

Ibex Peak Intel® Management Engine

Firmware Bring Up Guide

May 2009

Revision 0.74

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.

Copyright © 2009, Intel Corporation. All rights reserved.



Contents

1	Introduction	8
1.1	Purpose and Scope of this Document	8
1.2	Related Documentation	8
1.3	Intel® ME Firmware Features	9
1.4	Prerequisites	10
1.5	Acronyms and Definitions	11
1.5.1	General	11
1.5.2	Intel® Management Engine	12
1.5.3	System States and Power Management	13
1.6	Reference Documents	14
1.7	Number and Format	15
2	Braidwood Technology.....	16
2.1	Braidwood Firmware Bringup Process	16
2.2	NAND Configuration	18
2.2.1	NANDUtil Tool.....	18
3	Intel® QST Image Generation	20
3.1	Intel® QST INI files	20
3.2	Intel® QST Configuration Tool	20
3.2.1	Intel® QST Configuration DOS Tool	20
3.2.2	Intel® QST Configuration Windows* Tool	21
4	Quick Start and Kit Contents.....	23
4.1	Quick Start.....	24
4.2	Kit Contents	24
5	Bring Up Process — All Platforms.....	32
5.1	Bring Up Process.....	32
5.2	Assemble the SPI Flash Binary Image	32
5.2.1	Set Up the Build Environment	32
5.2.2	Load the Default Settings XML File.....	34
5.2.3	FITc Selection for CRB	34
5.2.4	Set Up GbE LAN PHY Firmware Region.....	35
5.2.5	Set Up Intel® ME Firmware Region.....	36
5.2.6	Selecting Platform SKU	38
5.2.7	Set Up BIOS Region.....	39
5.2.8	Set Up Descriptor and SPI Flash Device(s)	40
5.2.9	Set Up Soft Straps	46
5.2.10	Disable Platform Data Store Region	53
5.2.11	Configuration Parameters	54
5.2.12	Program Clock Control Parameters.....	66
5.2.13	Save Your Settings (Optional)	72
5.2.14	Build SPI Flash Binary Image	72
5.3	Burning the SPI Flash Image Binary.....	72
5.4	Flash Burner/Programmer	72
5.5	Flash Programming Tool.....	73
5.5.1	DOS Version.....	73
5.5.2	Windows* Version	74



6	Intel® Remote PC Assist Technology (RPAT).....	75
6.1	Intel® RPAT Consumer Firmware Bringup Process:	75
6.1.1	Intel® RPAT Consumer Bring Up	75
	Please Follow sections 5.1 – 5.2.1 as describe above (Assemble the SPI Flash Binary Image, Set Up the Build Environment).....	75
6.1.2	Selecting Intel® RPAT Consumer Platform SKU	75
6.1.3	Intel® RPAT Consumer bring up continued	76
6.1.4	Intel® RPAT Consumer Configuration Parameters	77
6.1.5	Intel® RPAT Consumer bring up cont.	83
6.2	Intel® RPAT Business Firmware Bringup Process	84
6.2.1	Intel® RPAT Business Bring Up	84
	Please Follow sections 5.1 – 5.2.1 as describe above (Assemble the SPI Flash Binary Image, Set Up the Build Environment).....	84
6.2.2	Selecting Intel® RPAT Business Platform SKU	84
6.2.3	Intel® RPAT Business bring-up continued	85
6.2.4	Intel® RPAT Business Configuration Parameters	85
6.2.5	Intel® RPAT Bussines bring up continued	92
7	Consumer SKU Intel® Identity Protection (Sentry Peak)	93
7.1	Intel® Identity Protection (Sentry Peak) Configuration:	93
7.2	Intel® Identity Protection Technology Verification Test	93
7.2.1	MEInfo Tool.....	94
7.2.2	MEInfo DOS Tool.....	94
7.2.3	MEInfo Windows Tool.....	95
	Appendix A – Ibex Peak Clock Configuration	96
A.1	Functional Blocks	97
A.2	Intel® ME Firmware Clock Control Parameters	97
A.2.1	FCSS – Flex Clock Source Select.....	98
A.2.2	OCKEN – Output Clock Enable.....	99
A.2.3	IBEN – Input Buffer Enable.....	101
A.2.4	PM1 – Power Management.....	102
A.2.5	PM2 – Power Management.....	103
A.2.6	SEBP1 – Single Ended Buffer Parameters.....	103
A.2.7	SEBP2 – Single Ended Buffer Parameters.....	105
A.2.8	PMSRCCLK1 – SRC Power Management	107
A.2.9	PMSRCCLK2 – SRC Power Management	110
	Appendix B – Flash Configurations.....	112
	Appendix C – Configuration Parameter Details	114
C.1	Firmware Update Override.....	114
C.2	Flash Descriptor Override Pin Strap Ignore.....	114
C.3	Si features parameters.....	115
C.4	Features Supported	115
C.5	Setup and Configuration.....	120
	Appendix D – Desktop CRB Information.....	121
D.6	Manufacturing Mode Jumper	121
D.7	CMOS Clear Jumper.....	122
	Appendix E – Mobile CRB Information.....	123
E.1	Redfort G3 Support	123
E.2	Redfort Virtual AC / DC Operation.....	123



