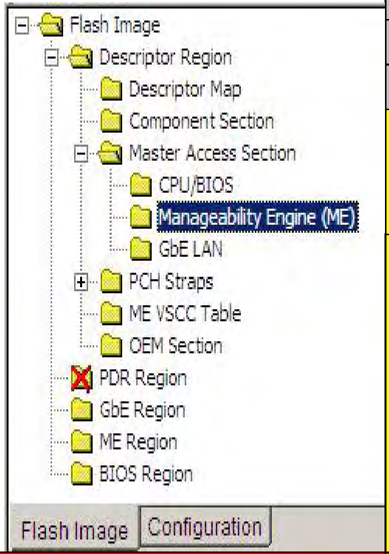
Location	Parameter	Default	Comments
	Flash Partition Boundary	0h	FPBA. Only applies to SPI flash parts with asymmetric block/sector erase sizes. Configured in main menu option **Build | Build Settings**.

4. On the navigation tree to the left, 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 in the table below.

Location	Parameter	Default	Comments
 Flash Image Descriptor Region Descriptor Map Component Section Master Access Section CPU/BIOS Manageability Engine (ME) GbE LAN PCH Straps ME VSCC Table OEM Section PDR Region GbE Region ME Region BIOS Region Flash Image Configuration	PCI Bus ID	0	
	PCI Device ID	0	
	PCI Function ID	0	
	Read access	FFh	Set to **0Bh** for a production platform. Leave at **FFh** (default) when building an SPI flash binary image for testing a platform on the lab bench.
	Write access	FFh	Set to **0Ah** for a production platform. Leave at **FFh** (default) when building an SPI flash binary image for testing a platform on the lab bench.

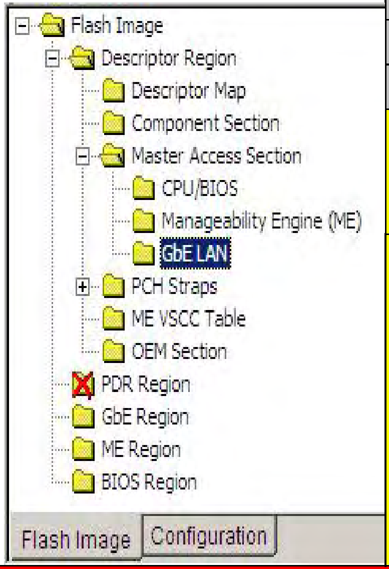
Note: If all Read/Write Master access settings for CPU/BIOS, Manageability Engine and GbE LAN are set to production platform values, then the Global Lock bit / End of Manufacturing bit will automatically be set. If the Global Lock bit / End of Manufacturing bit is set, the FOV mechanism will not be available.

5. On the navigation tree to the left, 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 in the table below.

Location	Parameter	Default	Comments
 Flash Image Descriptor Region Descriptor Map Component Section Master Access Section CPU/BIOS Manageability Engine (ME) GbE LAN PCH Straps ME VSCC Table OEM Section PDR Region GbE Region ME Region BIOS Region Flash Image Configuration	PCI Bus ID	0	
	PCI Device ID	0	
	PCI Function ID	0	
	Read access	FFh	Set to **0Dh** for a production platform. Leave at **FFh** (default) when building an SPI flash binary image for testing a platform on the lab bench.
	Write access	FFh	Set to **0Ch** for a production platform. Leave at **FFh** (default) when building an SPI flash binary image for testing a platform on the lab bench.

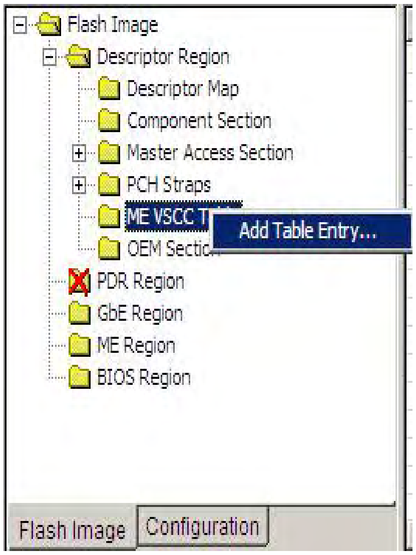
Note: If all Read/Write Master access settings for CPU/BIOS, Manageability Engine and GbE LAN are set to production platform values, then the Global Lock bit / End of Manufacturing bit will automatically be set. If the Global Lock bit / End of Manufacturing bit is set, the FOV mechanism will not be available.

6. On the navigation tree to the left, 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 in the table below.

Location	Parameter	Default	Comments
 Flash Image Descriptor Region Descriptor Map Component Section Master Access Section CPU/BIOS Manageability Engine (ME) GbE LAN PCH Straps ME VSCC Table OEM Section PDR Region GbE Region ME Region BIOS Region Flash Image Configuration	PCI Bus ID	1	
	PCI Device ID	3	
	PCI Function ID	0	
	Read access	FFh	Set to **08h** for a production platform. Leave at **FFh** (default) when building an SPI flash binary image for testing a platform on the lab bench.
	Write access	FFh	Set to **08h** for a production platform. Leave at **FFh** (default) when building an SPI flash binary image for testing a platform on the lab bench.

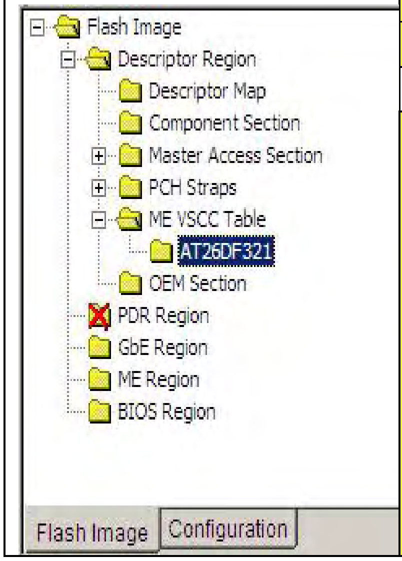
Note: If all Read/Write Master access settings for CPU/BIOS, Manageability Engine and GbE LAN are set to production platform values, then the Global Lock bit / End of Manufacturing bit will automatically be set. If the Global Lock bit / End of Manufacturing bit is set, the FOV mechanism will not be available.

7. On the navigation tree to the left, select the **Flash Image** tab. Select **Flash Image | Descriptor Region | ME VSCC Table**. Right click on **ME VSCC Table** to add entry name **AT26DF321**.

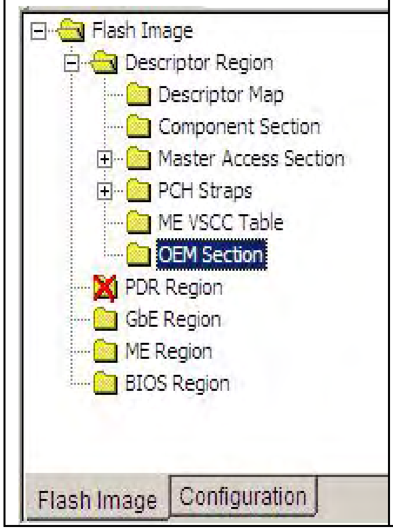


8. Select **Flash Image | Descriptor Region | ME VSCC Table** | **AT26DF321**. Set the parameters for the Atmel 4-MB SPI part in the **AT26DF321** section as shown in the table below.

Note: These VSCC Table setting are specifically for the Desktop and Mobile CRB platforms. Refer to the manufacturer specifications for your SPI flash part for proper setting information.

Location	Parameter	Default	Comments
	Vendor ID	0h	Set to **1Fh**.
	Device ID 0	0h	Set to **47h**.
	Device ID 1	0h	
	VSCC register value	0h	Set to **20152015h**.

9. On the navigation tree to the left, select the **Flash Image** tab. Select **Flash Image | Descriptor Region | OEM Section**. Set the parameters in the **OEM Section** as shown in the table below.

Location	Parameter	Default	Comments
 Flash Image Descriptor Region Descriptor Map Component Section Master Access Section PCH Straps ME VSCC Table OEM Section PDR Region GbE Region ME Region BIOS Region Flash Image Configuration	Binary input file		

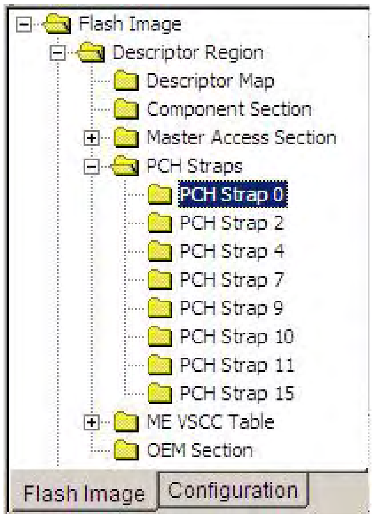
4.2.8 Set Up Soft Straps

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

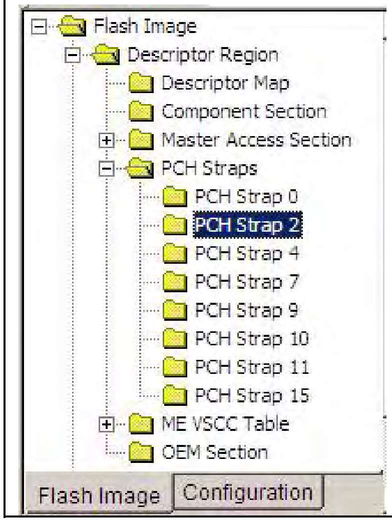
Note: For more detailed information on all Soft Strap parameters please refer to the **'PCH_SPI_ Programming_Guide'**

Default parameter value can be used for all platform designs.
Default parameter value cannot be used. Change this value based on guidelines provided.
Parameter is read only.

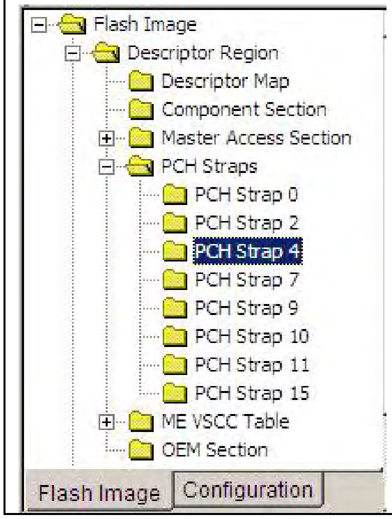
1. On the navigation tree to the left, select the **Flash Image** tab. Select **Flash Image | Descriptor Region | PCH Straps | PCH Strap 0**. Set the parameters in the **PCH Strap 0** section as shown in the table below.

Location	Parameter	Default	Comments
 Flash Image Descriptor Region Descriptor Map Component Section Master Access Section PCH Straps PCH Strap 0 PCH Strap 2 PCH Strap 4 PCH Strap 7 PCH Strap 9 PCH Strap 10 PCH Strap 11 PCH Strap 15 ME VSCC Table OEM Section Flash Image Configuration	BIOS Boot Block Size	64KB	Sets BIOS Boot Block Size
	Intel® Anti-Theft Technology Data Protection Disable	false	Leave this setting set to '**false'**
	DMI RequesterID Check Disable	false	Relevant to server platforms. Indicates if RequesterID checking during DMI accesses is disabled.
	LANPHYPC_GP12_SEL	Set to 1 (Native mode)	**0** = PCH GP12 is used as General Purpose Input/Output (GPIO) pin. **1** = PCH GP12 is used as LAN_PHYPC for Intel LAN.
	Intel® ME SMBus Enable	true	Enables Intel® ME SMBus.
	Intel® ME SMBus Frequency	100kHz	
	SMLink0 Enable	true	Enables SMLink0
	SMLink0 Frequency	100kHz	
	SMLink1 Enable	true	Enables SMLink1
	SMLink1 Frequency	100kHz	
	Chipset Config	01b	**01b** = Required value

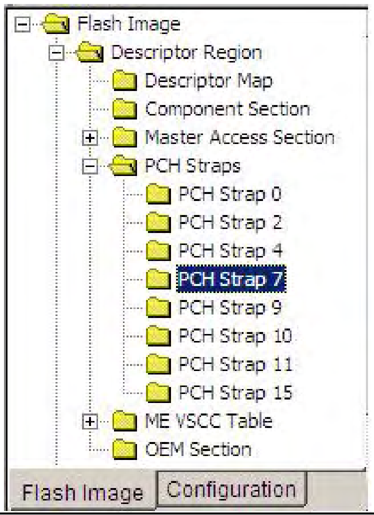
2. On the navigation tree to the left, select the **Flash Image** tab. Select **Flash Image | Descriptor Region | PCH Straps | PCH Strap 2**. Set the parameters in the **PCH Strap 2** section as shown in the table below.

Location	Parameter	Default	Comments
	SMBus I2C Address Enable (SMBI2CEN)	false	This is only for Ignition firmware testing purposes.
	SMBus I2C Address (SMBI2CA)	0h	Only valid for Ignition firmware.
	Intel[®] ME SMBus ASD Address Enable (MESMASDEN)	false	Intel[®] ME SMBus ASD Address Enable
	Intel[®] ME SMBus ASD Address (MESMASDA)	0h	Intel[®] ME SMBus ASD Address
	Intel[®] ME SMBus GP Address Enable	false	This is only for Ignition firmware testing purposes.
	Intel[®] ME SMBus GP Address	0h	This is only for Ignition firmware testing purposes.

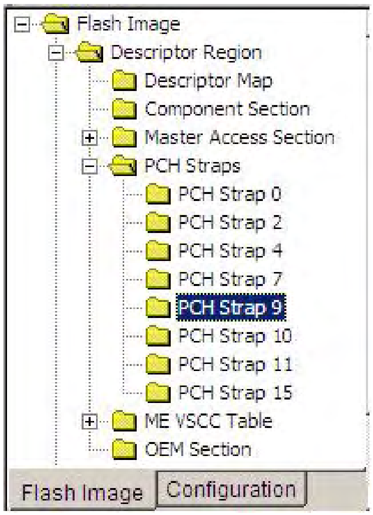
3. On the navigation tree to the left, select the **Flash Image** tab. Select **Flash Image | Descriptor Region | PCH Straps | PCH Strap 4**. Set the parameters in the **PCH Strap 4** section as shown in the table below.

Location	Parameter	Default	Comments
	GbE PHY SMBus Address	64h	Intel[®] Integrated LAN PHY SMBus Address
	GbE SMBus Address	70h	Intel[®] Integrated LAN SMBus Address
	GbE SMBus Address Enable	true	Intel[®] Integrated LAN SMBus Address enable
	PHY Connectivity	10: PHY on SMLink0	Determines if the LAN PHY is connected the SMBus2 segment.

4. On the navigation tree to the left, select the **Flash Image** tab. Select **Flash Image | Descriptor Region | PCH Straps | PCH Strap 7**. Set the parameters in the **PCH Strap 7** section as shown in the table below.

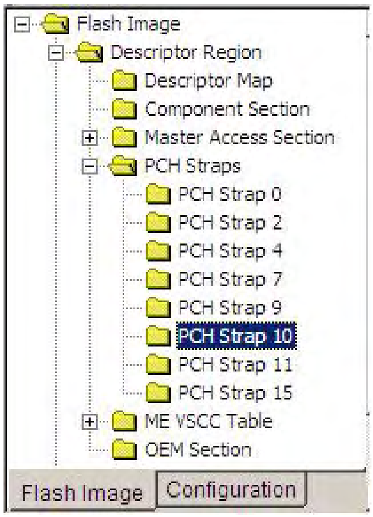
Location	**Parameter**	**Default**	**Comments**
 Flash Image Descriptor Region Descriptor Map Component Section Master Access Section PCH Straps PCH Strap 0 PCH Strap 2 PCH Strap 4 PCH Strap 7 PCH Strap 9 PCH Strap 10 PCH Strap 11 PCH Strap 15 ME VSCC Table OEM Section Flash Image Configuration	Intel® ME SMBus Subsystem Vendor & Device ID for ASF2	0	Intel® ME SMBus Subsystem Vendor & Device ID for ASF2

5. On the navigation tree to the left, select the **Flash Image** tab. Select **Flash Image | Descriptor Region | PCH Straps | PCH Strap 9**. Set the parameters in the **PCH Strap 9** section as shown in the table below.

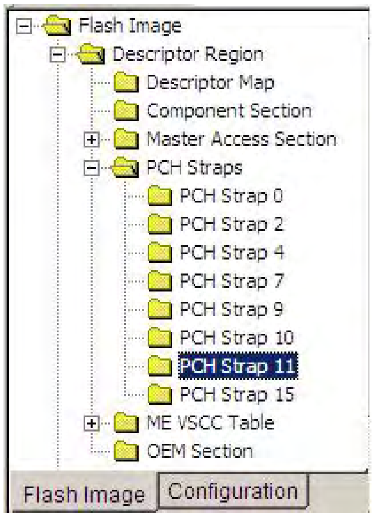
Location	**Parameter**	**Default**	**Comments**
 Flash Image Descriptor Region Descriptor Map Component Section Master Access Section PCH Straps PCH Strap 0 PCH Strap 2 PCH Strap 4 PCH Strap 7 PCH Strap 9 PCH Strap 10 PCH Strap 11 PCH Strap 15 ME VSCC Table OEM Section Flash Image Configuration	Intel® PHY Over PCI Express Enable (PHY_PCIE_EN)	true	**true** = Intel LAN is present **false** = Third-party LAN is present
	Intel® PHY PCIe Port Select (PHY_PCIEPORSEL)	101:Port 6	Only necessary if Intel LAN is present. **000** = Port 1 **001** = Port 2 **010** = Port 3 **011** = Port 4 **100** = Port 5 **101** = Port 6 **110** = Port 7 **111** = Port 8 This parameter must reflect platform topology.
	DMI Lane Reversal	false	This parameter must reflect platform topology. **Note:** If using the SFF Reference board this value needs to be set to '**true**'
	PCIe Lane Reversal 2	false	This parameter must reflect platform topology.
	PCIe Lane Reversal 1	false	This parameter must reflect platform topology.

Location	Parameter	Default	Comments
	PCIe Port Configuration 2	00: 4x1 Ports 5-8 (x1)	***Desktop CRB values*** - **00: 4x1 Ports 5-8 (x1)** ***Mobile CRB values*** **- 10: 2x2 Port 5 (x2), Port 7 (x2), Ports 6, 8 (disabled)**. This parameter must reflect platform topology.
	PCIe Port Configuration 1	00: 4x1 Ports 1-4 (x1)	This parameter must reflect platform topology.

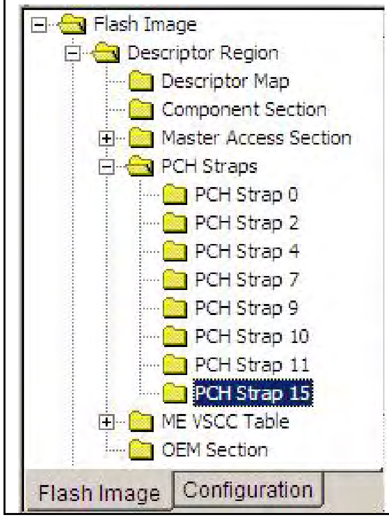
6. On the navigation tree to the left, select the **Flash Image** tab. Select **Flash Image \| Descriptor Region \| PCH Straps \| PCH Strap 10**. Set the parameters in the **PCH Strap 10** section as shown in the table below.

Location	Parameter	Default	Comments
 Flash Image Descriptor Region Descriptor Map Component Section Master Access Section PCH Straps PCH Strap 0 PCH Strap 2 PCH Strap 4 PCH Strap 7 PCH Strap 9 PCH Strap 10 PCH Strap 11 PCH Strap 15 ME VSCC Table OEM Section Flash Image Configuration	ME boot from flash	false	This option is read-only until an Intel ME Firmware binary image is loaded. See Section **4.2.4**
	ME MDDD Enable	false	**true** = Enable MDDD logging **false =** Disable MDDD logging
	ME MDDD Address	0x00	MDDD Address Set this to a value of '**0x38**' for MDDD logging.
	ICC OEM Config Select	0	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, up to 8 sets total.
	ME Reset Capture on CL_RST#	false	Determines if ME will assert at CL_RST#. **true =** ME will assert at the CL_RST# when it resets. **false =** ME will not asset at the CL_RST#.
	ME Debug – Emergency Mode Enable	false	This option enables the Net debug support: **false** = disabled **true** = Net debug enabled

7. On the navigation tree to the left, 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 in the table below.

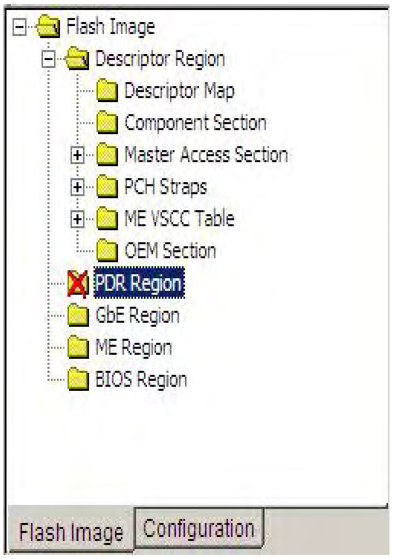
Location	Parameter	Default	Comments
 Flash Image Descriptor Region Descriptor Map Component Section Master Access Section PCH Straps PCH Strap 0 PCH Strap 2 PCH Strap 4 PCH Strap 7 PCH Strap 9 PCH Strap 10 PCH Strap 11 PCH Strap 15 ME VSCC Table OEM Section Flash Image Configuration	SMLink1 I2C Address Enable	true	***This must be set to true on any platform that uses PCH SMBus Thermal Reporting solution. This must be set to true for all Mobile platforms.*** Please see PCH SPI programming guide Softstrap Appendix for more Details.
	SMLink1 I2C Address	0x4Ch	The address 0x4C is the address required for Intel CRB. Please check with your BIOS and H/W designer to ensure that this address does not conflict. Please see PCH SPI programming guide Softstrap Appendix for more Details.
	SMLink1 GP Address Enable	true	***This must be set to true on any platform that uses PCH SMBus Thermal Reporting solution. This must be set to true for all Mobile platforms.*** Please see PCH SPI programming guide Softstrap Appendix for more Details.
	SMLink1 GP Address	0x4Bh	The address 0x4B is the address required for Intel CRB. Please check with your BIOS and H/W designer to ensure that this address does not conflict. Please see PCH SPI programming guide Softstrap Appendix for more Details.

8. On the navigation tree to the left, 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 in the table below.

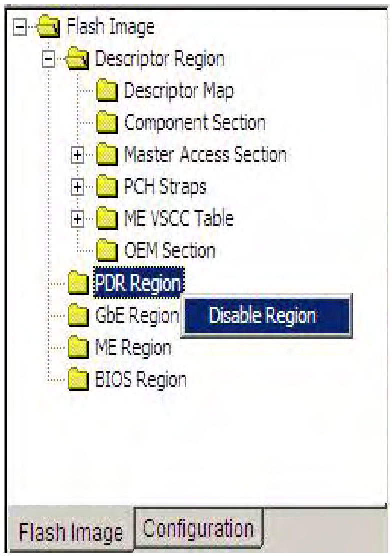
Location	Parameter	Default	Comments
 Flash Image Descriptor Region Descriptor Map Component Section Master Access Section PCH Straps PCH Strap 0 PCH Strap 2 PCH Strap 4 PCH Strap 7 PCH Strap 9 PCH Strap 10 PCH Strap 11 PCH Strap 15 ME VSCC Table OEM Section Flash Image Configuration	t209 Timing	1ms	t209 minimum timing value
	Intel® Integrated LAN Enable	true	Enables / Disables the Intel® Integrated LAN.

4.2.9 Disable Platform Data Store Region

1. On the navigation tree to the left, select the **Flash Image** tab. Select **Flash Image | PDR Region**. Ensure that the region is disabled (indicated by a red “X”).



If not, disable it by right-clicking on **Flash Image | PDR Region** and selecting **Disable Region** as shown below.



4.2.10 Configuration Parameters

The Configuration tab located at the bottom of the FITc window allows the user to set specific parameters.

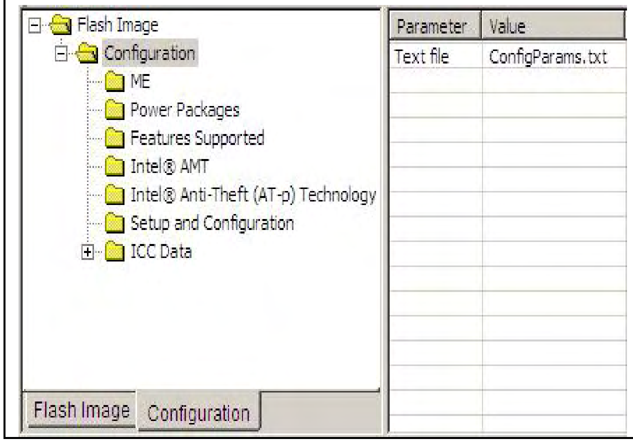
Note: ME region should be loaded before modifying any of the Configuration Parameters. Any Configuration Parameter data modified before the ME Regions is loaded will be lost.

If any of the parameters are changed from the Intel recommended value the offending row will be highlighted yellow. No errors will be reported. The highlighted yellow is designed to draw attention to these values were ensure these parameters were set correctly.

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

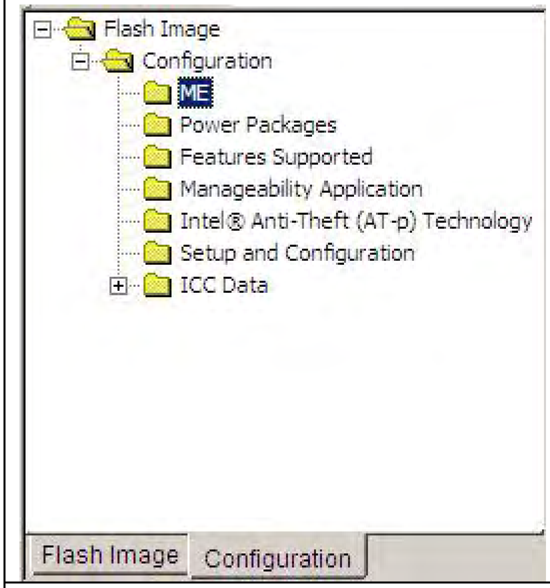
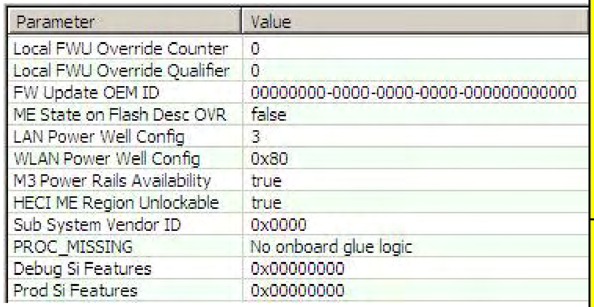
Default parameter value can be used for all platform designs.
Default parameter value cannot be used. Change this value based on guidelines provided.
Parameter is read only.

1. On the navigation tree to the left, select the **Configuration** tab. Select **Configuration** as shown below.

Location	Parameter	Default	Comments
	Text file	ConfigParams.txt	This value will allow the user to set the NVARs text file. The NVARs text file contains the values of all the parameters set in the NVARs region. This text file can be used in the command line argument to modify the default ME parameters using the “/nvars” option.