E.3	Redfort Virtual AC / DC Operation.....	124
Appendix F – Basic Bring-up steps		126
F.4	Basic Intel® AMT Bring-up steps	126

Figures

Figure 1-1. Clock Initialization Process (Simplified)	9
Figure 1-2. Thermal Reporting	10
Figure 3-1. Snapshot of executing the Intel® QST Windows Configuration Tool.....	22
Figure 7-1. Ibex Peak Buffer Through Mode Architecture.....	96
Figure 7-2. Configuration “A” — Desktop/Server/Workstation or Mobile.....	112
Figure 7-3. Configuration “B” — Mobile Only	112
Figure 7-4. Configuration “C” — Desktop/Server/Workstation Only	113
Figure 7-5. Configuration “D” — Mobile Only	113
Figure 7-6. Desktop CRB Manufacturing Mode Jumper Location.....	121
Figure 7-7. Desktop CRB CMOS Clear Location	122
Figure 7-8. Redfort CRB G3 Support	123
Figure 7-9. Redfort CRB Virtual Battery Jumper	123
Figure 7-10. Redfort ME WLAN Power Control Jumper settings	124
Figure 7-11. Basic Intel® AMT testing steps	126

Tables

Table 1-1. Number Format Notation.....	15
Table 1-2. Data Format Notation	15
Table 4-1. Kit Dashboard	23
Table 5-1. High Impact Clock Control Parameters	69
Table 7-1. Enabling Intel® Identity Protection (Sentry Peak)	93
Table 7-2. SSC Blocks.....	97
Table 7-3. Clock Dividers	97
Table 7-4. Flex Clock Source Select Parameters.....	98
Table 7-5. Output Clock Enable Parameters	99
Table 7-6. Input Buffer Enable Parameters.....	101
Table 7-7. Power Management Parameters	102
Table 7-8. Power Management Parameters	103
Table 7-9. Single Ended Buffer Parameters	103
Table 7-10. Single Ended Buffer Parameters	105
Table 7-11. SRC Power Management.....	107
Table 7-12. SRC Power Management.....	110
Table 7-13. Firmware Override Update Variables	114
Table 7-14. Si Features Options	115
Table 7-15. Feature default settings by SKU.....	116



Revision History

Revision Number	Description	Date
0.1	Initial Full SKU release	December 2008
0.2	<ul style="list-style-type: none">Updated FITc screen captures to reflect interface name changes.Added PCH B0 Bring Up section.Added Clock configuration information.	January 2009
0.3	<ul style="list-style-type: none">Updated QST section INI naming.Fixed start of B0 Bring-up section which was referencing to A0 / A1.	January 2009
0.4	<ul style="list-style-type: none">Updated the Fast Read Frequency to 50MhzAdded in the preliminary Configuration Tab section setting information.	February 2009
0.5	<ul style="list-style-type: none">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 CAdded new Flash Configuration section in Appendix B	February 2009
0.6	<ul style="list-style-type: none">Added new Kit Dashboard Table 3-1Added additional information to the Configuration Parameters section outlining proper Desktop / Mobile WLAN Power Well Config settings	February 2009
0.61	<ul style="list-style-type: none">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	<ul style="list-style-type: none">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	<ul style="list-style-type: none">Updated Kit Contents section with for Engineering Release	March 2009
0.64	<ul style="list-style-type: none">Removed A0 / A1 Bring-up section informationUpdated Braidwood section.Added Appendix E with Redfort Mobile CRB information on G3 and Virtual Battery options.	March 2009
0.65	<ul style="list-style-type: none">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



Introduction

Revision Number	Description	Date
0.66	<ul style="list-style-type: none">Updated Clock Control information and moved High Impact Clock sectionAdded Intel® RPAT section informationAdded additional information on CPU settings for the Mobile platform and updated the Virtual Battery section for better clarity.	April 2009
0.67	<ul style="list-style-type: none">Updated Strap 9 PCIe Port Configuration 2 section information for Desktop versus Mobile CRB configuration.Updated default XML file informationRemoved Intel® AT-d section informationRemoved the Mobile CRB CPU setting section.	April 2009
0.68	<ul style="list-style-type: none">Updated CCG and MPG BIOS version numbers in the Kit Contents sections for Alpha1 ReleaseUpdated Braidwood section.	April 2009
0.69	<ul style="list-style-type: none">Updated M3 Power Rail Availability option	April 2009
0.70	<ul style="list-style-type: none">Updated Kit Contents section	May 2009
0.71	<ul style="list-style-type: none">Added SKU Manager and Updated Feature Enable / Disable changes.	May 2009
0.72	<ul style="list-style-type: none">Removed DOS4GW.exe reference from Intel® QST section. It is not required for Ibex Peak	May 2009
0.73	<ul style="list-style-type: none">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	<ul style="list-style-type: none">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 RPAT section information	May 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

Introduction

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.