Parameter	Value
Text file	ConfigParams.txt

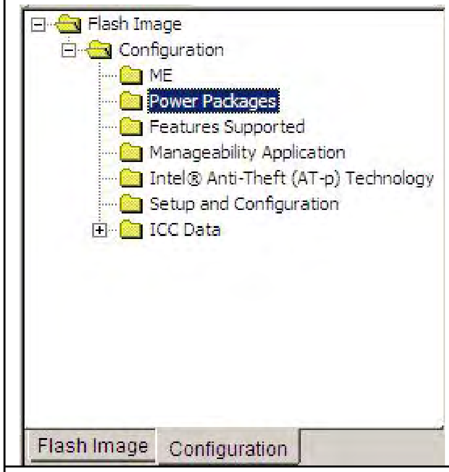
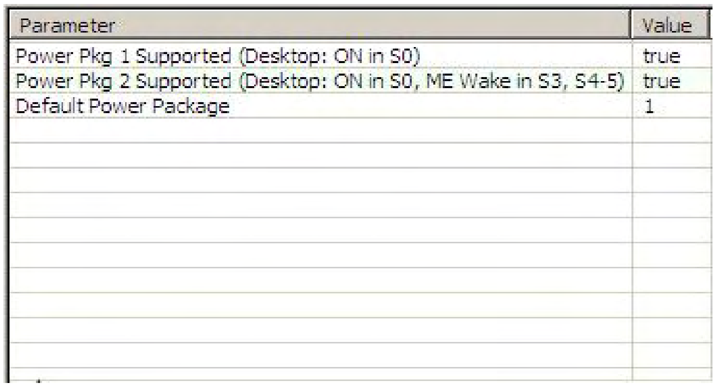
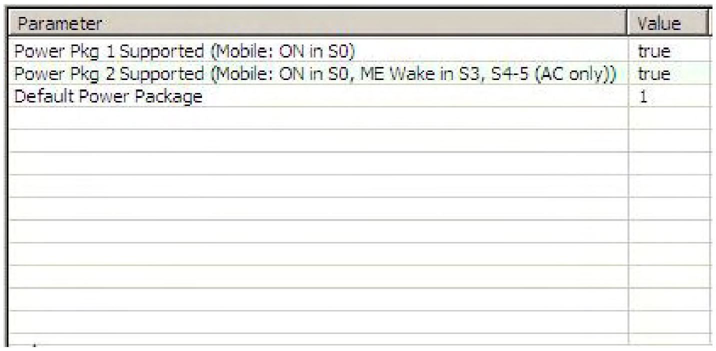
2. On the navigation tree to the left, select the **Configuratio**n tab. Select **ME** as shown below.

<table>
<tr><th>Location

Flash Image
Configuration
ME
Power Packages
Features Supported
Manageability Application
Intel® Anti-Theft (AT-p) Technology
Setup and Configuration
ICC Data
Flash Image Configuration</th><th>Parameter</th><th>Default</th><th>Comments</th></tr>
<tr><td rowspan="4"><table><tr><th>Parameter</th><th>Value</th></tr><tr><td>Local FWU Override Counter</td><td>0</td></tr><tr><td>Local FWU Override Qualifier</td><td>0</td></tr><tr><td>FW Update OEM ID</td><td>00000000-0000-0000-0000-000000000000</td></tr><tr><td>ME State on Flash Desc OVR</td><td>false</td></tr><tr><td>LAN Power Well Config</td><td>3</td></tr><tr><td>WLAN Power Well Config</td><td>0x80</td></tr><tr><td>M3 Power Rails Availability</td><td>true</td></tr><tr><td>HECI ME Region Unlockable</td><td>true</td></tr><tr><td>Sub System Vendor ID</td><td>0x0000</td></tr><tr><td>PROC_MISSING</td><td>No onboard glue logic</td></tr><tr><td>Debug Si Features</td><td>0x00000000</td></tr><tr><td>Prod Si Features</td><td>0x00000000</td></tr></table></td><td>Local FWU Override Counter</td><td>1</td><td>This parameter overrides the <b>MEBx</b> settings for local firmware update.
This value is configurable between <b>-1</b> and <b>255</b>.
(See <b>Appendix C.1</b>)</td></tr>
<tr><td>Local Firmware Override Qualifier</td><td>0</td><td>This parameter determines behavior for local firmware updates.
(See <b>Appendix C.1</b>)</td></tr>
<tr><td>FW Update OEM ID</td><td>00000000-0000-0000-0000-000000000000</td><td>This UUID will make sure that customers can only update a platform with an image coming from the platform OEM. If set to an all zero value then any input is valid when doing a firmware update.</td></tr>
<tr><td>ME State on Flash Desc OVR</td><td>false</td><td>This parameter controls ME behavior for Descriptor Override (GPIO33).
(See <b>Appendix C.2</b>)</td></tr>
</table>

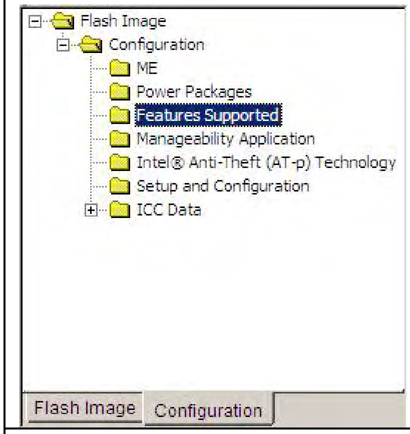
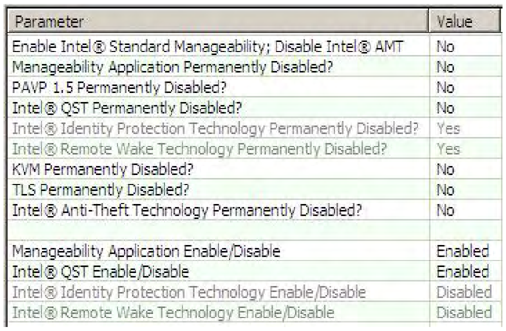
Location			
	LAN Power Well Config	3	This parameter determines the Power Well configuration for Intel® Wired LAN
	WLAN Power Well Config	0x80	This parameter determines the Power Well configuration for Intel® Wireless LAN **0x80 – Desktop** **0x84 - Mobile**
	M3 Power Rails Availability	true	This value will determine if M3 functionality will be available for firmware. For the Desktop and Mobile CRB platforms this value needs to be set to '**true**'. **Note:** M3 Power Rail availability depends on the specific platform design and needs to be set appropriately. For platforms with M3 support the value needs to be set **'true'** for proper firmware operation. For platforms without M3 support this value needs to be set to **'false'** for proper firmware operation.
	HECI ME Region Unlockable	true	Determines if Soft GPIO33 is available

Location			
	Sub System Vendor ID	0x0000	Used ONLY by Intel(R) Upgrade Service. This feature is currently available only on Intel(R) Q57 Express Chipsets. If enabling Intel(R) Upgrade Service, refer the MTP User Guide that is available after registration for detail on how to set this field. Registration and login is available at http://upgrades.intel.com
	PROC_Missing	No onboard glue logic	This value will determines if glue logic is present on desktop platform to detect a missing processor
	Debug Si Features	0x00000000	This parameter determines firmware Si debug features. (See **Appendix C.3**)
	Prod Si Features	0x00000000	This parameter determines firmware Si debug features. (See **Appendix C.3**)

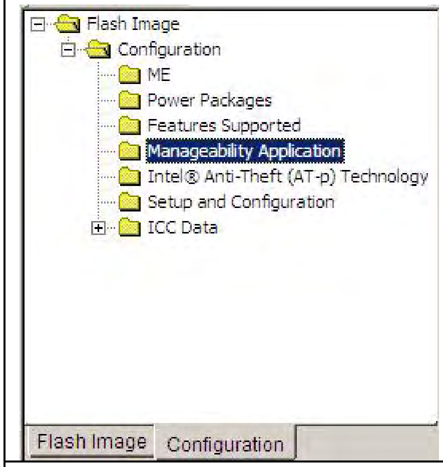
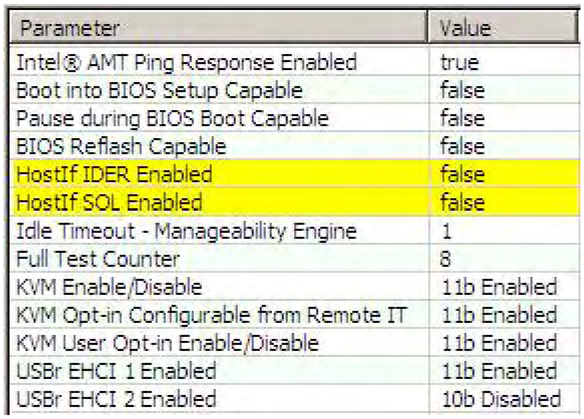
3. On the navigation tree to the left, select the **Configuration** tab. Select **Power Packages** as shown below.

<table>
<tr><th>Location

Flash Image
Configuration
ME
Power Packages
Features Supported
Manageability Application
Intel® Anti-Theft (AT-p) Technology
Setup and Configuration
ICC Data
Flash Image
Configuration</th><th>Parameter</th><th>Default</th><th>Comments</th></tr>
<tr><td rowspan="3">Desktop Power Packages
<table><tr><th>Parameter</th><th>Value</th></tr><tr><td>Power Pkg 1 Supported (Desktop: ON in S0)</td><td>true</td></tr><tr><td>Power Pkg 2 Supported (Desktop: ON in S0, ME Wake in S3, S4-5)</td><td>true</td></tr><tr><td>Default Power Package</td><td>1</td></tr></table></td><td>Power Pkg 1 Supported (Desktop: On in S0)</td><td>true</td><td>This parameter configures ME for S0 operation only.</td></tr>
<tr><td>Power Pkg 2 Supported (Desktop: On in S0, ME Wake in S3, S4-5)</td><td>true</td><td>This parameter configures ME for operation in S0 and ME Wake in S3, S4 and S5.</td></tr>
<tr><td>Default Power Package</td><td>1</td><td>This parameter determines the default Power Package used by firmware image.</td></tr>
<tr><td rowspan="3">Mobile Power Packages
<table><tr><th>Parameter</th><th>Value</th></tr><tr><td>Power Pkg 1 Supported (Mobile: ON in S0)</td><td>true</td></tr><tr><td>Power Pkg 2 Supported (Mobile: ON in S0, ME Wake in S3, S4-5 (AC only))</td><td>true</td></tr><tr><td>Default Power Package</td><td>1</td></tr></table></td><td>Power Pkg 1 Supported (Mobile: On in S0)</td><td>true</td><td>This parameter configures ME for S0 operation only.</td></tr>
<tr><td>Power Pkg 2 Supported (Mobile: On in S0, ME Wake in S3, S4-5)</td><td>true</td><td>This parameter configures ME for operation in S0 and ME Wake in S3, S4 and S5.</td></tr>
<tr><td>Default Power Package</td><td>1</td><td>This parameter determines the default Power Package used by firmware image.</td></tr>
</table>

4. On the navigation tree to the left, select the **Configuration** tab. Select **Features Supported** as shown below. See for further details about features supported for each SKU **Appendix** C.4

Location	Parameter	Default	Comments
 Flash Image Configuration ME Power Packages Features Supported Manageability Application Intel® Anti-Theft (AT-p) Technology Setup and Configuration ICC Data Flash Image Configuration			These options control the availability / visibility of firmware features. In instances where a specific feature is configurable in the MEBx disabling it through the 'Features Supported' section will hide / disable that specific feature in the MEBx.
 Parameter Value Enable Intel® Standard Manageability; Disable Intel® AMT No Manageability Application Permanently Disabled? No PAVP 1.5 Permanently Disabled? No Intel® QST Permanently Disabled? No Intel® Identity Protection Technology Permanently Disabled? Yes Intel® Remote Wake Technology Permanently Disabled? Yes KVM Permanently Disabled? No TLS Permanently Disabled? No Intel® Anti-Theft Technology Permanently Disabled? No Manageability Application Enable/Disable Enabled Intel® QST Enable/Disable Enabled Intel® Identity Protection Technology Enable/Disable Disabled Intel® Remote Wake Technology Enable/Disable Disabled This section is divided into two sub sections separated by a blank row: **Permanently disabled sub section (top section)** 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 **The "Shipping state" sub section (the lower sub section)** This determines the state that an OEM would ship a specific ME Application. This state (enabled /disabled) can be later changed through available interfaces such as MEBx / USB / Agent / Management Console etc.	Enable Intel® Standard Manageability; Disable Intel® AMT	No	**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. See for further details about features supported for each SKU Appendix C.4
	Intel® Manageability Application Permanently Disabled?	No	
	PAVP 1.5 Permanently Disabled?	No	
	Intel® QST Permanently Disabled?	No	
	Intel® Identity Protection Technology Permanently Disabled?	Yes	
	Intel® Remote Wake Technology Permanently Disabled?	Yes	
	KVM Permanently Disabled?	No	
	TLS Permanently Disabled?	No	
	Intel® Anti-Theft Technology Permanently Disabled?	No	
	Intel® Manageability Application Enable / Disable	Enabled	ME Application State – This determines the state that an OEM would ship a specific ME Application – This state (enabled /disabled) can be later changed through available interfaces such as MEBx / USB / Agent / Management Console etc. See for further details about features supported for each SKU Appendix C.4
	Intel® QST Enable / Disable	Enabled	
	Intel® Identity Protection Technology Enable / Disable	Disabled	
	Intel® Remote Wake Technology Enable / Disable	Disabled	

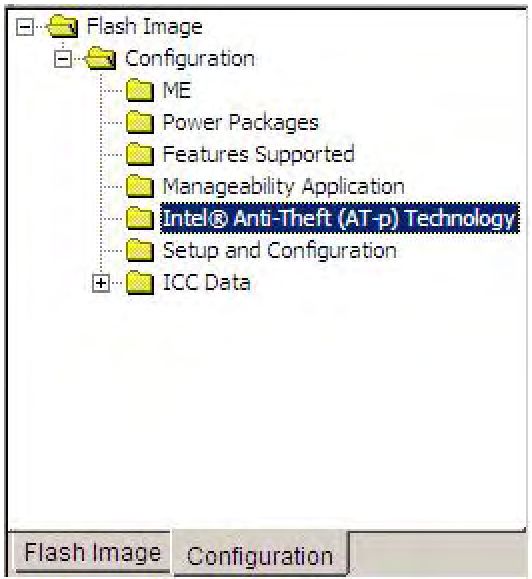
5. On the navigation tree to the left, select the **Configuration** tab. Select **Manageability Application** as shown below.

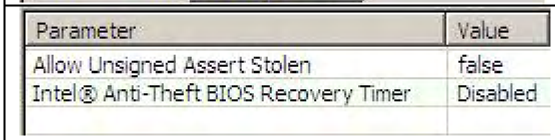
Location			
 Flash Image Configuration ME Power Packages Features Supported Manageability Application Intel® Anti-Theft (AT-p) Technology Setup and Configuration ICC Data Flash Image · Configuration	**Parameter**	**Default**	**Comments**
	Intel® AMT Ping Response Enabled	true	
	Boot into BIOS Setup Capable	false	
	Pause during BIOS Boot Capable	false	
	BIOS Reflash Capable	false	
	HostIf IDER Enabled	false	Enables / Disables IDEr redirection in base firmware image. true = IDEr enabled in default image false = IDEr disabled in default image
	HostIf SOL Enabled	false	Enables / Disables SOL redirection in base firmware image. true = SOL enabled in default image false = SOL disabled in default image

Parameter	Value
Intel® AMT Ping Response Enabled	true
Boot into BIOS Setup Capable	false
Pause during BIOS Boot Capable	false
BIOS Reflash Capable	false
HostIf IDER Enabled	false
HostIf SOL Enabled	false
Idle Timeout - Manageability Engine	1
Full Test Counter	8
KVM Enable/Disable	11b Enabled
KVM Opt-in Configurable from Remote IT	11b Enabled
KVM User Opt-in Enable/Disable	11b Enabled
USBr EHCI 1 Enabled	11b Enabled
USBr EHCI 2 Enabled	10b Disabled

Location			
	Idle Timeout – Manageability Engine	65535	
	Full Test Counter	8	
	KVM Enable / Disable	11b Enabled	This setting determines if the KVM feature is enabled or disabled
	KVM Opt-In Configurable from Remote IT	11b Enabled	This setting determines if the Network Administrator remotely control the KVM Opt in setting.
	KVM Opt-In Enable / Disable	11b Enabled	This setting determines if user consent is required to enter KVM sessions.
Note: Disabling both EHCI parameters will not disable the EHCI interfaces. When none of the EHCI parameters are set to enabled, the firmware will automatically enable and use EHCI1	USBr EHCI 1 Enabled	11b Enabled	
	USBr EHCI 2 Enabled	10b Disabled	

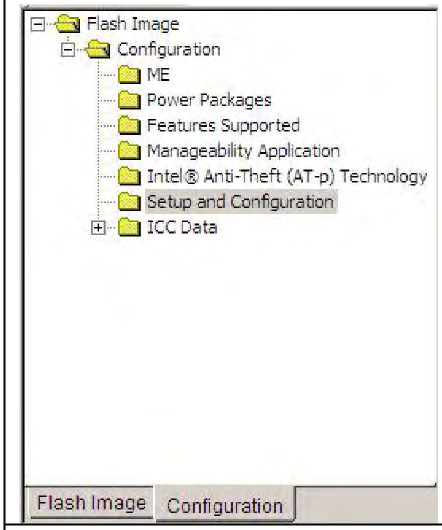
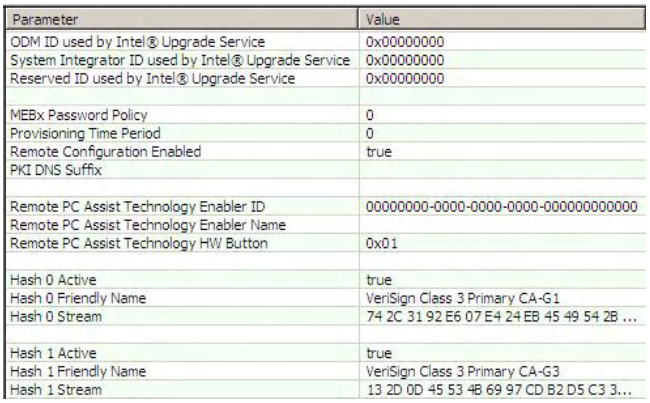
6. On the navigation tree to the left, select the **Configuration** tab. Select **Intel® Anti-Theft** (Intel® AT-p) Technology as shown below.

Location			
 Flash Image Configuration ME Power Packages Features Supported Manageability Application Intel® Anti-Theft (AT-p) Technology Setup and Configuration ICC Data Flash Image Configuration	**Parameter**	**Default**	**Comments**

Parameter — Value
Allow Unsigned Assert Stolen — false
Intel® Anti-Theft BIOS Recovery Timer — Disabled
	Allow Unsigned Assert Stolen	false	true = The Unsigned Assert Stolen is enabled
			false = The Unsigned Assert Stolen is disabled.

	Intel® Anti-Theft BIOS Recovery Timer	Disabled	This timer will enable a 30 minute window to allow a FW / BIOS re-flash before the system is powered down

7. On the navigation tree to the left, select the **Configuration** tab. Select **Setup and Configuration** as shown below.

Location	Parameter	Default	Comments
 Flash Image Configuration ME Power Packages Features Supported Manageability Application Intel® Anti-Theft (AT-p) Technology Setup and Configuration ICC Data Flash Image Configuration			
Parameter Value ODM ID used by Intel® Upgrade Service 0x00000000 System Integrator ID used by Intel® Upgrade Service 0x00000000 Reserved ID used by Intel® Upgrade Service 0x00000000 MEBx Password Policy 0 Provisioning Time Period 0 Remote Configuration Enabled true PKI DNS Suffix Remote PC Assist Technology Enabler ID 00000000-0000-0000-0000-000000000000 Remote PC Assist Technology Enabler Name Remote PC Assist Technology HW Button 0x01 Hash 0 Active true Hash 0 Friendly Name VeriSign Class 3 Primary CA-G1 Hash 0 Stream 74 2C 31 92 E6 07 E4 24 EB 45 49 54 2B ... Hash 1 Active true Hash 1 Friendly Name VeriSign Class 3 Primary CA-G3 Hash 1 Stream 13 2D 0D 45 53 4B 69 97 CD B2 D5 C3 3...	ODM ID used by Intel® Upgrade Service	0x00000000	Used ONLY by Intel(R) Upgrade Service. These features are currently available only on Intel(R) Q57 Express Chipsets. If enabling Intel(R) Upgrade Service, refer the MTP User Guide that is available after registration for detail on how to set this field. Registration and login is available at http://upgrades.intel.com
	System Integrator ID used by Intel® Upgrade Service	0x00000000	
	Reserved ID Used by Intel® Upgrade Service	0x00000000	
	MEBx Password Policy	0	
	Provisioning Time Period	0	

Location			
	Remote Configuration Enabled	true	
	PKI DNS Suffix		
	Remote PC Assist Technology Enabler Id	0	This value must be programmed with your OEM specific Id if you enable RCS in your image.
	Remote PC Assist Technology Enabler Name		This value must be programmed with your OEM specific RCS Enabler name.
	Remote PC Assist Technology HW Button	0x01	
	Hash 0 Active	true	(See **Appendix 0**)
	Hash 0 Friendly Name	VeriSign Class 3 Primary CA-G1	
	Hash 0 Stream	74 2C 31 92 E6 07 E4 24 EB 45 49 54 2B E1 BB C5 3E 61 74 E2	
	Hash 1 Active	true	
	Hash 1 Friendly Name	VeriSign Class 3 Primary CA-G3	
	Hash 1 Stream	13 2D 0D 45 53 4B 69 97 CD B2 D5 C3 39 E2 55 76 60 9B 5C C6	
	Hash 2 Active	true	
	Hash 2 Friendly Name	Go Daddy Class 2 CA	
	Hash 2 Stream	27 96 BA E6 3F 18 01 E2 77 26 1B A0 D7 77 70 02 8F 20 EE E4	
	Hash 3 Active	true	

Location			
	Hash 3 Friendly Name	Comodo AAA CA	
	Hash 3 Stream	D1 EB 23 A4 6D 17 D6 8F D9 25 64 C2 F1 F1 60 17 64 D8 E3 49	
	Hash 4 Active	true	
	Hash 4 Friendly Name	Starfield Class 2 CA	
	Hash 4 Stream	AD 7E 1C 28 B0 64 EF 8F 60 03 40 20 14 C3 D0 E3 37 0E B5 8A	
	Hash 5 Active	true	
	Hash 5 Friendly Name	VeriSign Class 3 Primary CA-G2	
	Hash 5 Stream	85 37 1C A6 E5 50 14 3D CE 28 03 47 1B DE 3A 09 E8 F8 77 0F	
	Hash 6 Active	false	
	Hash 6 Friendly Name		
	Hash 6 Stream		
	Hash 7 Active	false	
	Hash 7 Friendly Name		
	Hash 7 Stream		
	Hash 8 Active	false	
	Hash 8 Friendly Name		
	Hash 8 Stream		
	Hash 9 Active	false	
	Hash 9 Friendly Name		
	Hash 9 Stream		
	Hash 10 Active	false	

Location			
	Hash 10 Friendly Name		
	Hash 10 Stream		
	Hash 11 Active	false	
	Hash 11 Friendly Name		
	Hash 11 Stream		
	Hash 12 Active	false	
	Hash 12 Friendly Name		
	Hash 12 Stream		
	Hash 13 Active	false	
	Hash 13 Friendly Name		
	Hash 13 Stream		
	Hash 14 Active	false	
	Hash 14 Friendly Name		
	Hash 14 Stream		
	Hash 15 Active	false	
	Hash 15 Friendly Name		
	Hash 15 Stream		
	Hash 16 Active	false	
	Hash 16 Friendly Name		
	Hash 16 Stream		
	Hash 17 Active	false	
	Hash 17 Friendly Name		
	Hash 17 Stream		
	Hash 18 Active	false	
	Hash 18 Friendly Name		
	Hash 18 Stream		
	Hash 19 Active	false	

Location			
	Hash 19 Friendly Name		
	Hash 19 Stream		
	Hash 20 Active	false	
	Hash 20 Friendly Name		
	Hash 20 Stream		
	Hash 21 Active	false	
	Hash 21 Friendly Name		
	Hash 21 Stream		
	Hash 22 Active	false	
	Hash 22 Friendly Name		
	Hash 22 Stream		

4.2.11 Program Clock Control Parameters

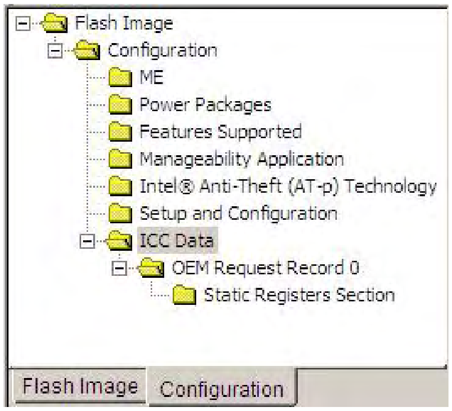
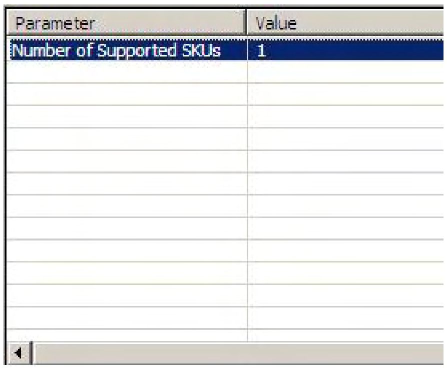
All parameters in this section are color-coded as per the key below.

Default parameter value can be used for all platform designs.
🟨 Your platform may require different parameter value. See parameter guidelines for more details.
▨ Parameter is read only.

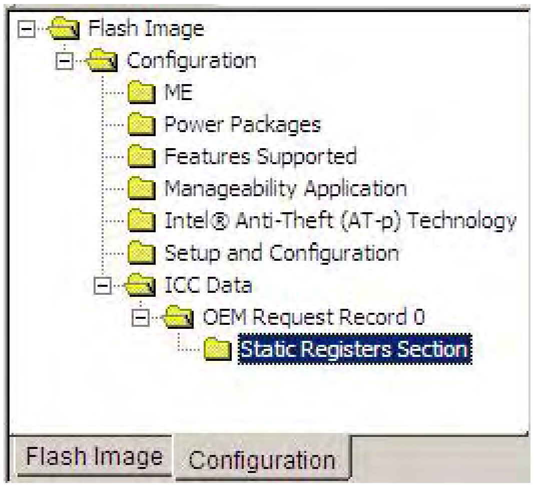
1. On the navigation tree to the left, select the **Configuration** tab. Select **Flash Image | Configuration | ICC Data**. Set the parameters in the **ICC Data** section as shown in the table below.

If testing/validating HDMI and DisplayPort* interfaces with Intel integrated graphics on your platform, significant changes need to be made to how you configure platform clocks. Please refer IBL document #425135 (Display Clock Integration – Technical Advisory 1.0) for the current POR change information on clock programming.