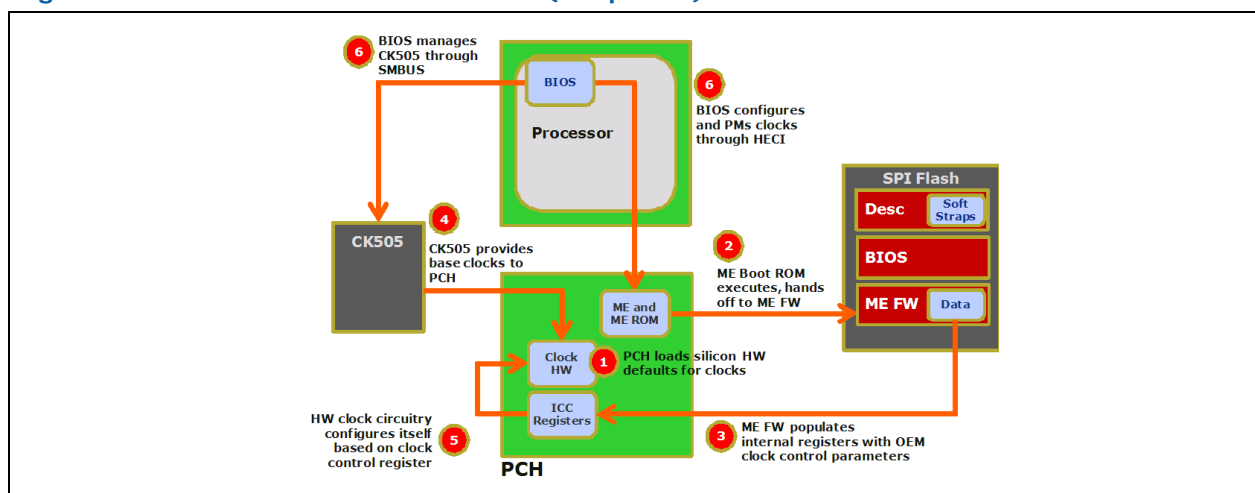
VIP: 16955 - Intel® 82578 Gigabit Ethernet Controller (Hanksville-D SVK) - Beta1 Update - TIC 180643 and checks required to ensure that this boot process is successful, and that Intel® ME Firmware is operating as expected.

1.3 Intel® ME Firmware Features

This firmware release includes the following applications:

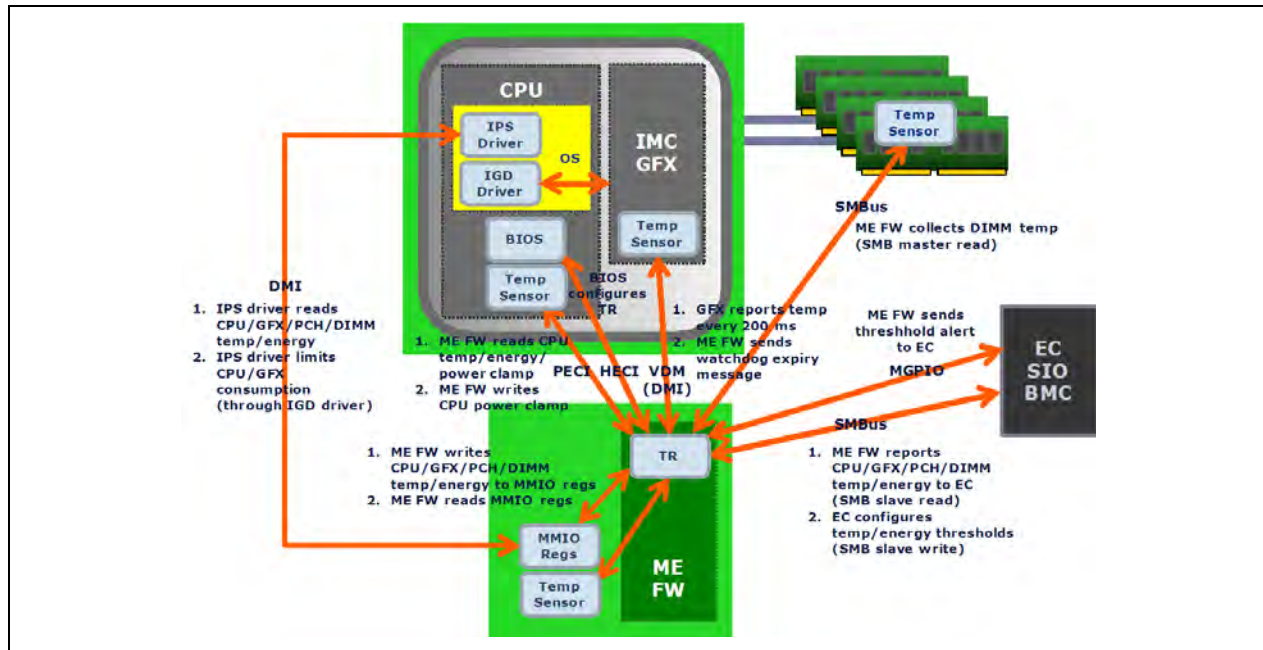
- Platform Clocks – Tune Ibex Peak clock silicon to the parameters of a specific board, configure clocks at run time, power manage clocks.
- Benefit:** Allows extensive customizability and soft control of “first generation” clock solution and makes clocks available before CPU powers up.