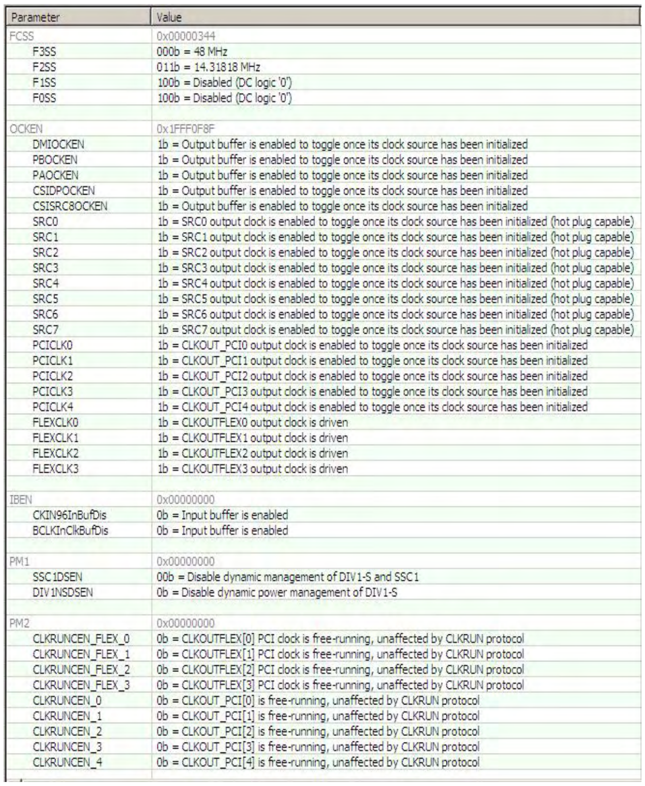
All other platform configurations may continue to use the clock programming steps outlined below.

Location	Parameter	Default	Comments
 Flash Image Configuration ME Power Packages Features Supported Manageability Application Intel® Anti-Theft (AT-p) Technology Setup and Configuration ICC Data OEM Request Record 0 Static Registers Section Flash Image Configuration	Number of Supported SKUs	1	Specify how many sets of clock configuration parameters need to be specified. It is possible that a clock control parameter set is required for each separate board design.
 Parameter: Number of Supported SKUs, Value: 1			

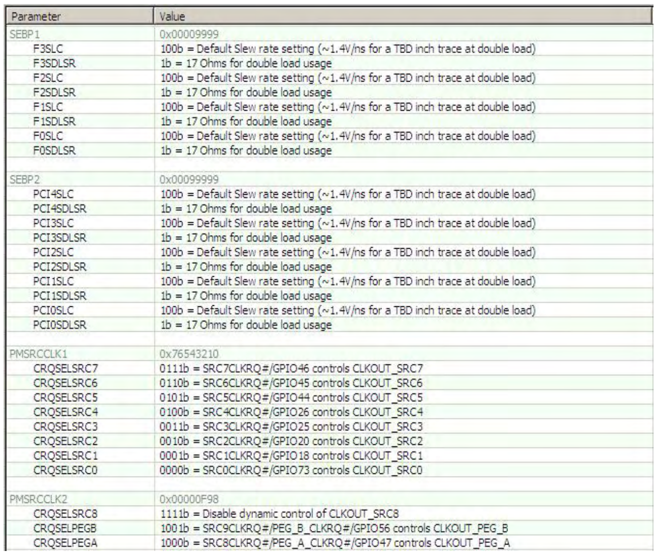
2. On the navigation tree to the left, select the Configuration tab. Select Flash Image | Configuration | ICC Data | OEM Req. Rec. Block | OEM Request Record 0 | Static Registers Section. Set the parameters in the Static Registers Section as shown in the table below.

Location	Parameter	Default	Comments
 Flash Image Configuration ME Power Packages Features Supported Manageability Application Intel® Anti-Theft (AT-p) Technology Setup and Configuration ICC Data OEM Request Record 0 Static Registers Section Flash Image Configuration	FCSS	0x00000344	Turn off unsupported clock output on CLKOUTFLEX2 and CLKOUTFLEX1. Thus: • F3SS = **000b = 48 MHz** • F2SS = **011b = 14.31818 MHz** • F1SS = **100b = Disabled (DC logic '0')** • F0SS = **100b = Disabled (DC logic '0')** See Section **A.2.1** for further details **Set CRB to:** **0x0000**4322: • F3SS = **10**0b = Disabled • F2SS = **011b = 14** MHz • F1SS = **010b** = 33.3 MHz **F0SS =** 010b **= 33.3 MHz**

Location	Parameter	Default	Comments
	PLLEN	0x8000040C	This parameter controls PLL enables. See Section **A.2.2**, page **104**. **0x8000040C** = Display Clock Intergration (DCI) Mode clock generation for Display Clock (PCH generation from 25-MHz crystal). • For the CRB, use this with MPG BIOS 072 or CG BIOS 154 or later. • Non-CRB BIOS requires VBIOS that supports DCI. • Use in OS requires Intel<Superscript>®<NonSuperscript> Graphics Accelerator Driver support for DCI. **0x8000041B** = Use this setting if platform supports external graphics only **0x8000041C** = Buffer Through Mode clock generation for Display Clock (CK505 generation from 14-MHz crystal). • This option may be used if the platform does not support any digital display outputs (DVI, HDMI, DisplayPort*) • For the CRB, use this with BIOSes earlier than MP072 or CG154. **Default is** 0x8000040C**.**
	OCKEN	0x1FFF0F8F	See Section **A.2.3** for further details

Location	Parameter	Default	Comments
	IBEN	0x00000000	See Section **A.2.5** for further details
	DIVEN	0x00000303	This parameter controls PLL enables. See Section **A.2.6**, page **108**. **0x00000303** = Display Clock Intergration (DCI) Mode clock generation for Display Clock. **0x00000100** = Use this setting if platform supports external graphics only **0x00000003** = Buffer Through Mode clock generation for Display Clock. **Default is** 0x00000303. **CRB is** 0x00000303.
	PM1	0x00000013	Allows VBIOS and Integrated Graphics Device driver to power manage DIV1S (see **A.2.7**, page **110**). This setting is also safe for processors without Integrated Graphics.
	PM2	0x00000000	See Section **A.2.8** for further details

Parameter	Value
FCSS	0x00000344
F3SS	000b = 48 MHz
F2SS	011b = 14.31818 MHz
F1SS	100b = Disabled (DC logic '0')
F0SS	100b = Disabled (DC logic '0')
OCKEN	0x1FFF0F8F
DMIOCKEN	1b = Output buffer is enabled to toggle once its clock source has been initialized
PBOCKEN	1b = Output buffer is enabled to toggle once its clock source has been initialized
PAOCKEN	1b = Output buffer is enabled to toggle once its clock source has been initialized
CSIDPOCKEN	1b = Output buffer is enabled to toggle once its clock source has been initialized
CSISRC8OCKEN	1b = Output buffer is enabled to toggle once its clock source has been initialized
SRC0	1b = SRC0 output clock is enabled to toggle once its clock source has been initialized (hot plug capable)
SRC1	1b = SRC1 output clock is enabled to toggle once its clock source has been initialized (hot plug capable)
SRC2	1b = SRC2 output clock is enabled to toggle once its clock source has been initialized (hot plug capable)
SRC3	1b = SRC3 output clock is enabled to toggle once its clock source has been initialized (hot plug capable)
SRC4	1b = SRC4 output clock is enabled to toggle once its clock source has been initialized (hot plug capable)
SRC5	1b = SRC5 output clock is enabled to toggle once its clock source has been initialized (hot plug capable)
SRC6	1b = SRC6 output clock is enabled to toggle once its clock source has been initialized (hot plug capable)
SRC7	1b = SRC7 output clock is enabled to toggle once its clock source has been initialized (hot plug capable)
PCICLK0	1b = CLKOUT_PCI0 output clock is enabled to toggle once its clock source has been initialized
PCICLK1	1b = CLKOUT_PCI1 output clock is enabled to toggle once its clock source has been initialized
PCICLK2	1b = CLKOUT_PCI2 output clock is enabled to toggle once its clock source has been initialized
PCICLK3	1b = CLKOUT_PCI3 output clock is enabled to toggle once its clock source has been initialized
PCICLK4	1b = CLKOUT_PCI4 output clock is enabled to toggle once its clock source has been initialized
FLEXCLK0	1b = CLKOUTFLEX0 output clock is driven
FLEXCLK1	1b = CLKOUTFLEX1 output clock is driven
FLEXCLK2	1b = CLKOUTFLEX2 output clock is driven
FLEXCLK3	1b = CLKOUTFLEX3 output clock is driven
IBEN	0x00000000
CKIN96InBufDis	0b = Input buffer is enabled
BCLKInClkBufDis	0b = Input buffer is enabled
PM1	0x00000000
SSC1DSEN	00b = Disable dynamic management of DIV1-S and SSC1
DIV1NSDSEN	0b = Disable dynamic power management of DIV1-S
PM2	0x00000000
CLKRUNCEN_FLEX_0	0b = CLKOUTFLEX[0] PCI clock is free-running, unaffected by CLKRUN protocol
CLKRUNCEN_FLEX_1	0b = CLKOUTFLEX[1] PCI clock is free-running, unaffected by CLKRUN protocol
CLKRUNCEN_FLEX_2	0b = CLKOUTFLEX[2] PCI clock is free-running, unaffected by CLKRUN protocol
CLKRUNCEN_FLEX_3	0b = CLKOUTFLEX[3] PCI clock is free-running, unaffected by CLKRUN protocol
CLKRUNCEN_0	0b = CLKOUT_PCI[0] is free-running, unaffected by CLKRUN protocol
CLKRUNCEN_1	0b = CLKOUT_PCI[1] is free-running, unaffected by CLKRUN protocol
CLKRUNCEN_2	0b = CLKOUT_PCI[2] is free-running, unaffected by CLKRUN protocol
CLKRUNCEN_3	0b = CLKOUT_PCI[3] is free-running, unaffected by CLKRUN protocol
CLKRUNCEN_4	0b = CLKOUT_PCI[4] is free-running, unaffected by CLKRUN protocol

Location	Parameter	Default	Comments
	SEBP1	0x00009999	See Section **A.2.9** for further details
	SEBP2	0x00099999	See Section **A.2.10** for further details
	PMSRCCLK1	0xFFFFFFFF	See Section **A.2.12** for further details
	PMSRCCLK1	0x00000FFF	See Section **A.2.13** for further details

Parameter	Value
SEBP1	0x00009999
F3SLC	100b = Default Slew rate setting (~1.4V/ns for a TBD inch trace at double load)
F3SDLSR	1b = 17 Ohms for double load usage
F2SLC	100b = Default Slew rate setting (~1.4V/ns for a TBD inch trace at double load)
F2SDLSR	1b = 17 Ohms for double load usage
F1SLC	100b = Default Slew rate setting (~1.4V/ns for a TBD inch trace at double load)
F1SDLSR	1b = 17 Ohms for double load usage
F0SLC	100b = Default Slew rate setting (~1.4V/ns for a TBD inch trace at double load)
F0SDLSR	1b = 17 Ohms for double load usage
SEBP2	0x00099999
PCI4SLC	100b = Default Slew rate setting (~1.4V/ns for a TBD inch trace at double load)
PCI4SDLSR	1b = 17 Ohms for double load usage
PCI3SLC	100b = Default Slew rate setting (~1.4V/ns for a TBD inch trace at double load)
PCI3SDLSR	1b = 17 Ohms for double load usage
PCI2SLC	100b = Default Slew rate setting (~1.4V/ns for a TBD inch trace at double load)
PCI2SDLSR	1b = 17 Ohms for double load usage
PCI1SLC	100b = Default Slew rate setting (~1.4V/ns for a TBD inch trace at double load)
PCI1SDLSR	1b = 17 Ohms for double load usage
PCI0SLC	100b = Default Slew rate setting (~1.4V/ns for a TBD inch trace at double load)
PCI0SDLSR	1b = 17 Ohms for double load usage
PMSRCCLK1	0x76543210
CRQSELSRC7	0111b = SRC7CLKRQ#/GPIO46 controls CLKOUT_SRC7
CRQSELSRC6	0110b = SRC6CLKRQ#/GPIO45 controls CLKOUT_SRC6
CRQSELSRC5	0101b = SRC5CLKRQ#/GPIO44 controls CLKOUT_SRC5
CRQSELSRC4	0100b = SRC4CLKRQ#/GPIO26 controls CLKOUT_SRC4
CRQSELSRC3	0011b = SRC3CLKRQ#/GPIO25 controls CLKOUT_SRC3
CRQSELSRC2	0010b = SRC2CLKRQ#/GPIO20 controls CLKOUT_SRC2
CRQSELSRC1	0001b = SRC1CLKRQ#/GPIO18 controls CLKOUT_SRC1
CRQSELSRC0	0000b = SRC0CLKRQ#/GPIO73 controls CLKOUT_SRC0
PMSRCCLK2	0x00000F98
CRQSELSRC8	1111b = Disable dynamic control of CLKOUT_SRC8
CRQSELPEGB	1001b = SRC9CLKRQ#/PEG_B_CLKRQ#/GPIO56 controls CLKOUT_PEG_B
CRQSELPEGA	1000b = SRC8CLKRQ#/PEG_A_CLKRQ#/GPIO47 controls CLKOUT_PEG_A

Note: Each dword parameter shown below is further broken down bit by bit in Flash Image Tool. Reference these bits in Section **A.2** (page **102**).

3. Repeat the last step **OEM Request Record 1** through **OEM Request Record 7**, as necessary.

The following clock control parameters have a high level of impact on platform boot. Inspect the configurations below to determine if they apply:

Table 4-1 Flash Image | Configuration | ICC Data | OEM Request Record 0 | Dynamic Registers Section

Location	Parameter	CRB Set To	Settings for Any Platform
On the navigation tree to the left: • Select the **Configuration** tab. • Select **Flash Image | Configuration | ICC Data| OEM Request Record 0 | Static Registers Section** • Set the parameters in the **Dynamic R**egisters Section section as shown • Each dword parameter shown below is further broken down bit by bit in Flash Image Tool. Reference these bits in Section A.2 (page 102)	SSCCTL	0x1010100	This parameter controls spread spectrum modulation capability of SSC blocks. See Section A.2.2, page 103. **0x1010100** = Display Clock Intergration (DCI) Mode clock generation for Display Clock. **0x1010101** = Use this setting if platform supports external graphics only **0x1010101** = Buffer Through Mode clock generation for Display Clock. Default is **0x1010100**.

Table 4-2 High Impact Clock Control Parameters

Clock Output Pin	XML Symbol and Bit Offsets	Default	Description
CLKOUT_FLEX3	FCSS[14:12]	000b	**FLEXCLK3 Source Select (F3SS):** Selects the source of clock to be driven out on CLKOUTFLEX3. **000b** = 48 MHz **001b** = Reserved **010b** = 33.3 MHz **011b** = 14.31818 MHz **100b** = Disabled (DC logic '0') **101b** = Disabled (DC logic '0') **110b** = Disabled (DC logic '0') **111b** = Reserved *Note:* **These clock select settings only take effect when this muxed FLEXCLK/GPIO pin is configured for FLEXCLK native usage. Refer to the *Ibex Peak EDS* for configuration of GPIO vs. native usage.**
CLKOUT_FLEX3	SEBP1[12]	1b	**FLEXCLK3 Single/Double Load Series Resistance (F3SDLSR):** Sets programmable series resistance for CLKOUTFLEX3. 0b **= 25 Ohms for single load usage** 1b **= 17 Ohms for double load usage**
CLKOUT_FLEX2	FCSS[10:8]	000b	**FLEXCLK2 Source Select (F3SS):** Selects the source of clock to be driven out on CLKOUTFLEX2. 000b **= Reserved** 001b **= Reserved** 010b **= 33.3 MHz** 011b **= 14.31818 MHz** 100b **= Disabled (DC logic '0')** 101b **= Disabled (DC logic '0')** 110b **= Disabled (DC logic '0')** 111b **= Reserved**
CLKOUT_FLEX2	SEBP1[8]	1b	**FLEXCLK2 Single/Double Load Series Resistance (F2SDLSR):** Sets programmable series resistance for CLKOUTFLEX2. 0b **= 25 Ohms for single load usage** 1b **= 17 Ohms for double load usage**
CLKOUT_FLEX1	FCSS[6:4]	011b	**FLEXCLK1 Source Select (F1SS):** Selects the source of clock to be driven out on CLKOUTFLEX1. **000b** = Reserved **001b** = Reserved **010b** = 33.3 MHz **011b** = 14.31818 MHz **100b** = Disabled (DC logic '0') **101b** = Disabled (DC logic '0') **110b** = Disabled (DC logic '0') **111b** = Reserved

Clock Output Pin	XML Symbol and Bit Offsets	Default	Description
			Note: **These clock select settings only take effect when this muxed FLEXCLK/GPIO pin is configured for FLEXCLK native usage. Refer to the *Ibex Peak EDS* for configuration of GPIO vs. native usage.**
CLKOUT_FLEX1	SEBP1[4]	1b	**FLEXCLK1 Single/Double Load Series Resistance (F1SDLSR):** Sets programmable series resistance for CLKOUTFLEX1. 0b **= 25 Ohms for single load usage** 1b **= 17 Ohms for double load usage**
CLKOUT_FLEX0	FCSS[2:0]	100b	**FLEXCLK0 Source Select (F0SS):** Selects the source of clock to be driven out on CLKOUTFLEX0. **000b** = Reserved **001b** = Reserved **010b** = 33.3 MHz **011b** = 14.31818 MHz **100b** = Disabled (DC logic ‘0’) **101b** = Disabled (DC logic ‘0’) **110b** = Disabled (DC logic ‘0’) **111b** = Reserved *Note:* **These clock select settings only take effect when this muxed FLEXCLK/GPIO pin is configured for FLEXCLK native usage. Refer to the *Ibex Peak EDS* for configuration of GPIO vs. native usage.**
CLKOUT_FLEX0	SEBP1[0]	1b	**FLEXCLK0 Single/Double Load Series Resistance (F0SDLSR):** Sets programmable series resistance for CLKOUTFLEX0. 0b **= 25 Ohms for single load usage** 1b **= 17 Ohms for double load usage**
CLKOUT_PCI4	SEBP2[16]	1b	**PCI4 Single/Double Load Series Resistance (PCI4SDLSR):** Sets programmable series resistance for CLKOUT_PCI4. 0b **= 25 Ohms for single load usage** 1b **= 17 Ohms for double load usage**
CLKOUT_PCI3	SEBP2[12]	1b	**PCI3 Single/Double Load Series Resistance (PCI3SDLSR):** Sets programmable series resistance for CLKOUT_PCI3. 0b **= 25 Ohms for single load usage** 1b **= 17 Ohms for double load usage**
CLKOUT_PCI2	SEBP2[8]	1b	**PCI2 Single/Double Load Series Resistance (PCI2SDLSR):** Sets programmable series resistance for CLKOUT_PCI2. 0b **= 25 Ohms for single load usage** 1b **= 17 Ohms for double load usage**

Clock Output Pin	XML Symbol and Bit Offsets	Default	Description
CLKOUT_PCI1	SEBP2[4]	1b	**PCI1 Single/Double Load Series Resistance (PCI1SDLSR):** Sets programmable series resistance for CLKOUT_PCI1. 0b = **25 Ohms for single load usage** 1b = **17 Ohms for double load usage**
CLKOUT_PCI0	SEBP2[0]	1b	**PCI0 Single/Double Load Series Resistance (PCI0SDLSR):** Sets programmable series resistance for CLKOUT_PCI0. 0b = **25 Ohms for single load usage** 1b = **17 Ohms for double load usage**

4.2.12 Save Your Settings (Optional)

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)** directory for easy access.

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

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

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

where:

- **<xml_file>** – The XML configuration file saved when configuring using the flash image tool.
- **/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 FIT, if necessary.

4.2.13 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 Section, page **38**)

4.3 Burning the SPI Flash Image Binary

Now that the SPI flash binary image file has been created, it can be programmed into the SPI flash device of the target machine. Either a flash programmer/burner or Flash Programming Tool can be used.

4.4 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 **0**, page **38**) where your generated SPI flash binary images 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 or images. For multiple SPI flash devices, the images are numbered sequentially to correspond to the first and second SPI flash device accordingly.

4.5 Flash Programming Tool

Flash Programming Tool (FPT) can be used to substitute for a flash burner/programmer provided the system is capable of booting to an Operating System (OS).

Note: On platforms with ME already enabled you need to disable the ME before flashing the image.

1. Enter the MEBx using the CRTL-P option presented during system boot.
2. Select the Intel® ME Configuration menu option and hit the 'Y' key.
3. Hit Enter on the Intel® ME State Control option.
4. Use the cursor ↑ ↓ and select the 'Disabled' option and hit the 'Enter' key.
5. Hit ESC to exit back to the previous menu.
6. Use the cursor ↑ ↓to select 'Exit' and hit the 'Enter' key then hit the 'Y' key.

4.5.1 DOS Version

The DOS version of FPT is supported on the following operating systems: DOS, Free DOS, and DRMK DOS. Windows XP SP2 and Windows PE.

1. Check DOS FPT directory contents. Using Explorer*, navigate to **(root)\Tools\System Tools\Flash Programming Tool\DOS**. Ensure that FPT DOS' directory contents are intact (see Section **3.2**, page **26**).
2. Copy the contents of DOS FPT directory to the root directory of a bootable USB drive.

3. Navigate to your **Output Directory** (as specified in Section Section **0**, page **38**) where your generated SPI flash binary images are saved. It is assumed that this image file is named **outimage.bin**. Copy this file to the root directory of a bootable USB drive.
4. Inventory the SPI flash devices on the target system. Boot the target system, change directory to the root directory of the bootable USB drive, and 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 ---
AT26DF321 ID: 0x1F4700 Size: 4096KB (32768Kb)
AT26DF321 ID: 0x1F4700 Size: 4096KB (32768Kb)
```

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

5. Program the SPI flash binary image. Change directory to the root directory of the bootable USB drive, and at the DOS prompt type:

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

4.5.2 Windows* Version

The Windows* version of FPT is supported on the following operating systems: Windows XP SP2 and Windows PE.

1. Check Windows* FPT directory contents. Using Explorer*, navigate to **(root)\Tools\System Tools\Flash Programming Tool\Windows**. Ensure that FPT Windows*' directory contents are intact (see Section **3.2**, page **26**).
2. Copy the contents of Windows* FPT directory to the root directory of a standard USB drive.
3. Navigate to your **Output Directory** (as specified in Section Section **0**, page **38**) where your generated SPI flash binary images are saved. It is assumed that this image file is named **outimage.bin**. Copy this file to the root directory of a standard USB drive.
4. Inventory the SPI flash devices on the target system. Boot the target system to Windows*, change directory (using Command Prompt) to the root directory of the bootable USB drive, and at the command line prompt type:

```
fptw.exe /i
```

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

```
--- Flash Devices Found ---
AT26DF321 ID: 0x1F4700 Size: 4096KB (32768Kb)
AT26DF321 ID: 0x1F4700 Size: 4096KB (32768Kb)
```

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

5. Program the SPI flash binary image. Change directory (using Command Prompt) to the root directory of the bootable USB drive, and at the command line prompt type:

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

§

5 Intel® Remote PC Assist Technology (Intel® RPAT)

This section is only applicable if Intel® Remote PC Assist Technology is to be configured on the target platform. This section only describes Intel® RPAT specific parameters not covered or to be changed in section 4.1 and 4.2.

- This section describes additional/ changed soft straps that need to be set to enable Intel® RPAT.
- There are two options for Intel® RPAT which are for Consumer and Business (vPro) system. Both described in separate section below.
- Please note that if hardware, BIOS or Intel® ME FW loaded on the platform does not support Intel® RPAT then Intel® RPAT cannot be enabled.
- Remote Connectivity Service Capability" Bit has no functional meaning to RPAT. Enabling/ Disabling this bit do not Enable/ Disable Intel® RPAT.

Note: Section 4.1 and 4.2 should be followed to configure all parameters. Parameters specific to RPAT will be described below. For all parameters not described below, values should be configured as per section 4.1 and 4.2

5.1 Intel® RPAT Consumer Firmware Bringup Process:

In order to bring up a RPAT consumer supported platform the following stages **must** be addressed – detailed description that includes screen shots located below:

5.1.1 Intel® RPAT Consumer Bring Up

Please Follow sections 4.1 – 4.2.1 as described above (Assemble the SPI Flash Binary Image, Set Up the Build Environment).

5.1.2 Selecting Intel® RPAT Consumer Platform SKU

This feature allows testing how firmware behaves with SKU'd HW using Super-SKU Ibex Peak.

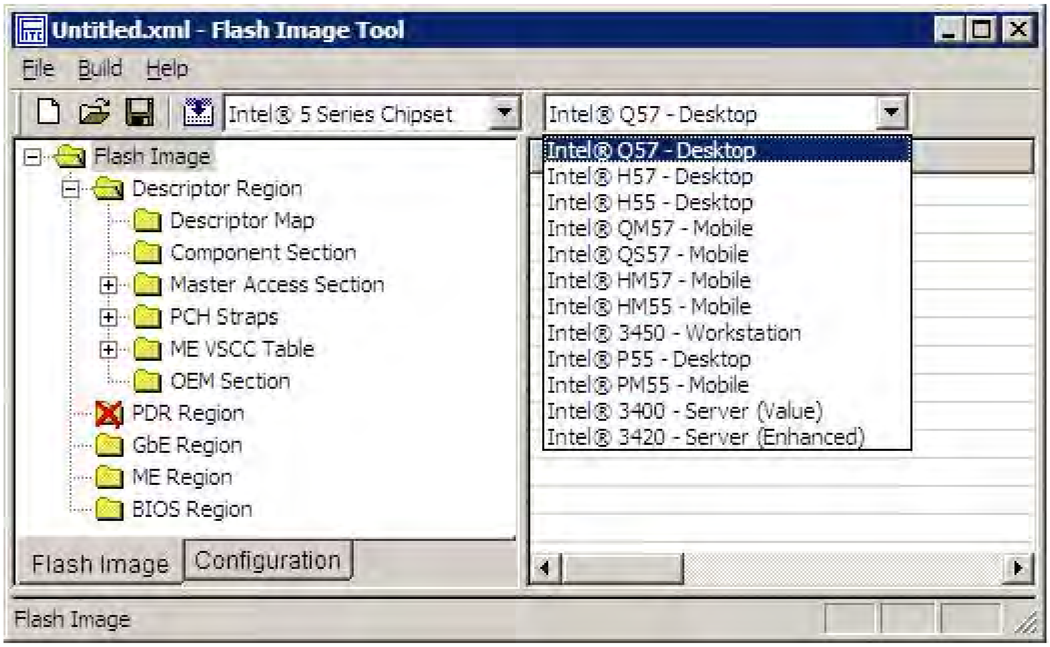
– Certain features only work with particular SKUs of firmware.
(For example Intel® AMT only works with corporate SKUs)

– When a SKU is selected in FITc the Super SKU Ibex Peak will then behave as if it were the selected SKU silicon from Intel ME perspective.

Intel® RPAT Consumer Platform supports several SKUs, please select the appropriate platform type for your specific chipset (to be configured in the table below):

- For Desktop– **H57, H55**
- For Mobile - **HM57, PM57**

Note:- The SKU Manager Selection option has no effect on Production Silicon



Note: The Features Supported and other Configuration tabs in FITc will show the appropriate changes to the firmware features under '**Configuration / Features Supported**' according to the SKU selected.

5.1.3 Intel® RPAT Consumer bring up continued

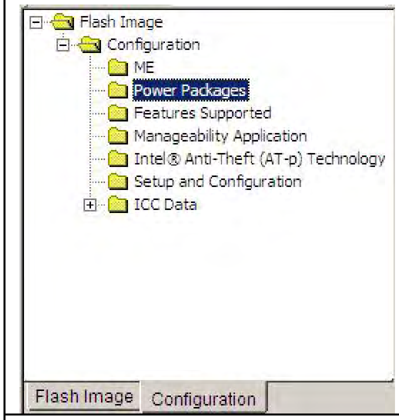
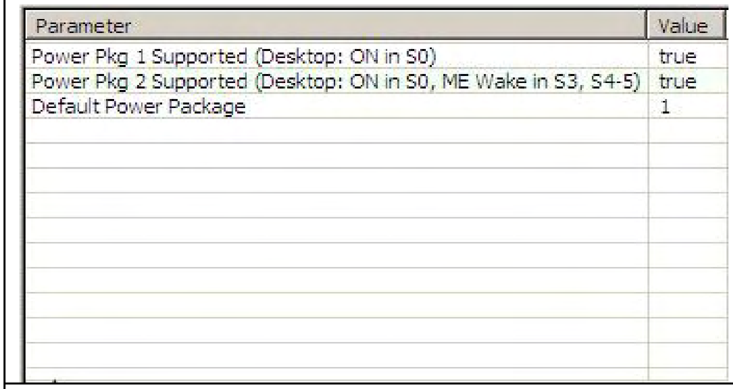
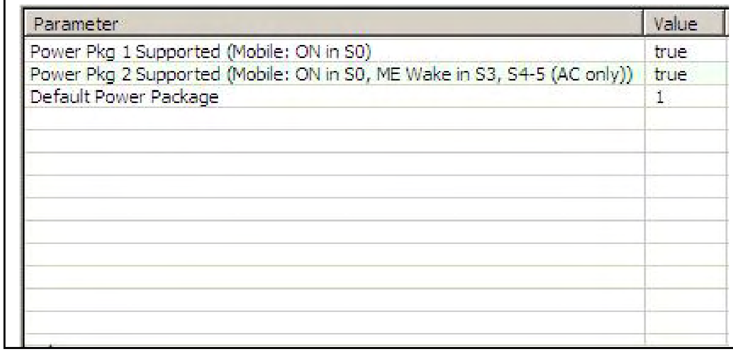
Follow instructions in sections 4.2.3 – 4.2.10 (including) as describe above.

5.1.4 Intel® RPAT Consumer Configuration Parameters

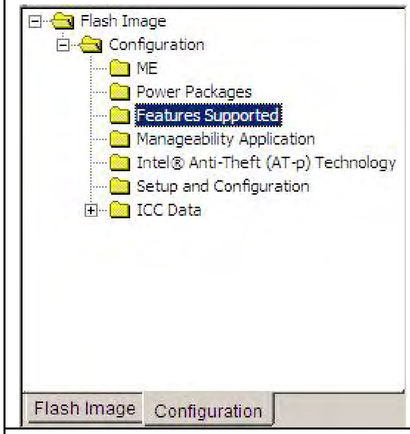
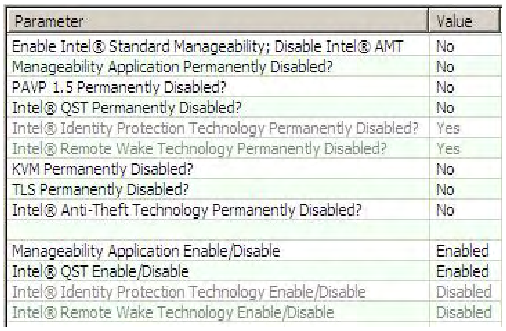
The Configuration tab located at the bottom of the FITc window allows the user to set specific parameters.

Configure all parameters as per section 5.2.11. Then follow below instructions to configure Intel ® RPAT consumer platform. Parameters with changes are only mentioned in this session.

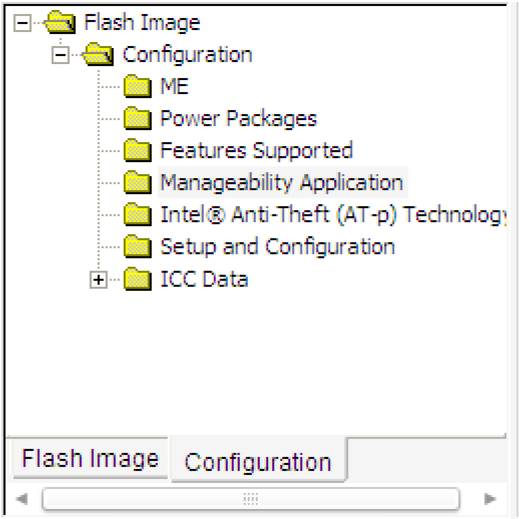
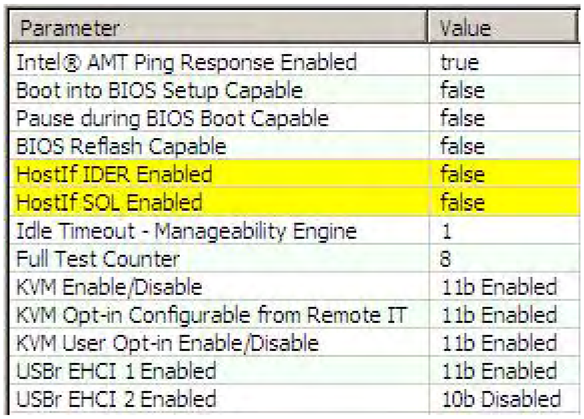
1. On the navigation tree to the left, select the **Configuration** tab. Select **Power Packages** as shown below. Only S0 required to be supported in RPAT consumer SKU's for both Desktop and Mobile.

<table>
<tr><th>Location
 </th><th>Parameter</th><th>Default</th><th>Comments</th></tr>
<tr><td>Desktop Power Packages
<table><tr><th>Parameter</th><th>Value</th></tr><tr><td>Power Pkg 1 Supported (Desktop: ON in S0)</td><td>true</td></tr><tr><td>Power Pkg 2 Supported (Desktop: ON in S0, ME Wake in S3, S4-5)</td><td>true</td></tr><tr><td>Default Power Package</td><td>1</td></tr></table></td><td>Power Pkg 2 Supported (Desktop: On in S0, ME Wake in S3, S4-5)</td><td>False</td><td>This parameter configures ME for operation in S0 and ME Wake in S3, S4 and S5.</td></tr>
<tr><td>Mobile Power Packages
<table><tr><th>Parameter</th><th>Value</th></tr><tr><td>Power Pkg 1 Supported (Mobile: ON in S0)</td><td>true</td></tr><tr><td>Power Pkg 2 Supported (Mobile: ON in S0, ME Wake in S3, S4-5 (AC only))</td><td>true</td></tr><tr><td>Default Power Package</td><td>1</td></tr></table></td><td>Power Pkg 2 Supported (Mobile: On in S0, ME Wake in S3, S4-5)</td><td>False</td><td>This parameter configures ME for operation in S0 and ME Wake in S3, S4 and S5.</td></tr>
</table>

2. On the navigation tree to the left, select the **Configuration** tab. Select **Features Supported** as shown below, <u>the configurations below are basically already set according to each SKU.</u>

Location	Parameter	Default	Comments
 Flash Image Configuration ME Power Packages Features Supported Manageability Application Intel® Anti-Theft (AT-p) Technology Setup and Configuration ICC Data Flash Image Configuration			These options control the availability / visibility of firmware features. In instances where a specific feature is configurable in the MEBx disabling it through the 'Features Supported' section will hide / disable that specific feature in the MEBx.
 Parameter — Value Enable Intel® Standard Manageability; Disable Intel® AMT — No Manageability Application Permanently Disabled? — No PAVP 1.5 Permanently Disabled? — No Intel® QST Permanently Disabled? — No Intel® Identity Protection Technology Permanently Disabled? — Yes Intel® Remote Wake Technology Permanently Disabled? — Yes KVM Permanently Disabled? — No TLS Permanently Disabled? — No Intel® Anti-Theft Technology Permanently Disabled? — No Manageability Application Enable/Disable — Enabled Intel® QST Enable/Disable — Enabled Intel® Identity Protection Technology Enable/Disable — Disabled Intel® Remote Wake Technology Enable/Disable — Disabled	Intel® Identity Protection Technology Permanently Disabled?	No	Note: Default parameter for this field is "yes". Change to "No" only if this technology is supported. For CRB keep default.
	Intel® Identity Protection Technology Enable / Disable	Enabled	
	Intel® Remote Wake Technology Enable / Disable	Disabled	

3. On the navigation tree to the left, select the **Configuration** tab. Select **Manageability Application** as shown below.

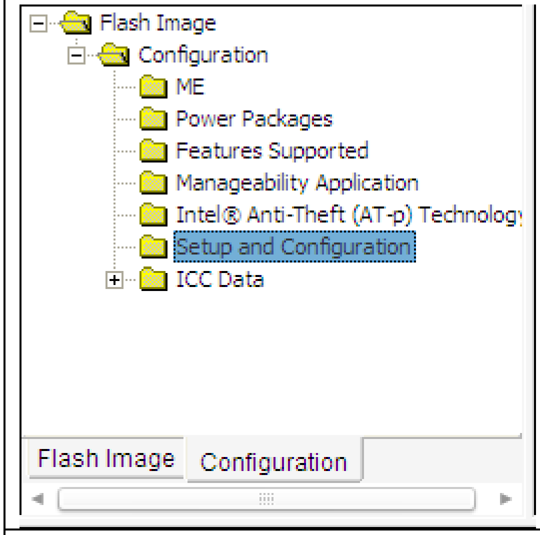
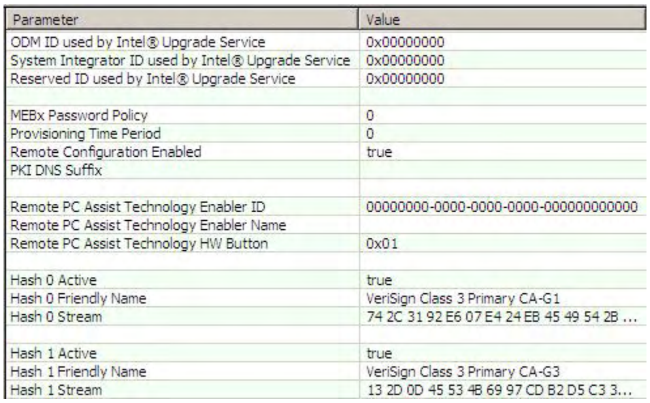
Location	Parameter	Default	Comments
			
	Boot into BIOS Setup Capable	true	
	Pause during BIOS Boot Capable	true	
	HostIf IDER Enabled	true	
	HostIf SOL Enabled	true	

Flash Image
- Configuration
  - ME
  - Power Packages
  - Features Supported
  - Manageability Application
  - Intel® Anti-Theft (AT-p) Technolog
  - Setup and Configuration
  - ICC Data

Flash Image | Configuration

Parameter	Value
Intel® AMT Ping Response Enabled	true
Boot into BIOS Setup Capable	false
Pause during BIOS Boot Capable	false
BIOS Reflash Capable	false
HostIf IDER Enabled	false
HostIf SOL Enabled	false
Idle Timeout - Manageability Engine	1
Full Test Counter	8
KVM Enable/Disable	11b Enabled
KVM Opt-in Configurable from Remote IT	11b Enabled
KVM User Opt-in Enable/Disable	11b Enabled
USBr EHCI 1 Enabled	11b Enabled
USBr EHCI 2 Enabled	10b Disabled

4. On the navigation tree to the left, select the **Configuration** tab. Select **Setup and Configuration** as shown below.

Location	Parameter	Default	Comments
			
	ODM ID used by Intel® Upgrade Service	0x00000000	
	System Integrator ID used by Intel® Upgrade Service	0x00000000	
	Remote PC Assist Technology Enabler Id	Valid OEM Specific ID to be provided	This value must be programmed with your OEM specific Id.
	Remote PC Assist Technology Enabler Name	Valid RPAT enabler name to be provided	This value must be programmed with your OEM specific Enabler name.
	Remote PC Assist Technology HW Button	0x01	This parameter specifies if the system incorporates a hardware button to be used for triggering a RPAT session. If HW button is enabled on the system this parameter should be set to 0x02

Parameter	Value
ODM ID used by Intel® Upgrade Service	0x00000000
System Integrator ID used by Intel® Upgrade Service	0x00000000
Reserved ID used by Intel® Upgrade Service	0x00000000
MEBx Password Policy	0
Provisioning Time Period	0
Remote Configuration Enabled	true
PKI DNS Suffix	
Remote PC Assist Technology Enabler ID	00000000-0000-0000-0000-000000000000
Remote PC Assist Technology Enabler Name	
Remote PC Assist Technology HW Button	0x01
Hash 0 Active	true
Hash 0 Friendly Name	VeriSign Class 3 Primary CA-G1
Hash 0 Stream	74 2C 31 92 E6 07 E4 24 EB 45 49 54 2B ...
Hash 1 Active	true
Hash 1 Friendly Name	VeriSign Class 3 Primary CA-G3
Hash 1 Stream	13 2D 0D 45 53 4B 69 97 CD B2 D5 C3 3...

5.1.5 Intel® RPAT Consumer bring up contiued.

Follow instructions in sections 4.2.12 – 4.5.2 (including) as described above.

5.2 Intel® RPAT Business Firmware Bringup Process

Follow sections 5.1 – 5.2.2 first. Then follow instructions below to configure Intel® RPAT Business firmware.

5.2.1 Intel® RPAT Business Bring Up

Please Follow sections 4.1 – 4.2.1 as describe above (Assemble the SPI Flash Binary Image, Set Up the Build Environment).

5.2.2 Selecting Intel® RPAT Business Platform SKU

This new feature allows testing how firmware behaves with SKU'd HW using Super-SKU Ibex Peak.

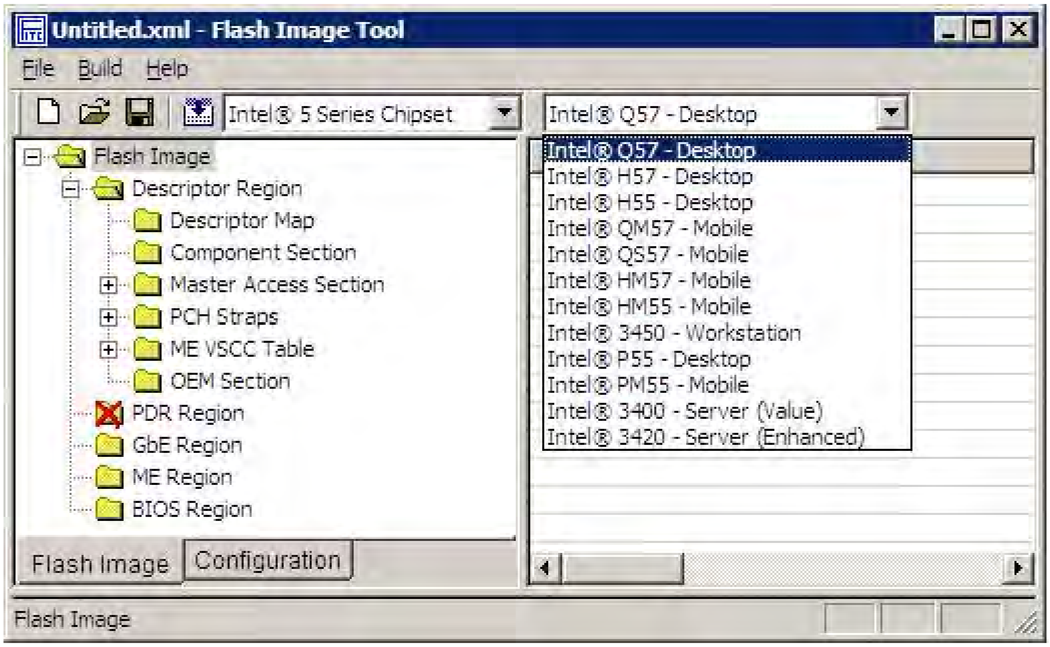
– Certain features only work with particular SKUs of firmware.
(For example Intel® AMT only works with corporate SKUs)

– When a SKU is selected in FITc the Super SKU Ibex Peak will then behave as if it were the selected SKU silicon from Intel ME perspective.

Intel® RPAT Business Platform supports several SKUs, please select the appropriate platform type for your specific chipset (to be configured in the table below):

- For Desktop– **Q57.**
- For Mobile - **QM57, QS57**

The SKU Manager Selection option has no effect on Production Silicon



Note: The Features Supported and other Configuration tabs in FITc will show the appropriate changes to the firmware features under '**Configuration / Features Supported**' according to the SKU selected.

5.2.3 Intel® RPAT Business bring-up continued

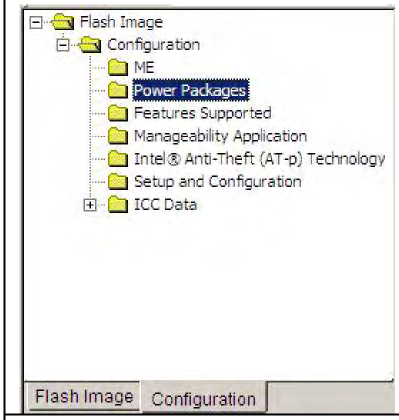
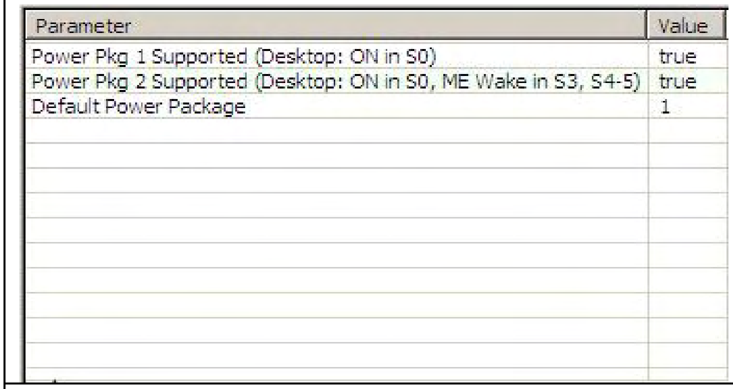
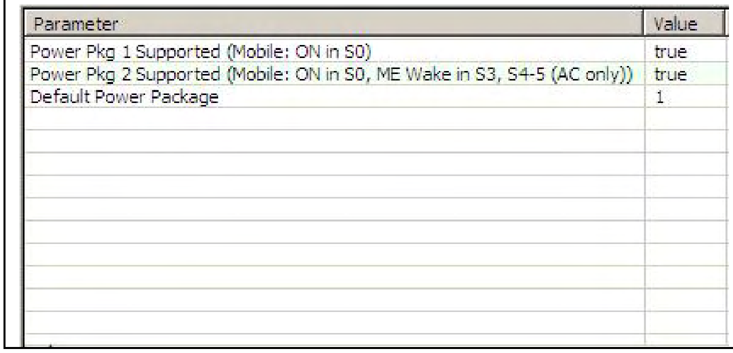
Follow instructions in sections 5.2.3 – 5.2.10 (including) as describe above.

5.2.4 Intel® RPAT Business Configuration Parameters

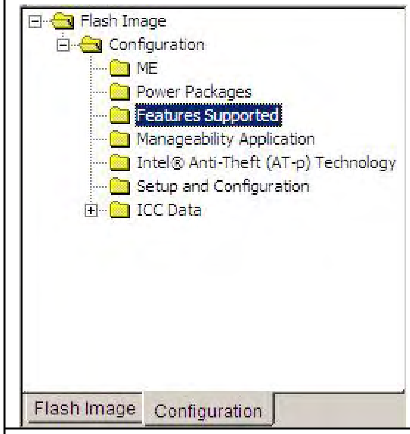
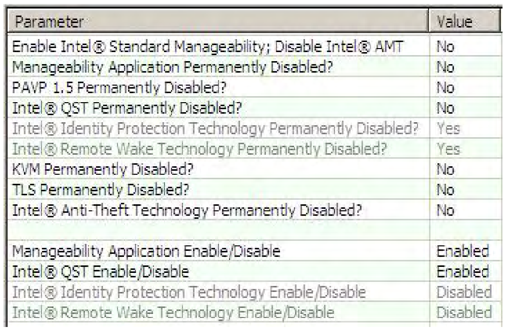
The Configuration tab located at the bottom of the FITc window allows the user to set specific parameters.

Configure all parameters as per section 5.2.11. Then follow below instructions to configure Intel ® RPAT Business platform. Parameters with changes are only mentioned in this session.

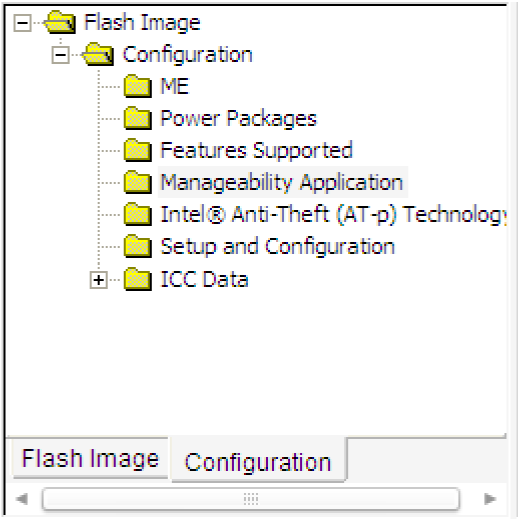
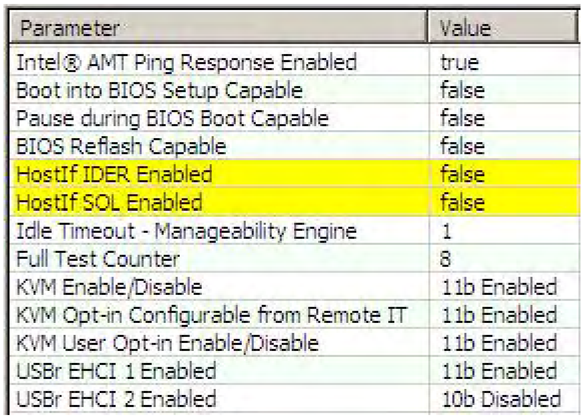
5. On the navigation tree to the left, select the **Configuration** tab. Select **Power Packages** as shown below, please make sure the below configuration (configures ME for operation in S0 and ME Wake in S3, S4 and S5).

<table>
<tr><th>Location
 </th><th>Parameter</th><th>Default</th><th>Comments</th></tr>
<tr><td>Desktop Power Packages
<table><tr><th>Parameter</th><th>Value</th></tr><tr><td>Power Pkg 1 Supported (Desktop: ON in S0)</td><td>true</td></tr><tr><td>Power Pkg 2 Supported (Desktop: ON in S0, ME Wake in S3, S4-5)</td><td>true</td></tr><tr><td>Default Power Package</td><td>1</td></tr></table></td><td>Default Power Package</td><td>1</td><td>This parameter determines the default Power Package used by firmware image. Set power package to 2 for RPAT proactive enrollment</td></tr>
<tr><td>Mobile Power Packages
<table><tr><th>Parameter</th><th>Value</th></tr><tr><td>Power Pkg 1 Supported (Mobile: ON in S0)</td><td>true</td></tr><tr><td>Power Pkg 2 Supported (Mobile: ON in S0, ME Wake in S3, S4-5 (AC only))</td><td>true</td></tr><tr><td>Default Power Package</td><td>1</td></tr></table></td><td>Default Power Package</td><td>1</td><td>This parameter determines the default Power Package used by firmware image. Set power package to 2 for RPAT proactive enrollment</td></tr>
</table>

6. On the navigation tree to the left, select the **Configuration** tab. Select **Features Supported** as shown below, <u>the configurations below are basically already set according to each SKU.</u>

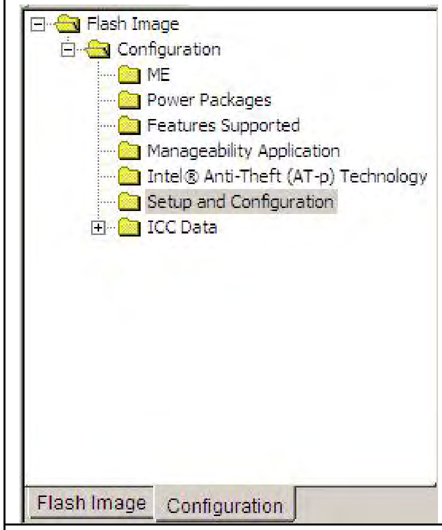
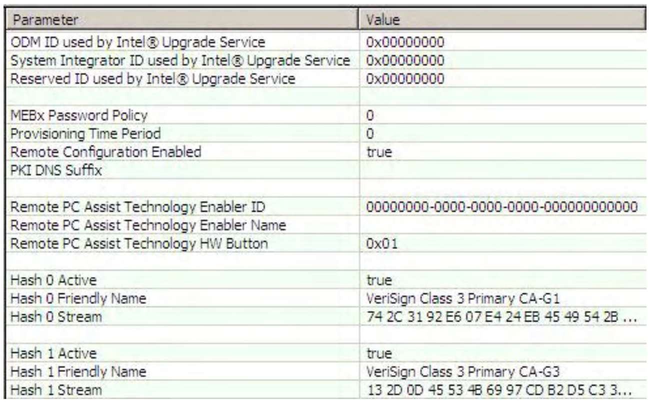
Location	Parameter	Default	Comments
 Flash Image Configuration ME Power Packages Features Supported Manageability Application Intel® Anti-Theft (AT-p) Technology Setup and Configuration ICC Data Flash Image Configuration			These options control the availability / visibility of firmware features. In instances where a specific feature is configurable in the MEBx disabling it through the 'Features Supported' section will hide / disable that specific feature in the MEBx.
Parameter – Value Enable Intel® Standard Manageability; Disable Intel® AMT – No Manageability Application Permanently Disabled? – No PAVP 1.5 Permanently Disabled? – No Intel® QST Permanently Disabled? – No Intel® Identity Protection Technology Permanently Disabled? – Yes Intel® Remote Wake Technology Permanently Disabled? – Yes KVM Permanently Disabled? – No TLS Permanently Disabled? – No Intel® Anti-Theft Technology Permanently Disabled? – No Manageability Application Enable/Disable – Enabled Intel® QST Enable/Disable – Enabled Intel® Identity Protection Technology Enable/Disable – Disabled Intel® Remote Wake Technology Enable/Disable – Disabled	Intel® Identity Protection Technology Permanently Disabled?	No	Note:- Default value for this parameter is "Yes". Set to "No" if supporting Intel® Identify Protection Technology. For CRB keep default.
	Intel® Identity Protection Technology Enable / Disable	Enabled	

7. On the navigation tree to the left, select the **Configuration** tab. Select **Intel® AMT** as shown below.

Location	Parameter	Default	Comments
			
	Boot into BIOS Setup Capable	true	
	Pause during BIOS Boot Capable	true	
	HostIf IDER Enabled	true	
	HostIf SOL Enabled	true	

Parameter	Value
Intel® AMT Ping Response Enabled	true
Boot into BIOS Setup Capable	false
Pause during BIOS Boot Capable	false
BIOS Reflash Capable	false
HostIf IDER Enabled	false
HostIf SOL Enabled	false
Idle Timeout - Manageability Engine	1
Full Test Counter	8
KVM Enable/Disable	11b Enabled
KVM Opt-in Configurable from Remote IT	11b Enabled
KVM User Opt-in Enable/Disable	11b Enabled
USBr EHCI 1 Enabled	11b Enabled
USBr EHCI 2 Enabled	10b Disabled

8. On the navigation tree to the left, select the **Configuration** tab. Select **Setup and Configuration** as shown below.

<table>
<tr><th>Location</th><th rowspan="2">Parameter</th><th rowspan="2">Default</th><th rowspan="2">Comments</th></tr>
<tr><td>
Flash Image
Configuration
ME
Power Packages
Features Supported
Manageability Application
Intel® Anti-Theft (AT-p) Technology
Setup and Configuration
ICC Data
Flash Image Configuration</td></tr>
<tr><td rowspan="5">
<table>
<tr><th>Parameter</th><th>Value</th></tr>
<tr><td>ODM ID used by Intel® Upgrade Service</td><td>0x00000000</td></tr>
<tr><td>System Integrator ID used by Intel® Upgrade Service</td><td>0x00000000</td></tr>
<tr><td>Reserved ID used by Intel® Upgrade Service</td><td>0x00000000</td></tr>
<tr><td></td><td></td></tr>
<tr><td>MEBx Password Policy</td><td>0</td></tr>
<tr><td>Provisioning Time Period</td><td>0</td></tr>
<tr><td>Remote Configuration Enabled</td><td>true</td></tr>
<tr><td>PKI DNS Suffix</td><td></td></tr>
<tr><td></td><td></td></tr>
<tr><td>Remote PC Assist Technology Enabler ID</td><td>00000000-0000-0000-0000-000000000000</td></tr>
<tr><td>Remote PC Assist Technology Enabler Name</td><td></td></tr>
<tr><td>Remote PC Assist Technology HW Button</td><td>0x01</td></tr>
<tr><td></td><td></td></tr>
<tr><td>Hash 0 Active</td><td>true</td></tr>
<tr><td>Hash 0 Friendly Name</td><td>VeriSign Class 3 Primary CA-G1</td></tr>
<tr><td>Hash 0 Stream</td><td>74 2C 31 92 E6 07 E4 24 EB 45 49 54 2B ...</td></tr>
<tr><td></td><td></td></tr>
<tr><td>Hash 1 Active</td><td>true</td></tr>
<tr><td>Hash 1 Friendly Name</td><td>VeriSign Class 3 Primary CA-G3</td></tr>
<tr><td>Hash 1 Stream</td><td>13 2D 0D 45 53 4B 69 97 CD B2 D5 C3 3...</td></tr>
</table>
</td><td>ODM ID used by Intel® Upgrade Service</td><td>0x00000000</td><td></td></tr>
<tr><td>System Integrator ID used by Intel® Upgrade Service</td><td>0x00000000</td><td></td></tr>
<tr><td>Remote PC Assist Technology Enabler Id</td><td>Valid OEM Specific ID to be provided</td><td>This value must be programmed with your OEM specific Id</td></tr>
<tr><td>Remote PC Assist Technology Enabler Name</td><td>Valid RPAT enabler name to be provided</td><td>This value must be programmed with your OEM specific Enabler name.</td></tr>
<tr><td>Remote PC Assist Technology HW Button</td><td>0x01</td><td>This parameter specifies if the system incorporates a hardware button to be used for triggering a RPAT session. If HW button is enabled on the system this parameter should be set to 0x02</td></tr>
</table>

5.2.5 Intel® RPAT Bussines bring up continued

Follow instructions in sections 4.2.12 – 4.5.2 (including) as described above.

§

6 Consumer SKU Intel® Identity Protection

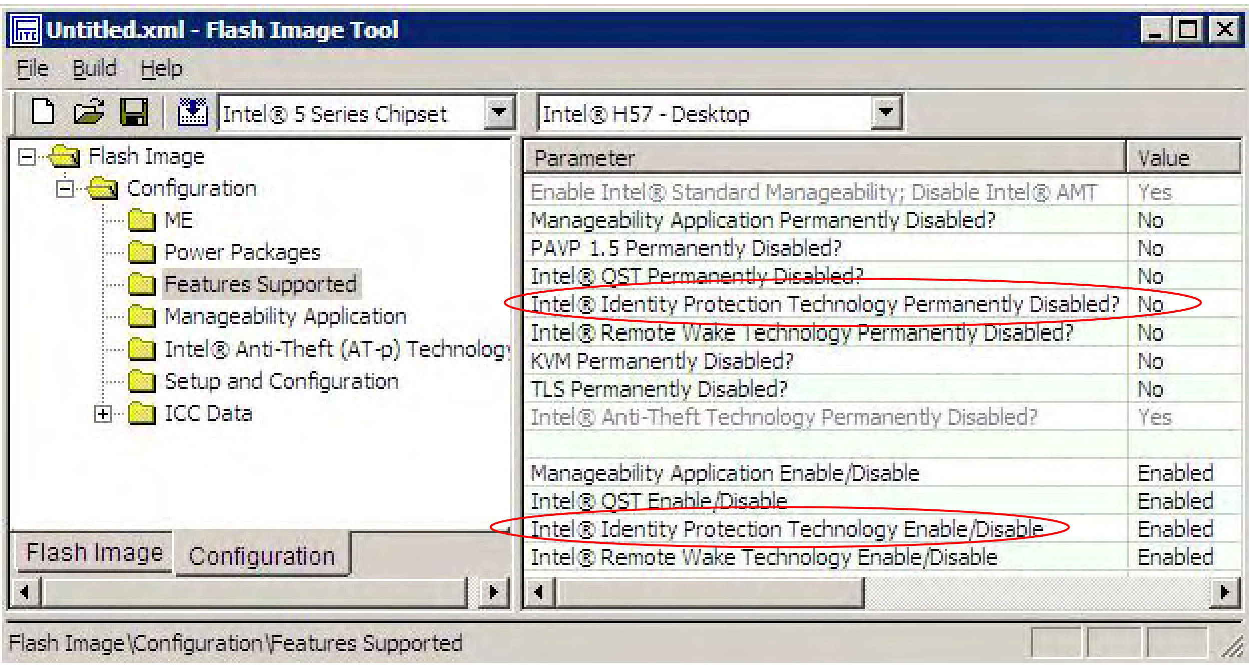
6.1 Intel® Identity Protection Configuration:

This section allows the user to specify which features will be supported in the system.

The settings below cover H57, H55 and HM57 SKU platforms.

1. To enable Intel® Identity Protection:
   a. Set the Intel® Identity Protection Technology Enable / Disable option to ‘**Enabled’** as shown below.
   b. Also ensure that the Intel® Identity Protection Technology Permanently Disabled option is set to ‘**No**’
   c. If enabled, this feature can be disabled in MEBx.

Table 6-1. Enabling Intel® Identity Protection



Intel® 5 Series Chipset

Intel® H57 - Desktop

Parameter	Value
Enable Intel® Standard Manageability; Disable Intel® AMT	Yes
Manageability Application Permanently Disabled?	No
PAVP 1.5 Permanently Disabled?	No
Intel® QST Permanently Disabled?	No
Intel® Identity Protection Technology Permanently Disabled?	No
Intel® Remote Wake Technology Permanently Disabled?	No
KVM Permanently Disabled?	No
TLS Permanently Disabled?	No
Intel® Anti-Theft Technology Permanently Disabled?	Yes
Manageability Application Enable/Disable	Enabled
Intel® QST Enable/Disable	Enabled
Intel® Identity Protection Technology Enable/Disable	Enabled
Intel® Remote Wake Technology Enable/Disable	Enabled

Flash Image\Configuration\Features Supported

6.2 Intel® Identity Protection Technology Verification Test