Figure 1-1. Clock Initialization Process (Simplified)



- 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



- Thermal Reporting – ME Firmware reports thermal and power information available only on PECC 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 PECC-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.



Introduction

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. Contains Intel® AT-d (previously known as Danbury) and 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	<p>The person who uses the computer (either Desktop or Mobile). In corporate, the user usually does not have an administrator privileges.</p> <p>The end user may not be aware to the fact that the platform is managed by Intel® AMT.</p>
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.



Introduction

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: <ul style="list-style-type: none">• OS is hung• After PCI reset• OS watch dog expires• OS is not present
SP	Sentry Peak
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.



Introduction

Acronym or Term	Definition
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*
<i>RS – Piketon/Kings Creek and Foxhollow – Platform Design Guide</i>	IBL 376563
<i>RS – Calpella – Platform Design Guide</i>	IBL 398905
<i>Calpella – ME-EC Specification</i>	IBL 394791
<i>Calpella – PCH-EC SMBus Protocol Specification</i>	IBL 390730
<i>RS – Piketon/Kings Creek and Foxhollow – BIOS Writer's Guide</i>	*
<i>Ibex Peak Platform Clocks – Debug and Test Guide</i>	*
<i>Ibex Peak Platform Clocks and Intel® Management Engine – Co-validation Guide</i>	*
<i>Ibex Peak Platform Intel® Management Engine – Hardware Debug and Test Guide</i>	*



Introduction

* 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
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 Braidwood Technology

- This section is only applicable if Braidwood Technology is to be configured on the target platform. If not, please skip this section and continue with the next section.
- This section describes the soft straps that need to be set to enable Braidwood Technology.
- Please note that if hardware, BIOS or Intel® ME FW loaded on the platform does not support Braidwood then Braidwood Technology cannot be enabled.
- **Braidwood SSD functionality is not currently supported and is disabled by default.**

Braidwood platform consists of following hardware components: Integrated physical NAND controller, Intel Fast Flash NAND module and ONFI 2.0 connector. NAND module can be motherboard down (soldered) or connector-based (ONFI 2.0 defined). Please follow the Braidwood FW bringup process to insert NAND module in the system. Integrated physical NAND controller is exposed via AHCI Port 6 (SSD) and via AHCI Port 7 (NVMe). The integrated physical NAND controller is accessible only by Braidwood FW.

BIOS must provide the required support for Braidwood. The requirements for Braidwood FW and BIOS communication must be implemented in BIOS before enabling Braidwood. Please refer to the latest Virtualization Engine (VE) BIOS Writers Guide for detailed BIOS requirements. Please contact your Intel Field Applications Engineer for the latest VE BIOS Writers Guide.

2.1 Braidwood Firmware Bringup Process

Note: If the NAND module has been used with another version of Braidwood FW and you plan to change the Braidwood FW, perform the whole NAND erase using the following command, remove the NAND module from the platform and then proceed with the bring up process. The NANDUtil tool and Braidwood firmware used must be from the same Intel® ME kit. (See section 2.2.1 for more details on NANDUtil tool).

NANDUtil.exe –erase –total

The Braidwood FW bring-up process involves the following steps:

1. Braidwood FW (NAND FW) is part of the Intel® ME FW image if the given ME SKU supports Braidwood. The Intel® ME firmware image should be integrated with the GbE and BIOS images using the Flash Image Tool to create the final flash image and set the correct soft straps. (See Section 4 – Quick Start and Kit Contents)

Note: To enable caching functionality using Intel® Rapid Storage Technology 9.5 driver in OS environment, the BIOS image must contain the



Braidwood Technology

Intel® RST 9.5 RAID OROM. The RAID OROM can be download from latest Intel® RST 9.5 kit.