This section describes the tools and procedures needed to test that Intel® Identity protection technology is responsive. More comprehensive functional tests can be found in the Compliance Kit. Note that any tools referenced in this section can be found in either the Consumer EIB Firmware kit or in the Intel® IPT Software Kit. Also note that the tools and documents provided in the latest kit release should supersede any version available from any other source.

6.2.1 MEInfo Tool

The MEInfo Tool reads and displays information from the ME and displays it on the screen. This tool will be used to test that Intel IPT is present and working.

Test	Description	Input	Output
IPT_1	1. Enable Intel® IPT in the MEBx on the SUT. 2. Boot the system to S0/M0 (using the OS required for SUT) 3. Run MEINFO. Look for the Intel® Identity Protection Technology Enablement field. Verify pass/fail criteria.	MEInfoWin.EXE	Intel IPT: Status Version

6.2.2 MEInfo DOS Tool

Location: Consumer EIB Firmware Kit, Intel® VIP

Path: .\firmware\Tools\System Tools\MEInfo\DOS

OS Support: MS-DOS 6.22, Windows 98 DOS, Free DOS, DRMK DOS

Documentation: For more details on this tool, please refer to the *System Tools User Guide.pdf*, located in the Consumer EIB Firmware Kit.

Pre-requisites: Create a DOS installation with MEInfo files from the Consumer EIB firmware kit.

Example 1: Execute MEInfo without any optional parameters:

a. Boot to DOS shell
b. Navigate to the directory containing MEInfo.exe
c. Execute MEInfo.exe from the command prompt
d. MEInfo will output many lines of data. In order to verify that Intel IPT is installed and responsive, look for the following data in the output:

Intel IPT Version	A string of the format WW.XX.YY.ZZ
Intel IPT Status	A string containing one of these values: Running – IPT enabled and working Not Configured – IPT enabled, but not provisioned Stopped – IPT disabled Error

e. On error, an error message is printed and a non-zero error level is returned.

6.2.3 MEInfo Windows Tool

Location: Consumer EIB Firmware Kit, Intel® VIP

Path: .\firmware\Tools\System Tools\MEInfo\Windows

OS Support: Microsoft* Windows* XP, Vista, RE

Documentation: For more details on this tool, please refer to the *System Tools User Guide.pdf*, located in the Consumer EIB Firmware Kit.

Pre-requisites: Create a Windows installation with LMS and MEI drivers. These are available in the Consumer EIB Firmware Kit:

.\Software Install\Setup.exe

6.2.3.1 Example 1: Execute MEInfoWin without any parameters

a. Boot to Microsoft Windows
b. Ensure that LMS and ME Drivers are installed
c. Navigate to the folder containing MEInfoWin.exe
d. Execute MEInfo.exe by double clicking its icon
e. The following are examples of executing MEInfo.
f. MEInfo will output many lines of data. In order to verify that Intel IPT is installed and responsive, look for the following data in the output:

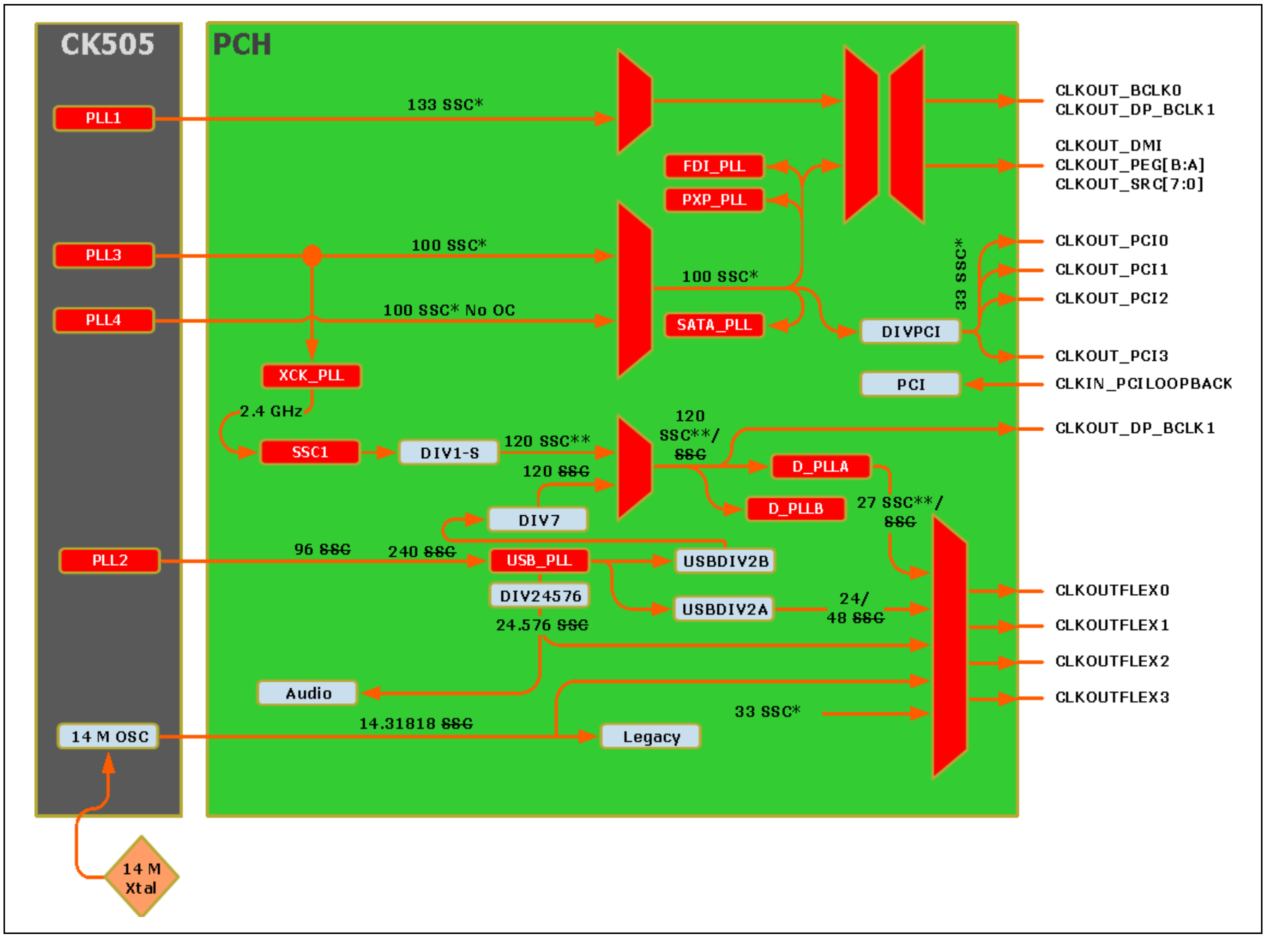
Intel IPT Version	A string of the format WW.XX.YY.ZZ
Intel IPT Status	A string containing one of these values: Enabled – IPT enabled and working Not Configured – IPT enabled, but not provisioned Disabled – IPT disabled Error

§

Appendix A – Ibex Peak Clock Configuration

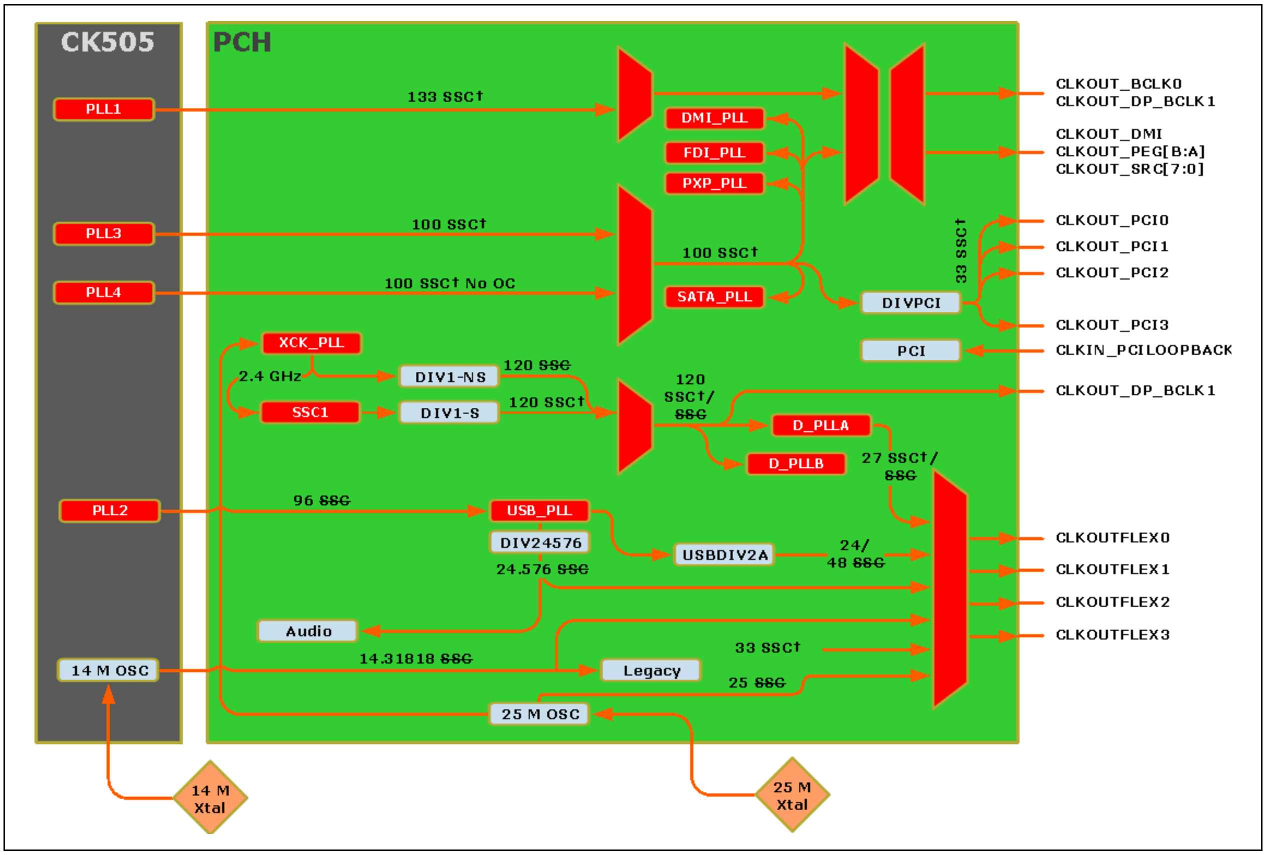
This chapter covers only the basic information needed for clock control parameter programming. For a more detailed treatment of PCH clocks, see *Ibex Peak Platform Clocks and Intel® Management Engine — Platform Compliancy Guide*.

Figure 6-1. Ibex Peak Buffer Through Mode Architecture



Note: Only 14.31818 MHz and 48 MHz outputs from CLKOUTFLEX[3:0] are guaranteed. All other output frequencies are available in PCH hardware, but not extensively tested or recommended for use.

Figure 6-2. Ibex Peak Display Clock Integration Architecture



A.1 Functional Blocks

There is 1 spread modulators in the Ibexpeak, labeled as follows:

Table 6-2. SSC Blocks

Modulator	Description
SSC1	Generates single phase 2.4-GHz output with spread for 120-MHz clock with spread generation by DIV1-S. Uses 2.4-GHz output of XCK PLL. Supplies CLKOUT_DP.

There are various clock dividers in the Ibex Peak, labeled as follows:

Table 6-3. Clock Dividers

Modulator	Description
DIV1-S	Generates 120-MHz clock with spread. Uses output of SSC1. Can be no spread if SSC1 is disabled. Supplies CLKOUT_DP.
DIV7	Generates 120-MHz clock with no spread. Uses output of USBDIV2B. Supplies

Modulator	Description
	CLKOUT_DP.
USBDIV1	Generates 96-MHz clock with no spread. Uses output of DIV5A. Supplies USB PLL.
USBDIV2A	Generates 24- or 48-MHz clock with no spread. Uses 96-MHz output of DIV5B or USBDIV1 (not shown). Supplies CLKOUTFLEX3.
USBDIV2B	Generates 240-MHz clock with no spread. Uses USB PLL's 1.92 GHz clock output. Supplies DIV7.
DIVPCI	Generates 33-MHz clock with spread. Uses output of either DIV2-S, DIV2-NS, or DIV4. Can be no spread if DIV2-NS is used or SSC4 is disabled. Supplies CLKOUT_PCI[4:0] and CLKOUTFLEX[3:0].

A.2 Intel® ME Firmware Clock Control Parameters

The following parameters can be specified for Intel ME Firmware programming. For more details on how to configure an SPI flash image with these clock control parameters see the Bring-Up Process chapter in the *Firmware Bring-Up Guide* included in the Intel ME Firmware kit.

Note: Clock control parameter specifications may be different between Buffer Through Mode, Display Clock Integration, and Full Clock Integration Mode. The specification for each mode is listed separately. For those parameters that are mode-agnostic, only a single specification is given.

A.2.1 FCSS – Flex Clock Source Select

BTM/DCI Default: 0000 0304h
ME FW Default: No changes from BTM/DCI defaults
Flash Image Tool and Config Wizard Default: 0000 0344h
Recommended Defaults:

- **Desktop CRB:** 0000 4444h
- **Mobile CRB DCI with Ext/Intg/Mixed Graphics:** 0000 4422h
- **Mobile CRB External Graphics Only or BTM with Ext/Intg Graphics:** 0000 4322h

Description: This parameter controls muxing to select sources for Flex Clock outputs

Flash Image Tool Configuration: Flash Image | Configuration | ICC Data | OEM Request Record [6:0] | Static Registers Section

Table 6-4. Flex Clock Source Select Parameters

Bits	Default	Description
31:15	0h	**Reserved (RSVD)**
14:12	000b	**FLEXCLK3 Source Select (F3SS):** Selects the source of clock to be driven out on CLKOUTFLEX3. **000b** = 48 MHz **001b** = Reserved **010b** = 33.3 MHz **011b** = 14.31818 MHz **100b** = Disabled (DC logic '0') **101b** = Disabled (DC logic '0') **110b** = Disabled (DC logic '0') **111b** = Reserved ***Note:*** These clock select settings only take effect when this muxed FLEXCLK/GPIO pin is configured for FLEXCLK native usage. Refer to the *Ibex Peak EDS* for configuration of GPIO vs. native usage.
11:11	0h	**Reserved (RSVD)**
10:8	011b	**FLEXCLK2 Source Select (F3SS):** Selects the source of clock to be driven out on CLKOUTFLEX2. **DCI / BTM** **000b** = Reserved **001b** = Reserved **010b** = 33.3 MHz **011b** = 14.31818 MHz **100b** = Disabled (DC logic '0') **101b** = Disabled (DC logic '0') **110b** = Disabled (DC logic '0') **111b** = Reserved ***Note:*** These clock select settings only take effect when this muxed FLEXCLK/GPIO pin is configured for FLEXCLK native usage. Refer to the Ibex Peak EDS for configuration of GPIO vs. native usage.
7:7	0h	**Reserved (RSVD)**
6:4	000b	**FLEXCLK1 Source Select (F1SS):** Selects the source of clock to be driven out on CLKOUTFLEX1. **000b** = Reserved **001b** = Reserved **010b** = 33.3 MHz **011b** = 14.31818 MHz **100b** = Disabled (DC logic '0') **101b** = Disabled (DC logic '0')

Bits	Default	Description
		110b = Disabled (DC logic ‘0’) **111b** = Reserved ***Note:*** These clock select settings only take effect when this muxed FLEXCLK/GPIO pin is configured for FLEXCLK native usage. Refer to the *Ibex Peak EDS* for configuration of GPIO vs. native usage.
3:3	0h	**Reserved (RSVD)**
2:0	100b	**FLEXCLK0 Source Select (F0SS):** Selects the source of clock to be driven out on CLKOUTFLEX0. **000b** = Reserved **001b** = Reserved **010b** = 33.3 MHz **011b** = 14.31818 MHz **100b** = Disabled (DC logic ‘0’) **101b** = Disabled (DC logic ‘0’) **110b** = Disabled (DC logic ‘0’) **111b** = Reserved ***Note:*** These clock select settings only take effect when this muxed FLEXCLK/GPIO pin is configured for FLEXCLK native usage. Refer to the *Ibex Peak EDS* for configuration of GPIO vs. native usage.

A.2.2 PLLEN* – PLL Enable

BTM/DCI Default: 00000404h (before PCH_PWROK), 8000040Ch (after PCH_PWROK)
ME FW/Flash Image Tool and Config Wizard Default: No changes from BTM/DCI defaults
Recommended Defaults:

- **DCI with Ext/Intg/Mixed Graphics:** 8000 040Ch
- **External Graphics Only:** 8000 041Bh
- **BTM with Ext/Intg Graphics:** 8000 041Ch

Description: This parameter controls PLL enables.
Flash Image Tool Configuration: Flash Image | Configuration | ICC Data | OEM Request Record [6:0] | Static Registers Section

Table 6-5. PLL Enable Parameters

Bits	Default	Description
31	1b	**Chipset Configuration (PCHCFG):** Must be set to **1b.**
30:11	0h	**Reserved (RSVD)**
10	1b	**Chipset Configuration (PCHCFG):** Must be set to **1b.**
9	1b	**DPLLA/DPLLB/SSC1 Ownership (DPLLSSC1OWN):** Controls the owner of DPLLA, DPLLB, and SSC1. **0b** = Display Driver register set controls DPLLA, DPLLB, and SSC1 **1b** = ME FW controls DPLLA, DPLLB, and SSC1. Note that ME FW only provides a subset of controls, to enable/disable the DPLLs and configure it for 27MHz spread or non-spread
8	0b	**DP120/BCLK1 Output Buffer Ownership (DPBCLK1OBOWN):** Controls the owner of CLKOUT_DP_BCLK1 output buffer. **0b** = Display Driver register controls CLKOUT_DP_BCLK1 output buffer. In this case, this output pin usage is to provide reference clock to the DPLL associated with the CPU embedded display.

Bits	Default	Description
		1b = ME FW controls CLKOUT_DP_BCLK1 output buffer. In this case, this output usage is to provide BCLK reference clock to the CPU. The default is display owned. ***Note:*** Specifically this field determines whether the display side control logic owns the gating/un-gating of the output clock source to the CLKOUT_DP_BCLK1 output pin, or whether the clock module side owns this gating / un-gating. This field does not have any effect at the output buffer tri-state/driven control.
7:5	0h	**Reserved (RSVD)**
4	0b	**Crystal Oscillator Disable (OSCDIS):** Disables the crystal oscillator when it is not used as a reference clock source to the XCK PLL. **0b** = Enable oscillator **1b** = Disable oscillator to save power ***Note:*** The crystal oscillator should be disabled when integrated graphics (or any other consumer of 120 MHz clock internal and external to Ibex Peak) is not utilized. The output frequency for PCH pin CLKOUT_DP_BCLK1 is controlled by parameter field "DP120/BCLK1 Clock Source Select" at CSS[9:8].
3	Strap (FITC/FICW assumes this value to be 1b)	**XCK VRM Bypass (XCKVRMBYP):** This read-only field reports the state of the VRM bypass hardstrap pin GPIO[27]/MGPIO[6]. Software reads this field to determine whether the VRM powers the XCKPLL circuitries. ME FW writes to "XCK VRM Disable" parameter field at 1230Ch[1] to disable power consuming circuitries in the VRM when it is not used. **0b** = Board powers XCK PLL circuitry **1b** = Integrated VRM powers XCK PLL circuitry ***Note:*** The true value of the hard strap, which resides in the suspend power well, is not reflected in this core well register field until Ibex Peak has received its PCH_PWROK indication. Software read of this register field prior to PCH_PWROK assertion will return zero because of power well crossing isolation.
2	1b	**XCK Voltage Divider Enable (XCKVDIVEN):** Enables the shared voltage divider associated with biasing current generation for the crystal oscillator and the PI blocks. The voltage divider should be disabled to save power when the crystal oscillator and none of the PI blocks are used. **0b** = Disable the voltage divider to save power **1b** = Enable the voltage divider ***Note:*** The XCK voltage divider should be disabled when integrated graphics (or any other consumer of 120 MHz clock internal and external to Ibex Peak) is not utilized. The output frequency for PCH pin CLKOUT_DP_BCLK1 is controlled by parameter field "DP120/BCLK1 Clock Source Select" at CSS[9:8].
1	0b	**XCK VRM Disable (XCKVRMDIS):** Disables the integrated VRM when it is not used to power XCK PLL circuitry. **0b** = Enable VRM **1b** = Disable VRM to save power ***Note:*** The XCK VRM should be disabled when integrated graphics (or any other consumer of 120 MHz clock internal and external to Ibex Peak) is not utilized. The output frequency for PCH pin CLKOUT_DP_BCLK1 is controlled by parameter field "DP120/BCLK1 Clock Source Select" at CSS[9:8].
0	0b	**XCK_PLL Disable (XCKDIS):** Disables the XCK PLL. **0b** = Enable XCK PLL **1b** = Disable XCK PLL ***Note:*** The XCK PLL should be disabled when integrated graphics (or any other consumer of 120 MHz clock internal and external to Ibex Peak) is not utilized. The output frequency for PCH pin CLKOUT_DP_BCLK1 is controlled by parameter field "DP120/BCLK1 Clock Source Select" at CSS[9:8].

A.2.3 OCKEN – Output Clock Enable

BTM/DCI Default: 1FFF 0F8Fh
ME FW/Flash Image Tool and Config Wizard Default: No changes from BTM/DCI defaults
Description: This parameter controls enabling of output buffers
Flash Image Tool Configuration: Flash Image | Configuration | ICC Data | OEM Request Record [6:0] | Static Registers Section

Table 6-6. Output Clock Enable Parameters

Bits	Default	Description
31:29	0h	**Reserved (RSVD)**
28	1b	**DMI Output Clock Enable (DMIOCKEN):** Controls the enabling of DMI clock toggling. When this clock output is not used, it should be gated to low state to save power. **0b** = Output clock is gated to low state **1b** = Output buffer is enabled to toggle once its clock source has been initialized
27	1b	**PEG_B Output Clock Enable (PBOCKEN):** Controls the enabling of PEG_B clock toggling. When this clock output is not used, it should be gated to low state to save power. **0b** = Output clock is gated to low state **1b** = Output buffer is enabled to toggle once its clock source has been initialized
26	1b	**PEG_A Output Clock Enable (PAOCKEN):** Controls the enabling of PEG_A clock toggling. When this clock output is not used, it should be gated to low state to save power. **0b** = Output clock is gated to low state **1b** = Output buffer is enabled to toggle once its clock source has been initialized
25	1b	**DP120/BCLK1 Output Clock Enable (DPBCLK1OCKEN):** Controls the enabling of CLKOUT_DP_BCLK1 clock toggling. When this clock output is not used, it should be gated to low state to save power. **0b** = Output clock is gated to low state **1b** = Output buffer is enabled to toggle once its clock source has been initialized ***Note:*** In order for this parameter field to take effect, the ownership of the muxed output clock pin CLKOUT_DP_BCLK1 must be configured to be clock-module-owned, via “BCLK/DP120 Output Buffer Ownership” parameter field at PLLEN[8]. When the ownership is under display control, the display logic side (not ME FW) determines whether the output clock pin CLKOUT_DP_BCLK1 toggles or gated to low state.
24	1b	**BCLK0 Output Clock Enable (BCLK0OCKEN):** Controls the enabling of CLKOUT_BCLK0 clock toggling. When this clock output is not used, it should be gated to low state to save power. **0b** = Output clock is gated to low state **1b** = Output clock is enabled to toggle once its clock source has been initialized
23:16	FFh	**SRC 7:0 Output Clock Enable (SRC70OCKEN):** Controls the enabling of SRC clock toggling. Each bit position controls the corresponding SRC output clock, e.g. bit 0 controls SRC0. When any clock output is not used, it should be gated to low state to save power. **0b** = Corresponding output clock is gated to low state **1b** = Corresponding output clock is enabled to toggle once its clock source has been initialized (hot plug capable)
15:12	0h	**Reserved (RSVD)**
11:7	1Fh	**PCICLK 4:0 Output Clock Enable (PCI40OCKEN):** Controls the enabling of PCI clock toggling. Each bit position controls the corresponding PCI output clock, e.g. bit 7 controls CLKOUT_PCI0. When any clock output is not used, it should be gated to low state to save power. This register bit may be updated dynamically. **0b** = Corresponding output clock is gated to low state

Bits	Default	Description
		1b = Corresponding output clock is enabled to toggle once its clock source has been initialized **A-stepping Note:** This parameter has no effect and clock output is always enabled. **B-stepping Note:** Parameter behaves normally.
6:4	0h	**Reserved (RSVD)**
3:0	Fh	**A-stepping Implementation:** **FLEXCLK 3:0 Output Buffer Enable (F30OBEN):** Controls the enabling of CLKOUTFLEX[3:0] output buffers. Each bit position controls the corresponding FLEXCLK output buffer, e.g. LSB (bit 0) controls CLKOUTFLEX0. **0b** = Corresponding output clock is tri-stated (not driven) **1b** = Corresponding output clock is driven ***Note:*** Actual driven logic state is a function of clock module state (such as during initialization, normal operation, dynamic clock management if supported, and preparation for system powering down). These bits also control the weak pull down of the FLEX input pad. Each bit position controls the corresponding FLEX weak pull down, e.g. LSB (bit 0) controls FLEX0. When the FLEX output buffer is tristated, the corresponding internal weak pull down should be enabled to avoid reliability issue due to floating input pad. **B-stepping Implementation:** **FLEXCLK 3:0 Output Clock Enable (PCI40OCKEN):** Controls the enabling of FLEXCLK toggling. Each bit position controls the corresponding FLEXCLK output clock, e.g. LSB (bit 0) controls CLKOUTFLEX0. When any clock output is not used, it should be gated to low state to save power. This register bit may be updated dynamically. **0b** = Corresponding output clock is gated to low state **1b** = Corresponding output clock is enabled to toggle once its clock source has been initialized **General Note Not Stepping Dependent:** CLKOUTFLEX[3:0] is muxed with GPIOs. Clock module logic should only enable the weak pull down when the muxed pin is configured for FLEXCLK usage (not DC logic '0') and FLEXCLK is tri-stated. FLEXCLK values can be set in the "Flex Clock Source Select" parameter at FCSS[31:0].

A.2.4 OBEN – Output Buffer Enable

BTM/DCI Default: 0F1F F1FFh
ME FW/Flash Image Tool and Config Wizard Default: No changes from BTM/DCI defaults

Description: This parameter has been deprecated. All functionality previously specified for this parameter is now available in OCKEN parameter.

Flash Image Tool Configuration: Not present in Flash Image Tool

A.2.5 IBEN – Input Buffer Enable

BTM/DCI Default: 0000 0000h
ME FW/Flash Image Tool and Config Wizard Default: No changes from BTM/DCI defaults

Description: This parameter controls enabling of input buffers
Flash Image Tool Configuration: Flash Image | Configuration | ICC Data | OEM Request Record [6:0] | Static Registers Section

Table 6-7. Input Buffer Enable Parameters