- a. To enable Braidwood, the following soft-straps must be set:
 - i. In Flash Image Tool, select 'Configuration' tab and then select 'Features Supported' option in left pane. Then check the value of 'Braidwood Technology Permanently Disabled?' parameter. The parameter value must be set to 'No' to enable Braidwood Technology.
 1. PCH Strap 14 parameter 'VE Enabled' must be set to 'true' to enabled VE. The above Configuration tab settings will also set this soft strap to 'true' for Braidwood Technology support.
 - ii. Other PCH Strap 14 Settings
 - The PCH Strap 14 settings can be done by using following parameters in Flash Image Tool.
 - To enable NVMHCI support, PCH Strap 14 parameter 'Braidwood Technology NVMHCI Enabled' must be set to 'true'.
 - Since SSD functionality is not currently supported, PCH Strap 14 parameter 'Braidwood Technology SSD Enabled' settings is ignored by Braidwood firmware.
 - PCH Strap 14 parameter 'VE Boot From Flash' must be set to 'false'. This soft strap is set to 'false' by default and it cannot be changed.

Note: For more detailed information on all Soft Strap parameters, please refer to the '**PCH_SPI_Programming_Guide**' available in this ME kit.

2. Braidwood does not have any special ME image flashing requirements. Current methods of flashing ME image such as Flash Programming Tool or Flash Burner/Programmer should be used. (See Section 4 – Quick Start and Kit Contents)
3. Power off the platform by removing power, wait for approximately 10 seconds and then boot the platform.
4. Enter to BIOS Setup and follow the steps below:
 - a. For CCG BIOS: Go to Chipset->VE Subsystem and set VE Subsystem option to Enable.

OR

For MPG BIOS: Go to Chipset->South Bridge Configuration -> Ibexpeak options and set VECI device to Enabled.

 - b. For CCG BIOS: Go to Advanced->SATA Configuration (**or** for MPG BIOS: Chipset->South Bridge Configuration->SATA Configuration) and set the correct SATA mode using following requirement:
 - i. SATA mode must be set to RAID to enable NVMHCI (cache) functionality. NVMHCI functionality cannot be enabled in IDE or AHCI mode.
 - c. For MPG BIOS only: Go to Chipset -> South Bridge Configuration -> Ibexpeak options and set the option "Set NAND Management Override" to Disabled.
 - d. Save changes, power off the platform by removing power.
5. Insert NAND module in ONFI connector on the platform and boot the platform.



Note: If you need to flash BIOS image after this step, the NAND module must be removed from the platform before flashing BIOS image. After flashing the BIOS image, go to step 3. If BIOS image is flashed without removing NAND module, it may result in NAND module corruption and the NAND module recovery may not be possible.

6. When correct soft-straps are set and final image is programmed on SPI, the system shall be ready to initialize and configure the NAND module.

2.2 NAND Configuration

NAND module must be configured before it can be used by the host. NAND module configuration involves creation of NVMHCI (cache) region. NANDUtil tool can be used to configure the NAND module.

Please note that Braidwood caching functionality cannot be exercised without NVMHCI-compliant storage driver such as Intel® Rapid Storage Technology 9.5 driver.

2.2.1 NANDUtil Tool

NANDUtil.exe will run on MS DOS version 6.22 and above. The NANDUtil tool can be accessed under the following directory:

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

Note: The NANDUtil tool and Braidwood firmware used must be from the same Intel® ME kit.

NANDUtil tool query command can be used for fetching the details of NAND from Braidwood FW as shown below:

1. Copy NANDUtil.exe from “Braidwood Tools” directory to the root directory of a bootable USB drive.
2. Boot the target system to DOS, change directory to the root directory of the bootable USB drive.
3. Braidwood FW may take several seconds after system power on to initialize the NAND module. It is recommended to use NANDUtil tool “query” command first and check that it executes successfully with no error codes returned. Type the following command at command prompt:

```
NANDUtil.exe -query
```

In case of an error, perform the whole NAND erase using the following command, power off the target system by removing power after successful completion of erase command, wait for approximately 10 seconds and go to step 2:

4. NANDUtil.exe -erase -totalUse the NANDUtil tool “create” command to create NVMHCI region by typing the following command at the DOS prompt:

```
NANDUtil.exe -create nvmmhci -percents 100
```



Braidwood Technology

Please refer to the **Braidwood Tools User Guide** available in the following directory for more details on NANDUtil tool functionality and NVMHCI region creation procedure:

- “Unzipped_folder” Tools\Braidwood Tools\
 5. Power down the system, wait for approximately 10 seconds and then boot the target system to DOS.
 6. Type the following command at command prompt to check the NVMHCI region:

```
NANDUtil.exe -query
```

7. When NVMHCI region creation completes successfully, power down the system and then boot the system using disk or volume with Windows OS installed in RAID mode.

Please refer to the latest Intel® RST kit on VIP for instructions to install Intel RST driver in and to enable caching functionality in Windows environment.

§



3 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.

3.1 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

3.2 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](#)).

3.2.1 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>]



Intel® QST Image Generation

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.

3.2.2 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 3-1. Snapshot of executing the Intel® QST Windows Configuration Tool

```
C:\WINDOWS\system32\cmd.exe

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)

§



4 Quick Start and Kit Contents

Table 4-1. 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	<input type="checkbox"/> Uses Ignition Firmware core (no UMA) <input checked="" type="checkbox"/> Uses Full Firmware core (uses UMA)	
Supported Manageability Power States	<input checked="" type="checkbox"/> S0/M0 <input checked="" type="checkbox"/> S3/M3 <input checked="" type="checkbox"/> S4/M3	<input checked="" type="checkbox"/> S5/M3 <input checked="" type="checkbox"/> Sx/Moff
Supported processors	Desktop (Quad Core) <input checked="" type="checkbox"/> Lynnfield LGA1156 ES2 (A2, Q2AL/Q2AP) Desktop (Dual Core) <input checked="" type="checkbox"/> Havendale LGA1156 ES1 (B0, Q2BK)	Mobile (Quad Core) <input checked="" type="checkbox"/> Clarksfield ES2 (A2, Qxxx) Mobile (Dual Core) <input checked="" type="checkbox"/> Auburndale ES1 (B0, Q2CZ)
Supported PCHs	Desktop <input checked="" type="checkbox"/> Ibex Peak ES3 (B1, QLLS)	Mobile/SFF <input checked="" type="checkbox"/> Ibex Peak ES3 (B1, Qxxx)
Supported Intel LAN PHYs	Desktop <input checked="" type="checkbox"/> 82578DM (Hanksville-D) ES1/ES2 (C0 , QLMJ)	Mobile <input checked="" type="checkbox"/> 82577LM (Hanksville-M) ES1/ES2 (A2, QLDT)
Tools	<input checked="" type="checkbox"/> Flash Image Tool (FIT, FITW) <input checked="" type="checkbox"/> Flash Programming Tool (FPT, FPTW) <input checked="" type="checkbox"/> MEInfo <input checked="" type="checkbox"/> AMTConfiguration <input checked="" type="checkbox"/> QST Tools	<input checked="" type="checkbox"/> MEManuf <input checked="" type="checkbox"/> UpdParam <input checked="" type="checkbox"/> Braidwood (NANDUtil) <input checked="" type="checkbox"/> FSTDOS











4.1 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 4.2, page 24)
2. Create SPI flash binary image using Flash Image Tool (5.2, page 32)
3. Program the SPI binary image into the target platform's SPI device(s) using Flash Image Tool, or a flash programmer (see Section 5.4, page 72), 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*).

4.2 Kit Contents

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

	Directory	
	File	
	Sub-directory	