Bits	Default	Description
31:2	0h	**Reserved (RSVD)**
1	0b	**CLKIN_DOT96 Input Buffer Disable (CKIN96InBufDis):** Controls the differential input buffer for CLKIN_DOT96. When CLKIN_DOT96 is not used, its input buffer should be turned off for power saving. **0b** = Input buffer is enabled **1b** = Input buffer is disabled for power saving ***A-stepping Note:*** This parameter has no effect and the CLKIN_DOT96 input is always enabled. ***B-stepping Note:*** Parameter behaves normally.
0	0b	**BCLK Input Clock Buffer Disable (BCLKInClkBufDis)**: Controls the differential input buffer for CLKIN_BCLK. **0b** = Input buffer is enabled **1b** = Input buffer is disabled for power saving. A weak pulldown ensures output nodes are not floating.

A.2.6 DIVEN* – Divider Enable

BTM/DCI Default: 0000 08C3h
ME FW/Flash Image Tool and Config Wizard Default: 0000 0303h
Recommended Defaults:

- **DCI with Ext/Intg/Mixed Graphics:** 0000 0303h
- **External Graphics Only:** 0000 0100h
- **BTM with Ext/Intg Graphics:** 0000 0003h

Description: This parameter controls enabling of divider blocks.

Flash Image Tool Configuration: Flash Image | Configuration | ICC Data | OEM Request Record [6:0] | Static Registers Section

Table 6-8. Divider Enable Parameters

Bits	Default	Description
31:12	0h	**Reserved (RSVD)**
11	HW: 1b ME FW: 1b FITC: 0b	**24.576Mhz Fractional Divisor Enable (24FDEN):** Enables fractional divisor for 24.576-Mhz clock generation (see see Figure 6-1, Page 101 Figure 6-2, page 101). When not used, the fractional divisor can be disabled for power saving. **0b =** Divider is disabled **1b =** Divider is enabled
10	0b	**Reserved (RSVD)**
9	BTM 0b DCI 1b	**XCK Reference Clock Select (XCKRS):** Selects the source of reference clock for XCK PLL. **0b** = CLKIN_DMI **1b** = 25-Mhz crystal oscillator
10:9	0b	**Reserved (RSVD)**
8	0b	**DIV7 Enable (DIV7EN):** Enables DIV7 clock divider (see see Figure 6-1, Page 101 Figure 6-2, page 101). **0b** = Divider is enabled (120 Mhz generated from USB PLL) **1b** = Divider is disabled (120Mhz generated by XCK PLL)
7:6	HW: 3h ME FW: 3h FITC: 0h	**Chipset Configuration (PCHCFG):** Set to 3h by hardware default, but recommended to be 0h.Set to 3h by hardware default, but recommended to be 0h.
5:2	0h	**Reserved (RSVD)**
1	1b	**DIV1-S Enable (DIV1SEN):** Enables DIV1-S clock divider (see see Figure 6-1, Page 101 Figure 6-2, page 101). **0b** = Divider is disabled **1b** = Divider is enabled
0	1b	**DIV1-NS Enable (DIV1NSEN):** Enables DIV1-NS clock divider (see see Figure 6-1, Page 101 Figure 6-2, page 101). **0b** = Divider is disabled **1b** = Divider is enabled ***Note:*** In BTM, 120-MHz non-spread will be enabled through USB PLL and DIV7. In PCIM, 120-MHz non-spread will be enabled through XCK PLL and DIV7.

A.2.7 PM1 – Power Management

BTM/DCI Default: 0000 0000h
ME FW Default: No changes from BTM/DCI defaults
Flash Image Tool and Config Wizard Default: 0000 0013h

Description: This parameter controls power management features of clocks
Flash Image Tool Configuration: Flash Image | Configuration | ICC Data | OEM Request Record [6:0] | Static Registers Section

Table 6-9. Power Management Parameters

Bits	Default	Description
31:4	0h	**Reserved (RSVD)**
4	HW: 0b ME FW: 0b FITC: 1b	**Dynamic SSC1 Shutdown Enable (SSC1DSEN):** Enables dynamic power management of DIV1-S (see see Figure 6-1, Page 101 Figure 6-2, page 101). Integrated graphics display may dynamically power manage SSC1 and DIV1-S when it is assigned ownership of SSC1 ("DPLLA/DPLLB/SSC1 Ownership" parameter field at PLLEN[9] is 0b) and SSC1 is globally enabled ("SSC1 Enable, Active Low" parameter field at SSCCTL[0] is 0b). This bit has no effect, (no dynamic power management of DIV1-S), when ME has ownership (PLLEN[9] is 1b). The following are logical combinations of this parameter field (MSB) and "Dynamic DIV1S Shutdown Enable" parameter field at PM1[0] (LSB). **00b =** Disable dynamic management of DIV1-S and SSC1 **01b =** Dynamic management of DIV1-S only. SSC1 stays up and maintains current state for lower clock recovery latency at the expense of power. **10b =** Reserved **11b =** Dynamic management of both DIV1-S and SSC1. Longer clock recovery latency but more power savings. **A-stepping Note:** This parameter has no effect and the divider output is always enabled. **B-stepping Note:** Parameter behaves normally.
3:2	0h	**Reserved (RSVD)**
1	HW: 0b ME FW: 0b FITC: 1b	**Dynamic DIV1-NS Shutdown Enable (DIV1NSDSEN):** Enables dynamic power management of DIV1-NS (see see Figure 6-1, Page 101 Figure 6-2, page 101). **0b =** Disable dynamic power management of DIV1-S **1b =** Enable dynamic power management of DIV1-S **A-stepping Note:** This parameter has no effect and the divider output is always enabled. **B-stepping Note:** Parameter behaves normally.
0	HW: 0b ME FW: 0b FITC: 1b	**Dynamic DIV1-S Shutdown Enable (DIV1SDSEN):** Enables dynamic power management of DIV1-S (see see Figure 6-1, Page 101 Figure 6-2, page 101). **Do not configure this parameter field on its own. See "DIV1 Shutdown Enable" parameter field at PM1[4].**

A.2.8 PM2 – Power Management

BTM/DCI Default: 0000 0000h
ME FW/Flash Image Tool and Config Wizard Default: No changes from BTM/DCI defaults

Description: This parameter controls power management features of clocks
Flash Image Tool Configuration: Flash Image | Configuration | ICC Data | OEM Request Record [6:0] | Static Registers Section

Table 6-10. Power Management Parameters

Bits	Default	Description
31:9	0h	**Reserved (RSVD)**
8:5	0000b	**CLKRUN Control Enable for PCI 33 Mhz on CLKOUTFLEX (CLKRUNCEN_FLEX):** Enables support for CLKRUN protocol for PCI 33 MHz clocks muxed out to CLKOUTFLEX[3:0]. **0b** = Corresponding CLKOUTFLEX PCI clock is free-running, unaffected by CLKRUN protocol **1b** = Corresponding CLKOUTFLEX PCI clock is shut off when CLKRUN protocol turns off PCI clocks ***Note:*** These bits must be clear (**0b**) when the corresponding CLKOUTFLEX pins are not configured for PCI 33Mhz clock. ***A-stepping Note:*** This parameter has no effect and the outputs are unaffected when CLKRUN protocol turns off PCI clocks. ***B-stepping Note:*** Parameter behaves normally.
4:0	0 0000b	**CLKRUN Control Enable (CLKRUNCEN):** Enables support for CLKRUN protocol for CLKOUT_PCI[4:0]. **0b** = Corresponding CLKOUT_PCI is free-running, unaffected by CLKRUN protocol **1b** = Corresponding CLKOUT_PCI is shut off when CLKRUN protocol turns off PCI clocks ***Note:*** This parameter does not enable CLKRUN protocol support for CLKOUTFLEX[3:0]. ***A-stepping Note:*** This parameter has no effect and the outputs are always disabled when CLKRUN protocol turns off PCI clocks. ***B-stepping Note:*** Parameter behaves normally.

A.2.9 SEBP1 – Single Ended Buffer Parameters

BTM/DCI Default: 0000 9999h
ME FW/Flash Image Tool and Config Wizard Default: No changes from BTM/DCI defaults

Description: This parameter controls double/single load series resistance and slew rate for FLEX clocks
Flash Image Tool Configuration: Flash Image | Configuration | ICC Data | OEM Request Record [6:0] | Static Registers Section

Table 6-11. Single Ended Buffer Parameters

Bits	Default	Description
31:16	0h	**Reserved (RSVD)**
15:13	100b	**FLEXCLK3 Slew Rate Control (F3SLC):** Controls slew rate for CLKOUTFLEX3. **000b** = Weakest slew rate setting (~0.6 V/ns for a TBD inch trace at double load) **001b** **010b** **011b** **100b** = Default Slew rate setting (~1.4V/ns for a TBD inch trace at double load) **101b** **110b** **111b** = Strongest slew rate setting (~2 V/ns for a TBD inch trace at double load)
12	1b	**FLEXCLK2 Single/Double Load Series Resistance (F2SDLSR):** Sets programmable series resistance for CLKOUTFLEX2. **0b** = 25 Ohms for single load usage **1b** = 17 Ohms for double load usage
11:9	100b	**FLEXCLK2 Slew Rate Control (F2SLC):** Controls slew rate for CLKOUTFLEX2. **000b** = Weakest slew rate setting (~0.6 V/ns for a TBD inch trace at double load) **001b** **010b** **011b** **100b** = Default Slew rate setting (~1.4V/ns for a TBD inch trace at double load) **101b** **110b** **111b** = Strongest slew rate setting (~2 V/ns for a TBD inch trace at double load)
8	1b	**FLEXCLK1 Single/Double Load Series Resistance (F1SDLSR):** Sets programmable series resistance for CLKOUTFLEX1. **0b** = 25 Ohms for single load usage **1b** = 17 Ohms for double load usage
7:5	100b	**FLEXCLK1 Slew Rate Control (F1SLC):** Controls slew rate for CLKOUTFLEX1. **000b** = Weakest slew rate setting (~0.6 V/ns for a TBD inch trace at double load) **001b** **010b** **011b** **100b** = Default Slew rate setting (~1.4V/ns for a TBD inch trace at double load) **101b** **110b** **111b** = Strongest slew rate setting (~2 V/ns for a TBD inch trace at double load)
4	1b	**FLEXCLK0 Single/Double Load Series Resistance (F0SDLSR):** Sets programmable series resistance for CLKOUTFLEX0.

Bits	Default	Description
		0b = 25 Ohms for single load usage **1b** = 17 Ohms for double load usage
3:1	100b	**FLEXCLK0 Slew Rate Control (F2SLC):** Controls slew rate for CLKOUTFLEX2. **000b** = Weakest slew rate setting (~0.6 V/ns for a TBD inch trace at double load) **001b** **010b** **011b** **100b** = Default Slew rate setting (~1.4V/ns for a TBD inch trace at double load) **101b** **110b** **111b** = Strongest slew rate setting (~2 V/ns for a TBD inch trace at double load)
0	1b	**FLEXCLK3 Single/Double Load Series Resistance (F3SDLSR):** Sets programmable series resistance for CLKOUTFLEX3. **0b** = 25 Ohms for single load usage **1b** = 17 Ohms for double load usage

A.2.10 SEBP2 – Single Ended Buffer Parameters

BTM/DCI Default: 0009 9999h
ME FW/Flash Image Tool and Config Wizard Default: No changes from BTM/DCI defaults

Description: This parameter controls double/single load series resistance and slew rate for PCI clocks. PCI Specifications 2.4 and 3.0 allow for an acceptable slew rate range of 1 to 4 V/ns. ME FW programmability allows for slew rate to be specified between 0.6 to 2 V/ns for two reasons:

1. Slew rates exceeding 2 V/ns can have adverse effects on platform EMI
2. Slew rates lower than 1 V/ns can be specified for EMI benefits, at the risk of violating PCI specification

Flash Image Tool Configuration: Flash Image | Configuration | ICC Data | OEM Request Record [6:0] | Static Registers Section

Table 6-12. Single Ended Buffer Parameters

Bits	Default	Description
31:16	0h	**Reserved (RSVD)**
19:17	100b	**PCI4 Slew Rate Control (PCI4SLC):** Controls slew rate for CLKOUTPCI4. **000b** = Weakest slew rate setting (~0.6 V/ns for a TBD inch trace at double load) **001b** **010b** **011b** **100b** = Default Slew rate setting (~1.4V/ns for a TBD inch trace at double load) **101b** **110b** **111b** = Strongest slew rate setting (~2 V/ns for a TBD inch trace at double load)
16	1b	**PCI3 Single/Double Load Series Resistance (PCI3SDLSR):** Sets programmable series

Bits	Default	Description
		resistance for CLKOUT_PCI3. **0b** = 25 Ohms for single load usage **1b** = 17 Ohms for double load usage
15:13	100b	**PCI3 Slew Rate Control (PCI3SLC):** Controls slew rate for CLKOUT_PCI3. **000b** = Weakest slew rate setting (~0.6 V/ns for a TBD inch trace at double load) **001b** **010b** **011b** **100b** = Default Slew rate setting (~1.4V/ns for a TBD inch trace at double load) **101b** **110b** **111b** = Strongest slew rate setting (~2 V/ns for a TBD inch trace at double load)
12	1b	**PCI2 Single/Double Load Series Resistance (PCI2SDLSR):** Sets programmable series resistance for CLKOUT_PCI2. **0b** = 25 Ohms for single load usage **1b** = 17 Ohms for double load usage
11:9	100b	**PCI2 Slew Rate Control (PCI2SLC):** Controls slew rate for CLKOUT_PCI2. **000b** = Weakest slew rate setting (~0.6 V/ns for a TBD inch trace at double load) **001b** **010b** **011b** **100b** = Default Slew rate setting (~1.4V/ns for a TBD inch trace at double load) **101b** **110b** **111b** = Strongest slew rate setting (~2 V/ns for a TBD inch trace at double load)
8	1b	**PCI1 Single/Double Load Series Resistance (PCI1SDLSR):** Sets programmable series resistance for CLKOUT_PCI1. **0b** = 25 Ohms for single load usage **1b** = 17 Ohms for double load usage
7:5	100b	**PCI1 Slew Rate Control (PCI1SLC):** Controls slew rate for CLKOUT_PCI1. **000b** = Weakest slew rate setting (~0.6 V/ns for a TBD inch trace at double load) **001b** **010b** **011b** **100b** = Default Slew rate setting (~1.4V/ns for a TBD inch trace at double load) **101b** **110b** **111b** = Strongest slew rate setting (~2 V/ns for a TBD inch trace at double load)
4	1b	**PCI0 Single/Double Load Series Resistance (PCI0SDLSR):** Sets programmable series resistance for CLKOUT_PCI0. **0b** = 25 Ohms for single load usage **1b** = 17 Ohms for double load usage
3:1	100b	**PCI0 Slew Rate Control (PCI0SLC):** Controls slew rate for CLKOUT_PCI0. **000b** = Weakest slew rate setting (~0.6 V/ns for a TBD inch trace at double load) **001b** **010b** **011b** **100b** = Default Slew rate setting (~1.4V/ns for a TBD inch trace at double load) **101b** **110b** **111b** = Strongest slew rate setting (~2 V/ns for a TBD inch trace at double load)

Bits	Default	Description
0	1b	**PCI4 Single/Double Load Series Resistance (PCI4SDLSR):** Sets programmable series resistance for CLKOUT_PCI4. **0b** = 25 Ohms for single load usage **1b** = 17 Ohms for double load usage

A.2.11 SSCCTL* – SSC Control

BTM/DCI Default: 0009 9999h
ME FW/Flash Image Tool and Config Wizard Default: No changes from BTM/DCI defaults

Description: This parameter controls double/single load series resistance and slew rate for PCI clocks. PCI Specifications 2.4 and 3.0 allow for an acceptable slew rate range of 1 to 4 V/ns. ME FW programmability allows for slew rate to be specified between 0.6 to 2 V/ns for two reasons:

3. Slew rates exceeding 2 V/ns can have adverse effects on platform EMI
4. Slew rates lower than 1 V/ns can be specified for EMI benefits, at the risk of violating PCI specification

Flash Image Tool Configuration: Flash Image | Configuration | ICC Data | OEM Request Record [6:0] | Static Registers Section

Table 6-13. Single Ended Buffer Parameters

Bits	Default	Description
31:3	0h	**Chipset Configuration (PCHCFG):** Must be set to 20 20 20h
2:1	0b	**SSC1 Spread Mode (SSC1_SprdMd):** Select the spread mode for SSC1. **00b** = Down spread **01b** = Center spread **10b** = ReservedUp spread **11b** = Reserved
0	0b	**SSC1 Enable, Active Low (SSC1_EnB):** Determines whether SSC1 (see Figure 6-1, Page 101 Figure 6-2, page 101) is enabled. **0b** = Enable SSC1 **1b** = Power off SSC1 and select bypass path to SSC1 output. SSC1 output will thus be non-spread.

A.2.12 PMSRCCLK1 – SRC Power Management

BTM/DCI Default: 7654 3210h
ME FW/Flash Image Tool and Config Wizard Default: FFFF FFFFh
Description: This parameter as signs dynamic CLKRQ# control of SRC clocks
Flash Image Tool Configuration: Flash Image | Configuration | ICC Data | OEM Request Record [6:0] | Static Registers Section

Table 6-14. SRC Power Management

Bits	Default	Description
31:28	HW: 0111b ME FW: 1111b FITC: 1111b	**CLKRQ# Select for CLKOUT_SRC7 (CRQSELSRC7):** Select external input CLKRQ# pin for dynamical control of CLKOUT_SRC7 output. **0000b =** SRC0CLKRQ#/GPIO73 controls CLKOUT_SRC7 **0001b =** SRC1CLKRQ#/GPIO18 controls CLKOUT_SRC7 **0010b =** SRC2CLKRQ#/GPIO20 controls CLKOUT_SRC7 **0011b =** SRC3CLKRQ#/GPIO25 controls CLKOUT_SRC7 **0100b =** SRC4CLKRQ#/GPIO26 controls CLKOUT_SRC7 **0101b =** SRC5CLKRQ#/GPIO44 controls CLKOUT_SRC7 **0110b =** SRC6CLKRQ#/GPIO45 controls CLKOUT_SRC7 **0111b** = SRC7CLKRQ#/GPIO46 controls CLKOUT_SRC7 **1000b** = SRC8CLKRQ#/PEG_A_CLKRQ#/GPIO47 controls CLKOUT_SRC7 **1001b =** SRC9CLKRQ#/PEG_B_CLKRQ#/GPIO56 controls CLKOUT_SRC7 **101xb =** Reserved **1110b =** Reserved **1111b =** Disable dynamic control of CLKOUT_SRC7 ***A-stepping Note:*** This parameter has no effect and the dynamic control CLKOUT_SRC7 output. ***B-stepping Note:*** Parameter behaves normally.
27:24	HW: 0110b ME FW: 1111b FITC: 1111b	**CLKRQ# Select for CLKOUT_SRC6 (CRQSELSRC6):** Select external input CLKRQ# pin for dynamical control of CLKOUT_SRC6 output. **0000b =** SRC0CLKRQ#/GPIO73 controls CLKOUT_SRC6 **0001b =** SRC1CLKRQ#/GPIO18 controls CLKOUT_SRC6 **0010b =** SRC2CLKRQ#/GPIO20 controls CLKOUT_SRC6 **0011b =** SRC3CLKRQ#/GPIO25 controls CLKOUT_SRC6 **0100b =** SRC4CLKRQ#/GPIO26 controls CLKOUT_SRC6 **0101b =** SRC5CLKRQ#/GPIO44 controls CLKOUT_SRC6 **0110b =** SRC6CLKRQ#/GPIO45 controls CLKOUT_SRC6 **0111b** = SRC7CLKRQ#/GPIO46 controls CLKOUT_SRC6 **1000b** = SRC8CLKRQ#/PEG_A_CLKRQ#/GPIO47 controls CLKOUT_SRC6 **1001b =** SRC9CLKRQ#/PEG_B_CLKRQ#/GPIO56 controls CLKOUT_SRC6 **101xb =** Reserved **1110b =** Reserved **1111b =** Disable dynamic control of CLKOUT_SRC6 ***A-stepping Note:*** This parameter has no effect and the dynamic control CLKOUT_SRC6 output. ***B-stepping Note:*** Parameter behaves normally.
23:20	HW: 0101b ME FW: 1111b FITC: 1111b	**CLKRQ# Select for CLKOUT_SRC5 (CRQSELSRC5):** Select external input CLKRQ# pin for dynamical control of CLKOUT_SRC5 output. **0000b =** SRC0CLKRQ#/GPIO73 controls CLKOUT_SRC5 **0001b =** SRC1CLKRQ#/GPIO18 controls CLKOUT_SRC5 **0010b =** SRC2CLKRQ#/GPIO20 controls CLKOUT_SRC5 **0011b =** SRC3CLKRQ#/GPIO25 controls CLKOUT_SRC5 **0100b =** SRC4CLKRQ#/GPIO26 controls CLKOUT_SRC5 **0101b =** SRC5CLKRQ#/GPIO44 controls CLKOUT_SRC5 **0110b =** SRC6CLKRQ#/GPIO45 controls CLKOUT_SRC5 **0111b** = SRC7CLKRQ#/GPIO46 controls CLKOUT_SRC5 **1000b** = SRC8CLKRQ#/PEG_A_CLKRQ#/GPIO47 controls CLKOUT_SRC5

Bits	Default	Description
		1001b = SRC9CLKRQ#/PEG_B_CLKRQ#/GPIO56 controls CLKOUT_SRC5 **101xb =** Reserved **1110b =** Reserved **1111b =** Disable dynamic control of CLKOUT_SRC5 ***A-stepping Note:*** This parameter has no effect and the dynamic control CLKOUT_SRC5 output. ***B-stepping Note:*** Parameter behaves normally.
19:16	HW: 0100b ME FW: 1111b FITC: 1111b	**CLKRQ# Select for CLKOUT_SRC4 (CRQSELSRC4):** Select external input CLKRQ# pin for dynamical control of CLKOUT_SRC4 output. **0000b =** SRC0CLKRQ#/GPIO73 controls CLKOUT_SRC4 **0001b =** SRC1CLKRQ#/GPIO18 controls CLKOUT_SRC4 **0010b =** SRC2CLKRQ#/GPIO20 controls CLKOUT_SRC4 **0011b =** SRC3CLKRQ#/GPIO25 controls CLKOUT_SRC4 **0100b =** SRC4CLKRQ#/GPIO26 controls CLKOUT_SRC4 **0101b** = SRC5CLKRQ#/GPIO44 controls CLKOUT_SRC4 **0110b =** SRC6CLKRQ#/GPIO45 controls CLKOUT_SRC4 **0111b** = SRC7CLKRQ#/GPIO46 controls CLKOUT_SRC4 **1000b** = SRC8CLKRQ#/PEG_A_CLKRQ#/GPIO47 controls CLKOUT_SRC4 **1001b =** SRC9CLKRQ#/PEG_B_CLKRQ#/GPIO56 controls CLKOUT_SRC4 **101xb =** Reserved **1110b =** Reserved **1111b =** Disable dynamic control of CLKOUT_SRC4 ***A-stepping Note:*** This parameter has no effect and the dynamic control CLKOUT_SRC4 output. ***B-stepping Note:*** Parameter behaves normally.

Bits	Default	Description