	File	
	File	
	Sub-directory	
	File	
	File	

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:



Quick Start and Kit Contents

<i>(root)</i>	Location of extracted archive contents.
<i>FW Bring Up Guide.pdf</i>	This document.
<i>403598_PCH_SPI_Programming_Guide_Rev1_1.pdf</i>	How to program SPI device parameters, VSCC tables, descriptor region details. This document's contents are integrated with the Firmware Bring Up Guide.
<i>Intel(R)AMT_6_0_OEM_WebUI_Guide_rev0_3.pdf</i>	WebUI OEM Users guide.
<i>Drivers</i>	MEI / LMS_SOL Drivers
<i>MEI_SOLInstaller</i>	
<i>Drivers</i>	
<i>MEI</i>	
<i>heci.cat</i>	
<i>HECI.inf</i>	
<i>HECI.sys</i>	
<i>HECIx64.sys</i>	
<i>SOL</i>	
<i>mesrl.cat</i>	
<i>mesrl.inf</i>	
<i>mesrle.cat</i>	
<i>mesrle.inf</i>	
<i>IMSS</i>	
<i>AMT_COM_InterfaceLib.dll</i>	
<i>AMT_SW_GUI.dll</i>	
<i>PrivacyIconClient.exe</i>	
<i>PrivacyIconClient.exe.config</i>	
<i>readme.txt</i>	
<i>Intel Control Center</i>	
<i>SetupICC.exe</i>	
<i>Lang</i>	MEI / LMS_SOL Setup Localized Languages.
<i>LMS</i>	
<i>LMS.exe</i>	
<i>NTService_license.txt</i>	



Quick Start and Kit Contents

MEWMIProv_REL	
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	



Quick Start and Kit Contents

MEcp64.exe	
NVM Image	
BIOS	
CGIBX142.rom - Piketon – Desktop CRB BIOS MPG058.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	
82578 GbE NVM Readme.doc 82578_C0_VEROPT62_DSK.bin – Desktop GbE firmware 82577 GbE NVM Readme.doc 82577_A3_LAN_SWITCH_VEROPT61_MBL.bin – Mobile Gbe firmware 82577_A3_NON_LAN_SWITCH_VEROPT63_MBL.bin – Mobile Gbe firmware	Intel LAN PHY firmware binary. Use with desktop, server, or workstation Ibex Peak based platforms.
ME_BIOS_Extension	
mebx_launch_6.0.3.0003.bin	
mebx_main_6.0.3.0003.bin	
Tools	
AMT Tools	Refer to the Intel(R) AMT Tools User Guide.pdf for further details on the tools / usage in this folder.
Intel(R) AMT Tools User Guide.pdf	
AMTConfiguration	
ConfigurationServer.exe	
gSOAP_license.txt	



Quick Start and Kit Contents

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	
getcfig.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	
Braidwood Tools	Refer to the Braidwood_Tools_User_Guide.pdf for further details on the tools /usage in this folder.
NANDUtil.exe	



Quick Start and Kit Contents

Braidwood Tools User Guide.pdf	
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	



Quick Start and Kit Contents

Flash Image Tool		Refer to the System Tools User Guide.pdf for further details on the tools / usage in this folder.
	<i>fitc.exe</i>	
	<i>vsccommn.bin</i>	
	<i>fitc.ini</i>	
	<i>fitctmpl.xml</i>	
	<i>newfiletmpl.xml</i>	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.
	<i>License.rtf</i>	
	<i>DOS</i>	
	<i>fparts.txt</i>	Database of supported SPI flash devices.
	<i>fpt.exe</i>	Flash Programming Tool binary for DOS.
	<i>fptcfg.ini</i>	
	<i>vsccommn.bin</i>	
	<i>Windows</i>	