15:12	HW: 0011b ME FW: 1111b FITC: 1111b	**CLKRQ# Select for CLKOUT_SRC3 (CRQSELSRC3):** Select external input CLKRQ# pin for dynamical control of CLKOUT_SRC3 output. **0000b =** SRC0CLKRQ#/GPIO73 controls CLKOUT_SRC3 **0001b =** SRC1CLKRQ#/GPIO18 controls CLKOUT_SRC3 **0010b =** SRC2CLKRQ#/GPIO20 controls CLKOUT_SRC3 **0011b =** SRC3CLKRQ#/GPIO25 controls CLKOUT_SRC3 **0100b =** SRC4CLKRQ#/GPIO26 controls CLKOUT_SRC3 **0101b =** SRC5CLKRQ#/GPIO44 controls CLKOUT_SRC3 **0110b =** SRC6CLKRQ#/GPIO45 controls CLKOUT_SRC3 **0111b** = SRC7CLKRQ#/GPIO46 controls CLKOUT_SRC3 **1000b** = SRC8CLKRQ#/PEG_A_CLKRQ#/GPIO47 controls CLKOUT_SRC3 **1001b =** SRC9CLKRQ#/PEG_B_CLKRQ#/GPIO56 controls CLKOUT_SRC3 **101xb =** Reserved **1110b =** Reserved **1111b =** Disable dynamic control of CLKOUT_SRC3 ***A-stepping Note:*** This parameter has no effect and the dynamic control CLKOUT_SRC3 output. ***B-stepping Note:*** Parameter behaves normally.
11:8	HW: 0010b ME FW: 1111b FITC: 1111b	**CLKRQ# Select for CLKOUT_SRC2 (CRQSELSRC2):** Select external input CLKRQ# pin for dynamical control of CLKOUT_SRC2 output. **0000b =** SRC0CLKRQ#/GPIO73 controls CLKOUT_SRC2 **0001b =** SRC1CLKRQ#/GPIO18 controls CLKOUT_SRC2 **0010b =** SRC2CLKRQ#/GPIO20 controls CLKOUT_SRC2 **0011b =** SRC3CLKRQ#/GPIO25 controls CLKOUT_SRC2 **0100b =** SRC4CLKRQ#/GPIO26 controls CLKOUT_SRC2 **0101b =** SRC5CLKRQ#/GPIO44 controls CLKOUT_SRC2 **0110b =** SRC6CLKRQ#/GPIO45 controls CLKOUT_SRC2 **0111b** = SRC7CLKRQ#/GPIO46 controls CLKOUT_SRC2 **1000b** = SRC8CLKRQ#/PEG_A_CLKRQ#/GPIO47 controls CLKOUT_SRC2 **1001b =** SRC9CLKRQ#/PEG_B_CLKRQ#/GPIO56 controls CLKOUT_SRC2 **101xb =** Reserved **1110b =** Reserved **1111b =** Disable dynamic control of CLKOUT_SRC2 ***A-stepping Note:*** This parameter has no effect and the dynamic control CLKOUT_SRC2 output. ***B-stepping Note:*** Parameter behaves normally.
7:4	HW: 0001b ME FW: 1111b FITC: 1111b	**CLKRQ# Select for CLKOUT_SRC1 (CRQSELSRC1):** Select external input CLKRQ# pin for dynamical control of CLKOUT_SRC1 output. **0000b =** SRC0CLKRQ#/GPIO73 controls CLKOUT_SRC1 **0001b =** SRC1CLKRQ#/GPIO18 controls CLKOUT_SRC1 **0010b =** SRC2CLKRQ#/GPIO20 controls CLKOUT_SRC1 **0011b =** SRC3CLKRQ#/GPIO25 controls CLKOUT_SRC1 **0100b =** SRC4CLKRQ#/GPIO26 controls CLKOUT_SRC1 **0101b =** SRC5CLKRQ#/GPIO44 controls CLKOUT_SRC1 **0110b =** SRC6CLKRQ#/GPIO45 controls CLKOUT_SRC1 **0111b** = SRC7CLKRQ#/GPIO46 controls CLKOUT_SRC1 **1000b** = SRC8CLKRQ#/PEG_A_CLKRQ#/GPIO47 controls CLKOUT_SRC1 **1001b =** SRC9CLKRQ#/PEG_B_CLKRQ#/GPIO56 controls CLKOUT_SRC1 **101xb =** Reserved **1110b =** Reserved **1111b =** Disable dynamic control of CLKOUT_SRC1 ***A-stepping Note:*** This parameter has no effect and the dynamic control CLKOUT_SRC1 output. ***B-stepping Note:*** Parameter behaves normally.

Bits	Default	Description
3:0	HW: 0000b ME FW: 1111b FITC: 1111b	**CLKRQ# Select for CLKOUT_SRC0 (CRQSELSRC0):** Select external input CLKRQ# pin for dynamical control of CLKOUT_SRC0 output. **0000b =** SRC0CLKRQ#/GPIO73 controls CLKOUT_SRC0 **0001b =** SRC1CLKRQ#/GPIO18 controls CLKOUT_SRC0 **0010b =** SRC2CLKRQ#/GPIO20 controls CLKOUT_SRC0 **0011b =** SRC3CLKRQ#/GPIO25 controls CLKOUT_SRC0 **0100b =** SRC4CLKRQ#/GPIO26 controls CLKOUT_SRC0 **0101b =** SRC5CLKRQ#/GPIO44 controls CLKOUT_SRC0 **0110b =** SRC6CLKRQ#/GPIO45 controls CLKOUT_SRC0 **0111b** = SRC7CLKRQ#/GPIO46 controls CLKOUT_SRC0 **1000b** = SRC8CLKRQ#/PEG_A_CLKRQ#/GPIO47 controls CLKOUT_SRC0 **1001b =** SRC9CLKRQ#/PEG_B_CLKRQ#/GPIO56 controls CLKOUT_SRC0 **101xb =** Reserved **1110b =** Reserved **1111b =** Disable dynamic control of CLKOUT_SRC0 ***A-stepping Note:*** This parameter has no effect and the dynamic control CLKOUT_SRC0 output. ***B-stepping Note:*** Parameter behaves normally.

A.2.13 PMSRCCLK2 – SRC Power Management

BTM/DCI Default: 0000 0F98h
ME FW/Flash Image Tool and Config Wizard Default: FFFF FFFFh
0000 0FFFh
Description: This parameter assigns dynamic CLKRQ# control of SRC clocks
Flash Image Tool Configuration: Flash Image | Configuration | ICC Data | OEM Request Record [6:0] | Static Registers Section

Table 6-15. SRC Power Management

Bits	Default	Description
31:12	0h	**Reserved (RSVD)**
11:8	HW: 1001b ME FW: 1111b FITC: 1111b	**Chipset Configuration (PCHCFG):** Must be set to **1111b**.
7:4	HW: 1000b ME FW: 1111b FITC: 1111b	**CLKRQ# Select for CLKOUT_PEG_B (CRQSELPEGB):** Select external input CLKRQ# pin for dynamical control of CLKOUT_PEG_B output. **0000b =** SRC0CLKRQ#/GPIO73 controls CLKOUT_PEG_B **0001b =** SRC1CLKRQ#/GPIO18 controls CLKOUT_PEG_B **0010b =** SRC2CLKRQ#/GPIO20 controls CLKOUT_PEG_B **0011b =** SRC3CLKRQ#/GPIO25 controls CLKOUT_PEG_B **0100b =** SRC4CLKRQ#/GPIO26 controls CLKOUT_PEG_B **0101b =** SRC5CLKRQ#/GPIO44 controls CLKOUT_PEG_B **0110b =** SRC6CLKRQ#/GPIO45 controls CLKOUT_PEG_B **0111b** = SRC7CLKRQ#/GPIO46 controls CLKOUT_PEG_B **1000b** = SRC8CLKRQ#/PEG_A_CLKRQ#/GPIO47 controls CLKOUT_PEG_B **1001b** = SRC9CLKRQ#/PEG_B_CLKRQ#/GPIO56 controls CLKOUT_PEG_B **101xb =** Reserved **1110b =** Reserved **1111b =** Disable dynamic control of CLKOUT_PEG_B ***A-stepping Note:*** This parameter has no effect and the dynamic control CLKOUT_PEG_B output. ***B-stepping Note:*** Parameter behaves normally.
3:0	HW: 1000b ME FW: 1111b FITC: 1111b	**CLKRQ# Select for CLKOUT_PEG_A (CRQSELPEGA):** Select external input CLKRQ# pin for dynamical control of CLKOUT_PEG_A output. **0000b =** SRC0CLKRQ#/GPIO73 controls CLKOUT_PEG_A **0001b =** SRC1CLKRQ#/GPIO18 controls CLKOUT_PEG_A **0010b =** SRC2CLKRQ#/GPIO20 controls CLKOUT_PEG_A **0011b =** SRC3CLKRQ#/GPIO25 controls CLKOUT_PEG_A **0100b =** SRC4CLKRQ#/GPIO26 controls CLKOUT_PEG_A **0101b =** SRC5CLKRQ#/GPIO44 controls CLKOUT_PEG_A **0110b =** SRC6CLKRQ#/GPIO45 controls CLKOUT_PEG_A **0111b** = SRC7CLKRQ#/GPIO46 controls CLKOUT_PEG_A **1000b** = SRC8CLKRQ#/PEG_A_CLKRQ#/GPIO47 controls CLKOUT_PEG_A **1001b =** SRC9CLKRQ#/PEG_B_CLKRQ#/GPIO56 controls CLKOUT_PEG_A **101xb =** Reserved **1110b =** Reserved **1111b =** Disable dynamic control of CLKOUT_PEG_A ***A-stepping Note:*** This parameter has no effect and the dynamic control CLKOUT_PEG_A output. ***B-stepping Note:*** Parameter behaves normally.

Appendix B – Flash Configurations

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

Figure 6-3. Configuration "A" — Desktop / Server / Workstation or Mobile

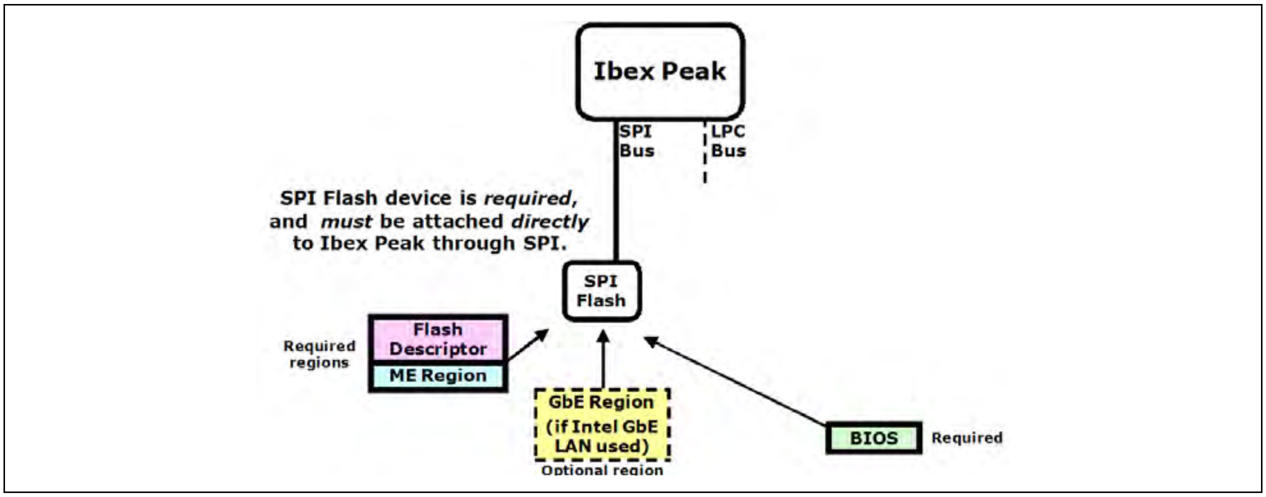

Ibex Peak
SPI Bus
LPC Bus
SPI Flash device is *required*, and *must* be attached *directly* to Ibex Peak through SPI.
SPI Flash
Required regions
Flash Descriptor
ME Region
GbE Region (if Intel GbE LAN used)
Optional region
BIOS
Required

Figure 6-4. Configuration "B" — Mobile Only

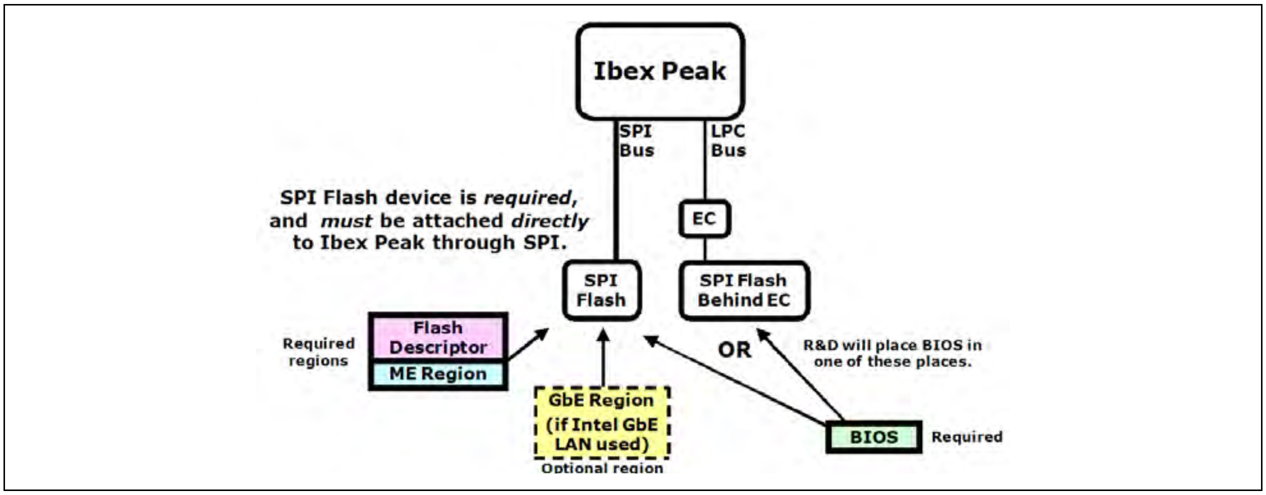

Ibex Peak
SPI Bus
LPC Bus
SPI Flash device is *required*, and *must* be attached *directly* to Ibex Peak through SPI.
EC
SPI Flash
SPI Flash Behind EC
Required regions
Flash Descriptor
ME Region
OR
R&D will place BIOS in one of these places.
GbE Region (if Intel GbE LAN used)
Optional region
BIOS
Required

Figure 6-5. Configuration "C" — Desktop / Server / Workstation Only

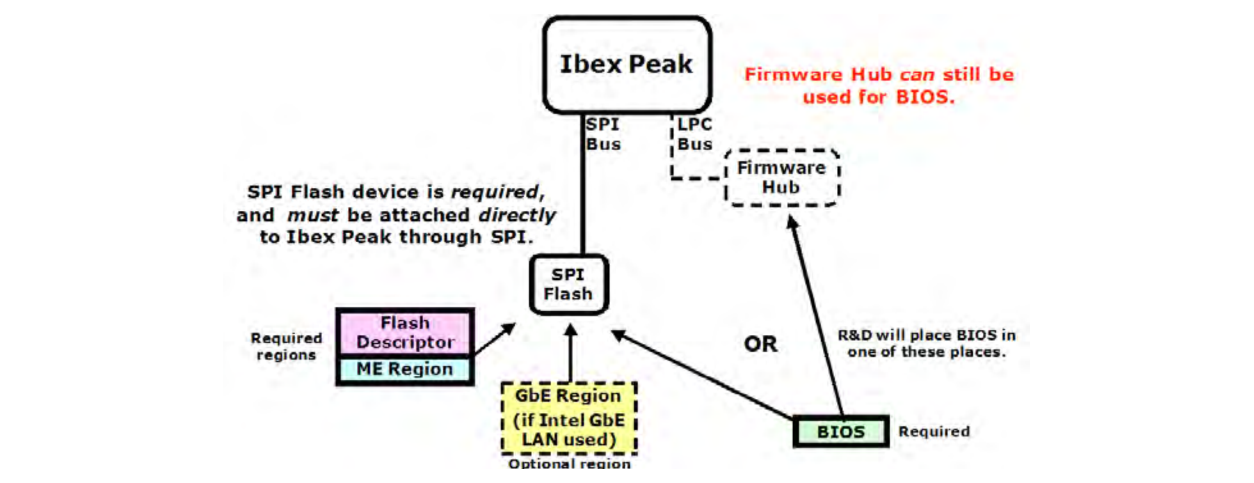
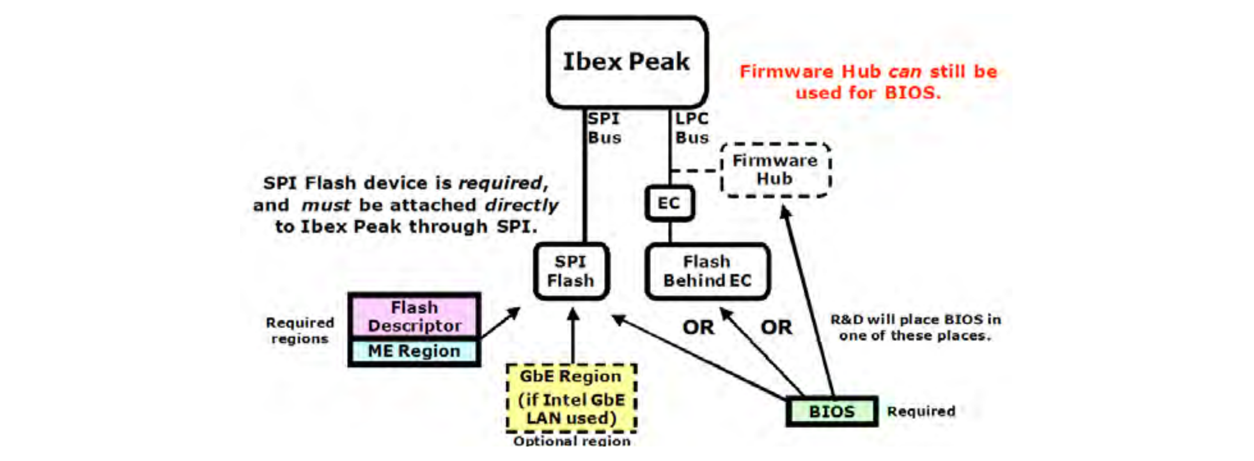

Ibex Peak
Firmware Hub can still be used for BIOS.
SPI Bus
LPC Bus
Firmware Hub
SPI Flash device is required, and must be attached directly to Ibex Peak through SPI.
SPI Flash
Required regions
Flash Descriptor
ME Region
OR
R&D will place BIOS in one of these places.
GbE Region (if Intel GbE LAN used)
Optional region
BIOS
Required

Figure 6-6. Configuration "D" — Mobile Only


Ibex Peak
Firmware Hub can still be used for BIOS.
SPI Bus
LPC Bus
Firmware Hub
EC
SPI Flash device is required, and must be attached directly to Ibex Peak through SPI.
SPI Flash
Flash Behind EC
Required regions
Flash Descriptor
ME Region
OR
OR
R&D will place BIOS in one of these places.
GbE Region (if Intel GbE LAN used)
Optional region
BIOS
Required

Appendix C – Configuration Parameter Details

C.1 Firmware Update Override

When **Local FWU Override Counter** has a value between 1 and 255, firmware updates are allowed even if updates are disabled in the ME BIOS Extension settings. After the flash is programmed, each time the machine restarts it causes **Local FWU Override Counter** to be decremented. When **Local FWU Override Counter** reaches 0, firmware updates are no longer allowed if they are not enabled by the MEBx settings.

Note: The restart that takes place after the flash memory has been programmed also causes **Local FWU Override Counter** to be decremented. Therefore if you want to enable updating the firmware **N** times, you need to assign **Local FWU Override Counter** the initial value **N+1**.

If **Local FWU Override Counter** is set to -1 and **Local Firmware Override Qualifier** is set to 0, firmware updates are always allowed regardless of the settings in the MEBx.

The following table shows the possible value combinations for the two variables. To enable local firmware updates, make sure both variables are assigned the correct values.

Table 6-16. Firmware Override Update Variables

	Local FWU Override Qualifier = 0 (zero)	Local FWU Override Qualifier = 1 (one)	Local FWU Override Qualifier = 2 (two)
Local FWU Override counter = 0 (zero)	Local Firmware Updates NOT Allowed	Local Firmware Updates NOT Allowed	Local Firmware Updates NOT Allowed
Local FWU Override Counter = -1 (minus one)	Local Firmware Updates Allowed	Local Firmware Updates NOT Allowed	Local Firmware Updates Allowed only until ME is configured
Local FWU Override Counter = 0<n<255	Local Firmware Updates Allowed	Local Firmware Updates Allowed	Local Firmware Updates Allowed

C.2 Flash Descriptor Override Pin Strap Ignore

This bit determines if ME will be disabled when the manufacturing override jumper set.

False – ME will enters a disabled state to safely program the full SPI device if the manufacturing mode jumper is set.

True – ME will NOT enter a disabled if the manufacturing mode jumper is set.

C.3 Si features parameters

These options allow for various debugging features.

Table 6-17. Si Features Options

Parameter	Description	Default Value
Debug Si Features	Bit 0: Disable timeout on BIOS HECI messaging Bit 1: Disable FW watchdog timer	**0x00000000**
Prod Si Features	Bit 1: Disable FW watchdog timer	**0x00000000**

C.4 Features Supported

These options control the availability / visibility of firmware features.

In instances where a specific feature is configurable in the MEBx disabling it through the 'Features Supported' section will hide / disable that specific feature in the MEBx.

The ability to change certain options is SKU dependent and some of default values will be grayed out and will not be changeable depending on the SKU Selected.

Note:

The Intel® Manageability Application setting combines several manageability technologies that are related to each other. This setting controls the following manageability technologies:

Intel® Active Management Technology
Intel® Standard Management
Intel® Remote PC Asset Technology for Consumer
Intel® Remote PC Asset Technology for Business
Fast Call for Help
Intel® KVM Remote Assistance Application

Setting "Intel® Manageability Application Permanently Disabled?" to "Yes" will permanently disable all the features listed above without any way to enable them at a later time. The only way to re-enable these features is to completely re-burn the ME region with this setting value set to "No." A firmware update using ***FWUpdLcl.exe*** cannot re-enable features.

Note: Consumer OEMs should configure their image with Intel ® Remote Wake Technology to be permanently 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 6-18. Feature default settings by SKU

SKU	Feature	Default Value
Intel® Q57	Enable Intel® Standard Manageability; Disable Intel® AMT	No
	Intel® Manageability Application Permanently Disabled?	No
	PAVP 1.5 Permanently Disabled?	No
	Intel® QST Permanently Disabled?	No
	Intel® Identity Protection Technology Permanently Disabled?	Yes
	Intel® Remote Wake Technology Permanently Disabled?	Yes
	KVM Permanently Disabled?	No
	TLS Permanently Disabled?	No
	Intel® Anti-Theft Technology Permanently Disabled?	No
	Intel® Manageability Application Enable / Disable	Enabled
	Intel® QST Enable / Disable	Enabled
	Intel® Identity Protection Technology Enable / Disable	Disabled
	Intel® Remote Wake Technology Enable / Disable	Disabled
Intel® H57	Enable Intel® Standard Manageability; Disable Intel® AMT	Yes
	Intel® Manageability Application Permanently Disabled?	No
	PAVP 1.5 Permanently Disabled?	No
	Intel® QST Permanently Disabled?	No
	Intel® Identity Protection Technology Permanently Disabled?	No
	Intel® Remote Wake Technology Permanently Disabled?	No
	KVM Permanently Disabled?	No
	TLS Permanently Disabled?	No
	Intel® Anti-Theft Technology Permanently Disabled?	No
	Intel® Manageability Application Enable / Disable	Enabled
	Intel® QST Enable / Disable	Enabled
	Intel® Identity Protection Technology Enable / Disable	Enabled
	Intel® Remote Wake Technology Enable / Disable	Enabled
Intel® H55	Enable Intel® Standard Manageability; Disable Intel® AMT	Yes
	Intel® Manageability Application Permanently Disabled?	No
	PAVP 1.5 Permanently Disabled?	No
	Intel® QST Permanently Disabled?	No
	Intel® Identity Protection Technology Permanently Disabled?	No
	Intel® Remote Wake Technology Permanently Disabled?	No
	KVM Permanently Disabled?	No

SKU	Feature	Default Value
	TLS Permanently Disabled?	No
	Intel® Anti-Theft Technology Permanently Disabled?	Yes
	Intel® Manageability Application Enable / Disable	Enabled
	Intel® QST Enable / Disable	Enabled
	Intel® Identity Protection Technology Enable / Disable	Enabled
	Intel® Remote Wake Technology Enable / Disable	Enabled
[redacted]	[redacted]	[redacted]
Intel® QM57	Enable Intel® Standard Manageability; Disable Intel® AMT	No
	Intel® Manageability Application Permanently Disabled?	No
	PAVP 1.5 Permanently Disabled?	No
	Intel® QST Permanently Disabled?	Yes
	Intel® Identity Protection Technology Permanently Disabled?	Yes
	Intel® Remote Wake Technology Permanently Disabled?	Yes
	KVM Permanently Disabled?	No
	TLS Permanently Disabled?	No
	Intel® Anti-Theft Technology Permanently Disabled?	No
	Intel® Manageability Application Enable / Disable	Enabled
	Intel® QST Enable / Disable	Disabled
	Intel® Identity Protection Technology Enable / Disable	Disabled
	Intel® Remote Wake Technology Enable / Disable	Disabled
[redacted]	[redacted]	[redacted]
Intel® QS57	Enable Intel® Standard Manageability; Disable Intel® AMT	No
	Intel® Manageability Application Permanently Disabled?	No
	PAVP 1.5 Permanently Disabled?	No
	Intel® QST Permanently Disabled?	Yes
	Intel® Identity Protection Technology Permanently Disabled?	Yes
	Intel® Remote Wake Technology Permanently Disabled?	Yes
	KVM Permanently Disabled?	No
	TLS Permanently Disabled?	No
	Intel® Anti-Theft Technology Permanently Disabled?	No
	Intel® Manageability Application Enable / Disable	Enabled
	Intel® QST Enable / Disable	Disabled
	Intel® Identity Protection Technology Enable / Disable	Disabled
	Intel® Remote Wake Technology Enable / Disable	Disabled
[redacted]	[redacted]	[redacted]
Intel® HM57	Enable Intel® Standard Manageability; Disable Intel® AMT	Yes
	Intel® Manageability Application Permanently Disabled?	No
	PAVP 1.5 Permanently Disabled?	No
	Intel® QST Permanently Disabled?	Yes
	Intel® Identity Protection Technology Permanently Disabled?	No
	Intel® Remote Wake Technology Permanently Disabled?	Yes
	KVM Permanently Disabled?	No

SKU	Feature	Default Value
	TLS Permanently Disabled?	No
	Intel® Anti-Theft Technology Permanently Disabled?	No
	Intel® Manageability Application Enable / Disable	Enabled
	Intel® QST Enable / Disable	Disabled
	Intel® Identity Protection Technology Enable / Disable	Enabled
	Intel® Remote Wake Technology Enable / Disable	Disabled
[redacted]	[redacted]	[redacted]
Intel® HM55	Enable Intel® Standard Manageability; Disable Intel® AMT	Yes
	Intel® Manageability Application Permanently Disabled?	Yes
	PAVP 1.5 Permanently Disabled?	No
	Intel® QST Permanently Disabled?	Yes
	Intel® Identity Protection Technology Permanently Disabled?	Yes
	Intel® Remote Wake Technology Permanently Disabled?	Yes
	KVM Permanently Disabled?	Yes
	TLS Permanently Disabled?	Yes
	Intel® Anti-Theft Technology Permanently Disabled?	Yes
	Intel® Manageability Application Enable / Disable	Disabled
	Intel® QST Enable / Disable	Disabled
	Intel® Identity Protection Technology Enable / Disable	Disabled
	Intel® Remote Wake Technology Enable / Disable	Disabled
[redacted]	[redacted]	[redacted]
Intel® 3450	Enable Intel® Standard Manageability; Disable Intel® AMT	No
	Intel® Manageability Application Permanently Disabled?	No
	PAVP 1.5 Permanently Disabled?	No
	Intel® QST Permanently Disabled?	No
	Intel® Identity Protection Technology Permanently Disabled?	Yes
	Intel® Remote Wake Technology Permanently Disabled?	Yes
	KVM Permanently Disabled?	No
	TLS Permanently Disabled?	No
	Intel® Anti-Theft Technology Permanently Disabled?	No
	Intel® Manageability Application Enable / Disable	Enabled
	Intel® QST Enable / Disable	Enabled
	Intel® Identity Protection Technology Enable / Disable	Disabled
	Intel® Remote Wake Technology Enable / Disable	Disabled

C.5 Setup and Configuration

These options allow OEMs enter and enable up to 22 custom Remote Configuration Hash values into their firmware image.

Note: Base firmware images contain 5 pre-defined Hash values.

Hash 'x' Active where **'x'** represents one of the 22 possible Remote Configuration Hash entries determines if the specific Hash entry is enabled or disabled.

Hash 'x' Friendly Name where **'x'** represents one of the 22 possible Remote Configuration Hash entries determines the Friendly name designation for that Hash entry.

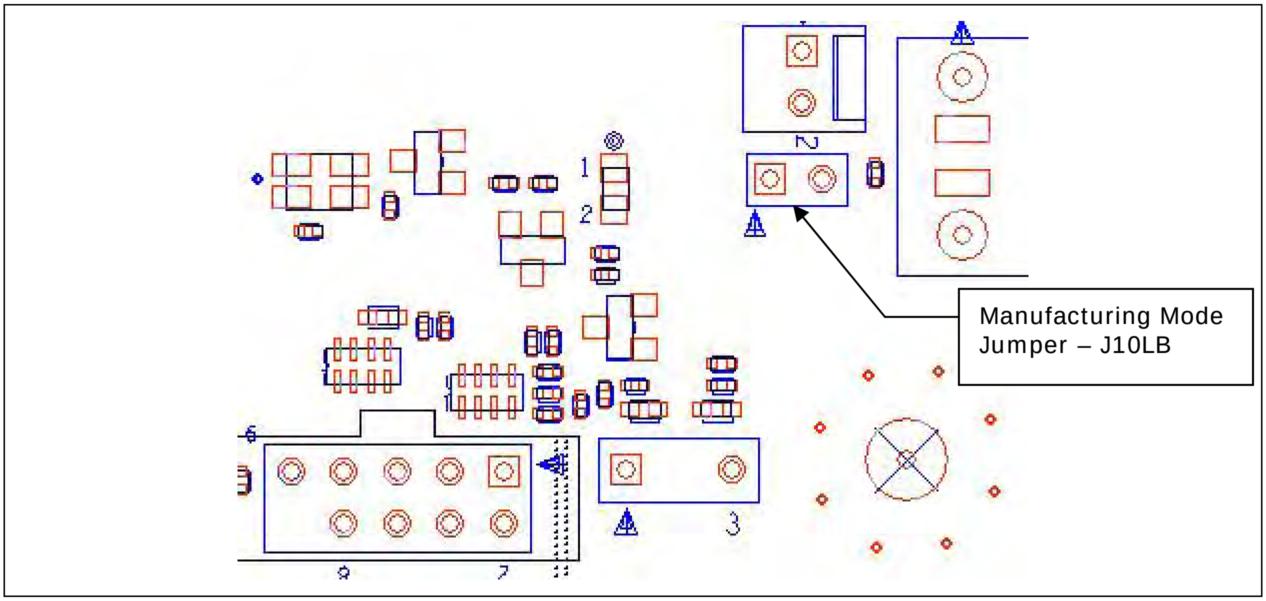
Hash 'x' Stream where **'x'** represents one of the 22 possible Remote Configuration Hash entries designates the either the Raw Hash value or certificate file for that Hash entry.

Appendix D – Desktop CRB Information

D.6 Manufacturing Mode Jumper

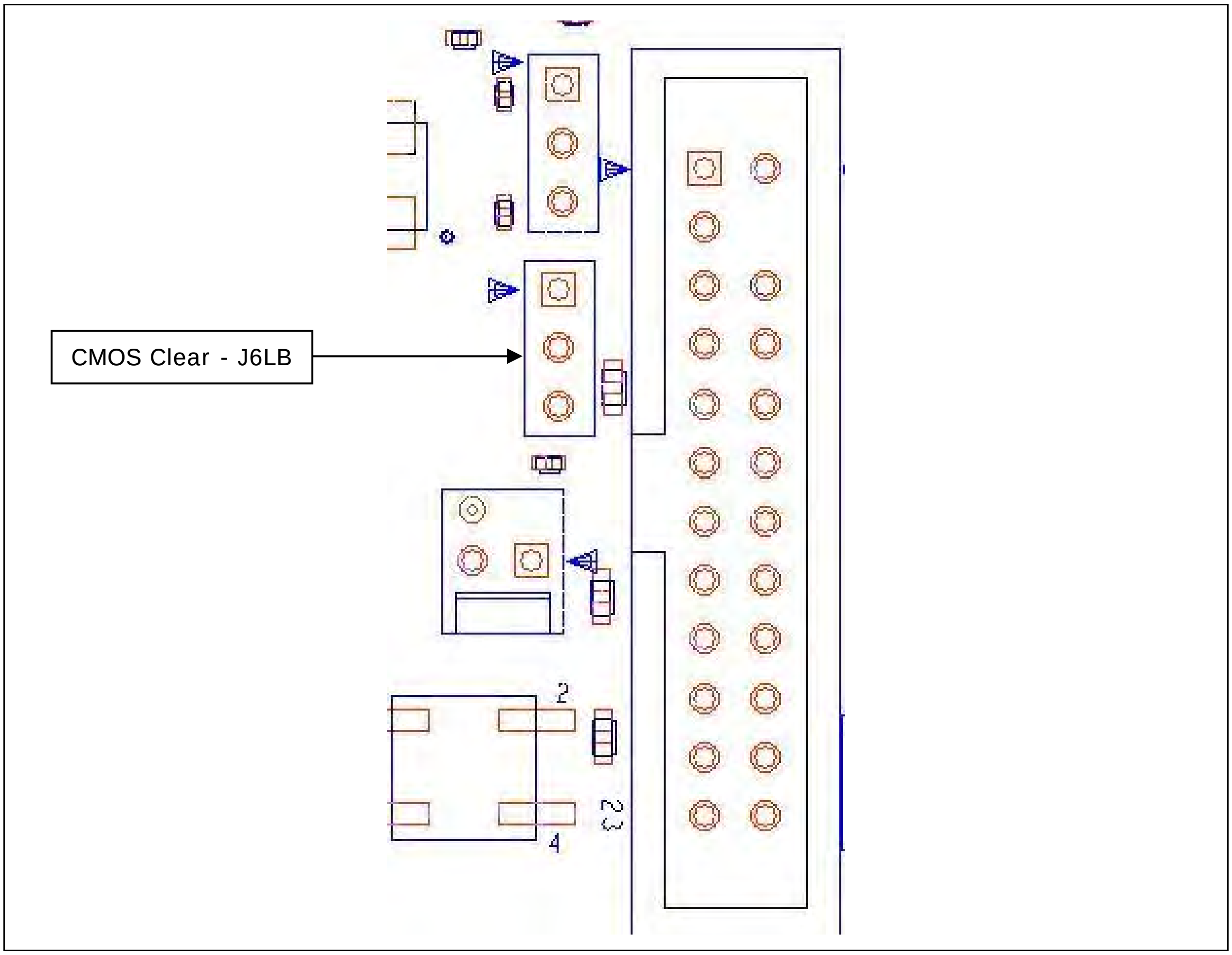
The Manufacturing Mode (Flash Override) jumper permits or denies CPU write access to the SPI flash devices at the hardware level. When this jumper is open, the CPU will not have write access to the flash (if those permissions are not present in firmware). Normally these permissions are set in the firmware image, so this jumper would normally only be set in the event you need to override the firmware permission settings to write a new image to flash. Close this jumper only if you need to override firmware permissions to load a new ME firmware image onto the flash part (when permissions set in FW would otherwise prevent you from doing so). This jumper should be removed (left open) under normal operating conditions, wherein access permissions to the flash are controlled by the firmware.

Figure 6-7. Desktop CRB Manufacturing Mode Jumper Location



D.7 CMOS Clear Jumper

Figure 6-8. Desktop CRB CMOS Clear Location

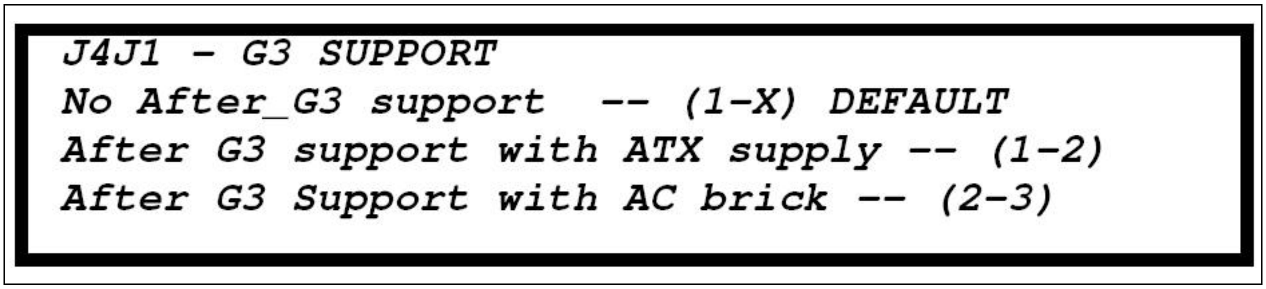


Appendix E – Mobile CRB Information

E.1 Redfort G3 Support

The following information is required in order to enable G3 support on the Redfort Mobile CRB.

Figure 6-9. Redfort CRB G3 Support



```
J4J1 - G3 SUPPORT
No After_G3 support  -- (1-X) DEFAULT
After G3 support with ATX supply -- (1-2)
After G3 Support with AC brick -- (2-3)
```

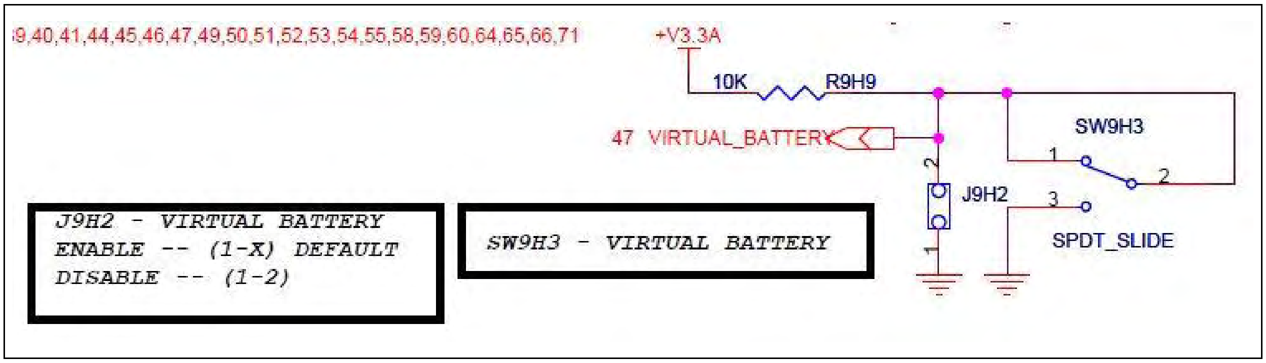
E.2 Redfort Virtual AC / DC Operation

The following information is required in order to enable / disable the Virtual Battery (AC / DC) mode support on the Redfort Mobile CRB.

It can be selected by one of the following methods:

1. Keeping pin 1-2 of J9H2 open and SW9H3 in 1-2 position indicates the system is in AC mode.
2. Keeping pin 1-2 of J9H2 shorted or SW9H3 in 2-3 position indicates the system is in DC mode.

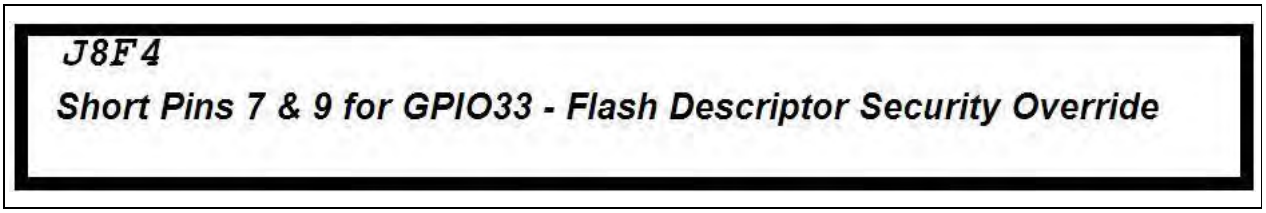
Figure 6-10. Redfort CRB Virtual Battery Jumper



E.3 Redfort Manufacturing Mode Jumper Location

The Manufacturing Mode (Flash Override) jumper permits or denies CPU write access to the SPI flash devices at the hardware level. When this jumper is open, the CPU will not have write access to the flash (if those permissions are not present in firmware). Normally these permissions are set in the firmware image, so this jumper would normally only be set in the event you need to override the firmware permission settings to write a new image to flash. Close this jumper only if you need to override firmware permissions to load a new ME firmware image onto the flash part (when permissions set in FW would otherwise prevent you from doing so). This jumper should be removed (left open) under normal operating conditions, wherein access permissions to the flash are controlled by the firmware.

Figure 6-11. Redfort CRB Manufacturing Mode Jumper



J8F4

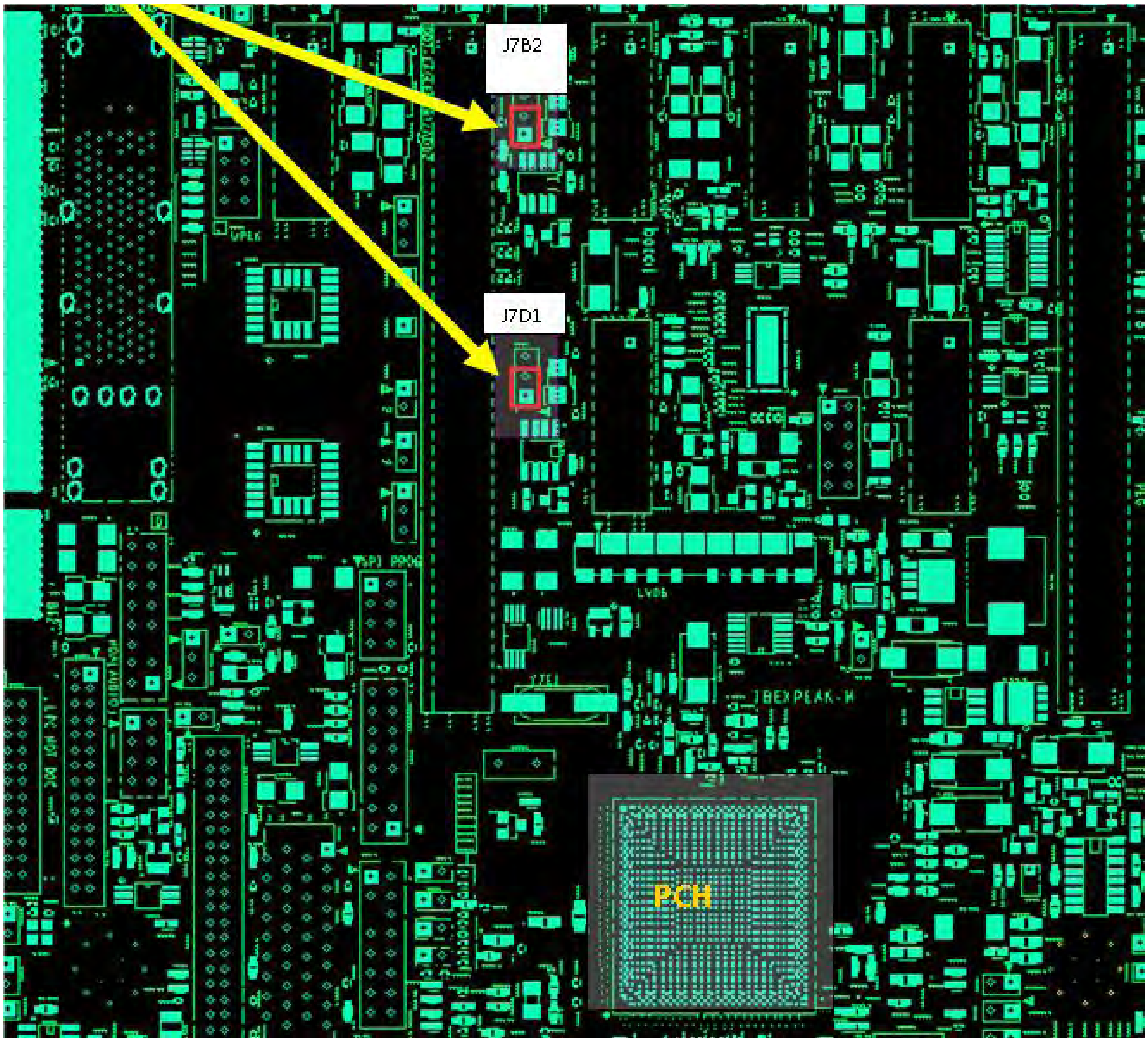
Short Pins 7 & 9 for GPIO33 - Flash Descriptor Security Override

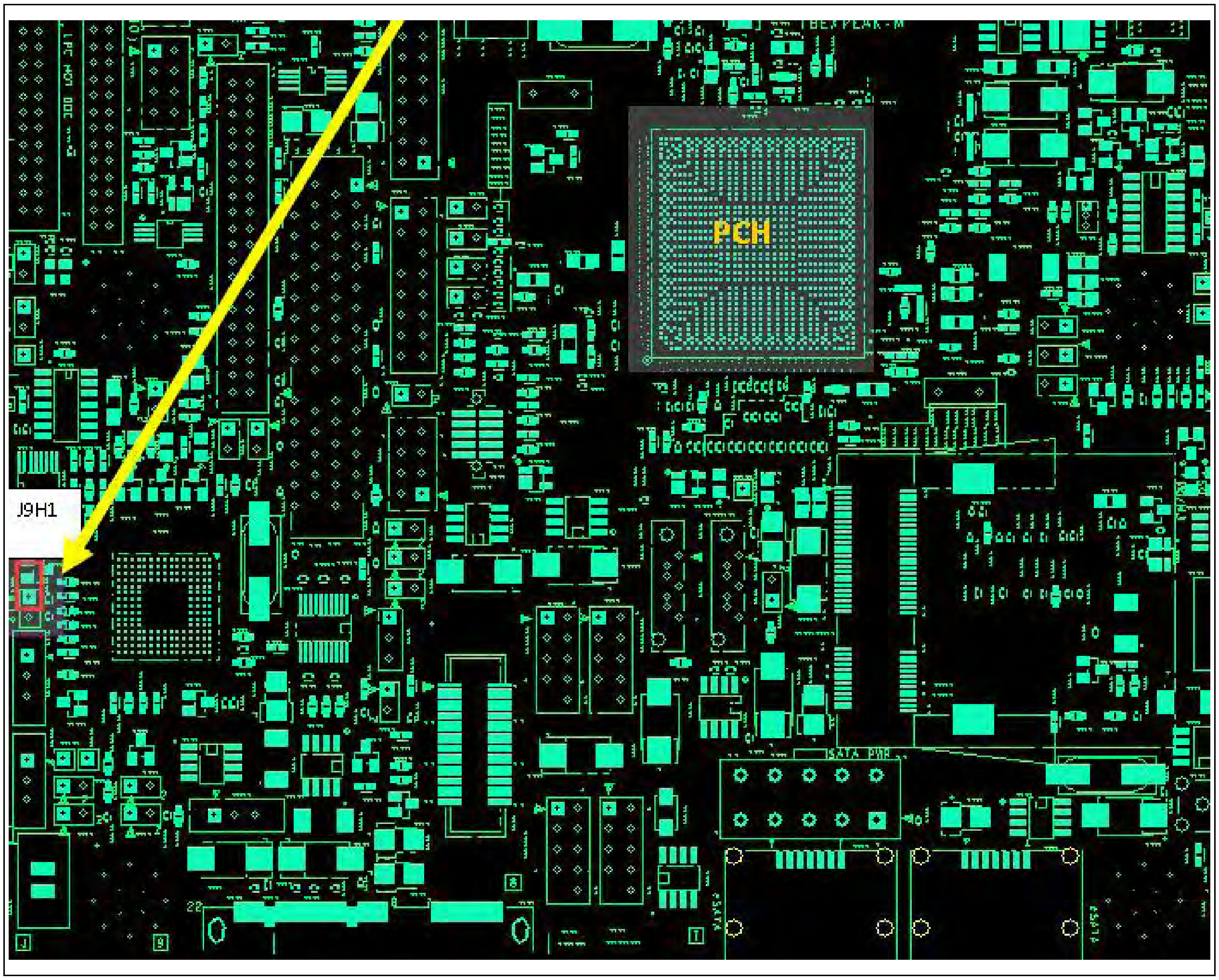
E.4 Redfort Virtual AC / DC Operation

Make sure you are setting the jumpers correctly

- Set jumper J7B2 to pin 1-2 (short)
- Set jumper J7D1 to pin 1-2 (short)
- Set jumper J9H1 to pin 1-X (Open) (on the next page)

Figure 6-12. Redfort ME WLAN Power Control Jumper settings




J9H1
PCH
IBEX PEAK-M
SATA PWR

Appendix F – Basic Bring-up steps

F.5 Basic Intel® AMT Bring-up steps

The following information is for basic bring-up to verify basic functionality for Intel® AMT, WebUI and Ping response on the platform.

Figure 6-13. Basic Intel® AMT testing steps

Configure your type FITc under the Configuration tab for either Desktop or MOBILE using steps outlined in Configuration Parameters section **2**.
Create SPI flash binary image using FITc by following steps as documented in the Firmware Bring-up guide.
Load SPI binary image into the target platform's SPI device(s) using FPT (Flash Image Tool), or a flash programmer.
Boot the system and verify that you are seeing the MEBx CTRL-P prompt.
Enter MEBx and set manageability mode to AMT.
Boot the system verify that the Windows OS is up and running and install MEI and LMS / SOL drivers. **NOTE:** This document assumes you have downloaded and properly installed the required .NET version 3.5 provided as separate download from the actual Firmware / Tools kit releases posted on VIP prior to loading the MEI / LMS Driver stack. **Link:** http://download.microsoft.com/download/6/0/f/60fc5854-3cb8-4892-b6db-bd4f42510f28/dotnetfx35.exe
Connect to AMT using the WebUI and verify that AMT responds back.
Boot the system and verify that the Windows OS is up and running and then connect to AMT and you are able to receive ping response.

Appendix G – Intel® AMT 6.0 Errata

On exiting PRE provisioning state in corporate platforms, Intel® AMT / Configuration Server provisioning logic shall automatically set power package 2 as the current power package (S0 only + ME Wake on Sx for desktop, S0 only + ME Wake on Sx/AC for mobile).

Note: This behavior is specific to Intel ® AMT 6.0 only. No assumptions should be made that this behavior will be carried forward into future Intel ® AMT product releases.