	<i>fparts.txt</i>	Database of supported SPI flash devices.
	<i>fptcfg.ini</i>	
	<i>fptw.exe</i>	Flash Programming Tool binary for 32-bit Windows operating systems.
	<i>sseidrvdli32e.DLL</i>	
	<i>ssepmxdli32e.DLL</i>	
	<i>ssepmxdrv.SYS</i>	
	<i>vsccommn.bin</i>	
FWUpdate		Refer to the System Tools User Guide.pdf for further details on the tools / usage in this folder.
	<i>Local-DOS</i>	
	<i>FWUpdLcl.exe</i>	
	<i>Local-Win</i>	
	<i>FWUpdLcl.exe</i>	
	<i>gSOAP_license.txt</i>	



Quick Start and Kit Contents

	<i>xerces-c_2_7.dll</i>	
MEInfo		Refer to the System Tools User Guide.pdf for further details on the tools / usage in this folder.
DOS		
	<i>MEInfo.exe</i>	
Windows		
	<i>MEInfoWin.exe</i>	
	<i>sseIdrv.dll32e.dll</i>	
	<i>ssePmxdll32e.dll</i>	
	<i>ssepmdrv.sys</i>	
MEManuf		Refer to the System Tools User Guide.pdf for further details on the tools / usage in this folder.
DOS		
	<i>AUTOEXEC.BAT</i>	
	<i>MEManuf.exe</i>	
	<i>vsccommn.bin</i>	
Windows		
	<i>MEManufWin.exe</i>	
	<i>sseIdrv.dll32e.dll</i>	
	<i>ssePmxdll32e.dll</i>	
	<i>ssepmdrv.sys</i>	
	<i>vsccommn.bin</i>	
UpdParam		Refer to the System Tools User Guide.pdf for further details on the tools / usage in this folder.
	<i>UpdParam.exe</i>	



5 Bring Up Process — All Platforms

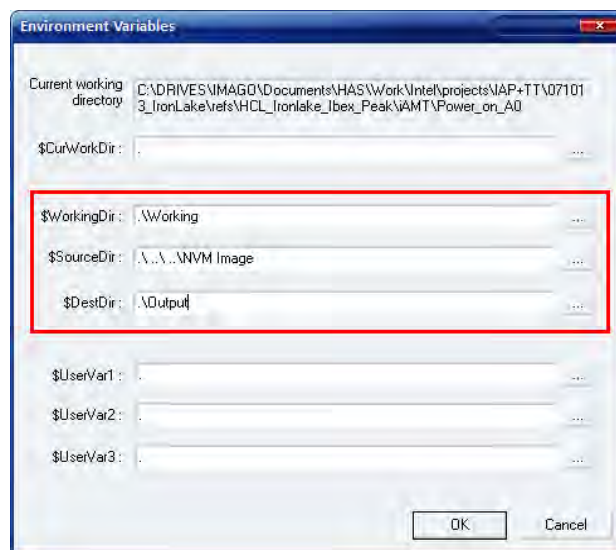
5.1 Bring Up Process

5.2 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.

5.2.1 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 4.2, page 24). 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.



Bring Up Process — All Platforms

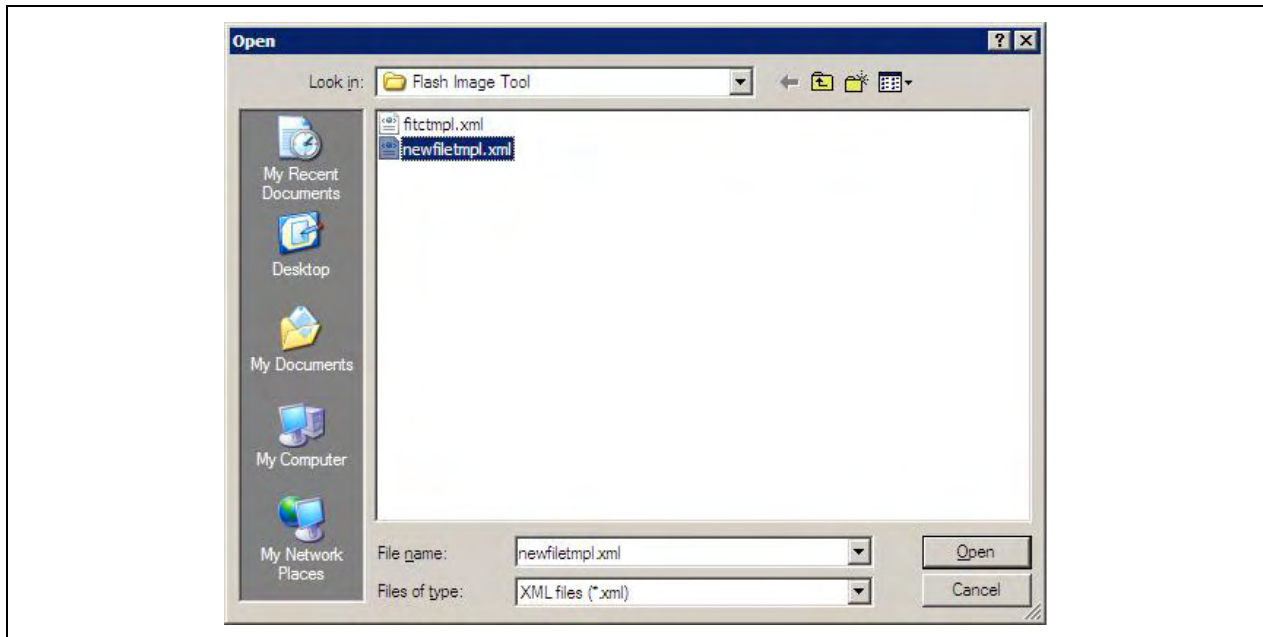
3. In the main menu select **Build | Build Settings....** Leave the defaults for **Output Path**, **Generate intermediate build files**, and **Build compact image** as shown. Change the **Flash Block/Sector Erase Size** as appropriate for your SPI flash part(s).





5.2.2 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**.



5.2.3 FITc Selection for CRB

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



5.2.4 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
	GbE LAN region length	0h	
	Binary input file		Navigate to your Source Directory (as specified in Section 5.2.2, page 34) 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.



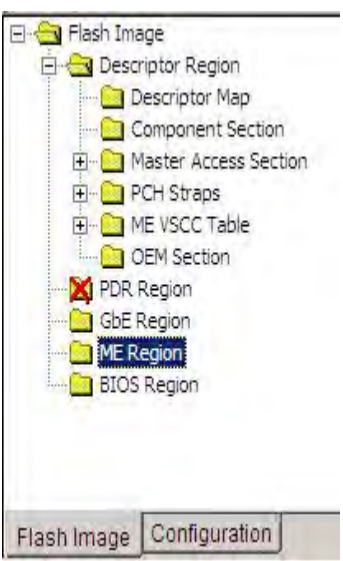
5.2.5 Set Up Intel® ME Firmware Region

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
	Binary input file		Navigate to your Source Directory (as specified in Section 5.2.2, page 34) 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 49).
	Intel® QST config file		Enable QST navigate to the directory location where the qstbinary.bin file was created (as shown in Section 3) 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.



Bring Up Process — All Platforms

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.



5.2.6 Selecting Platform SKU

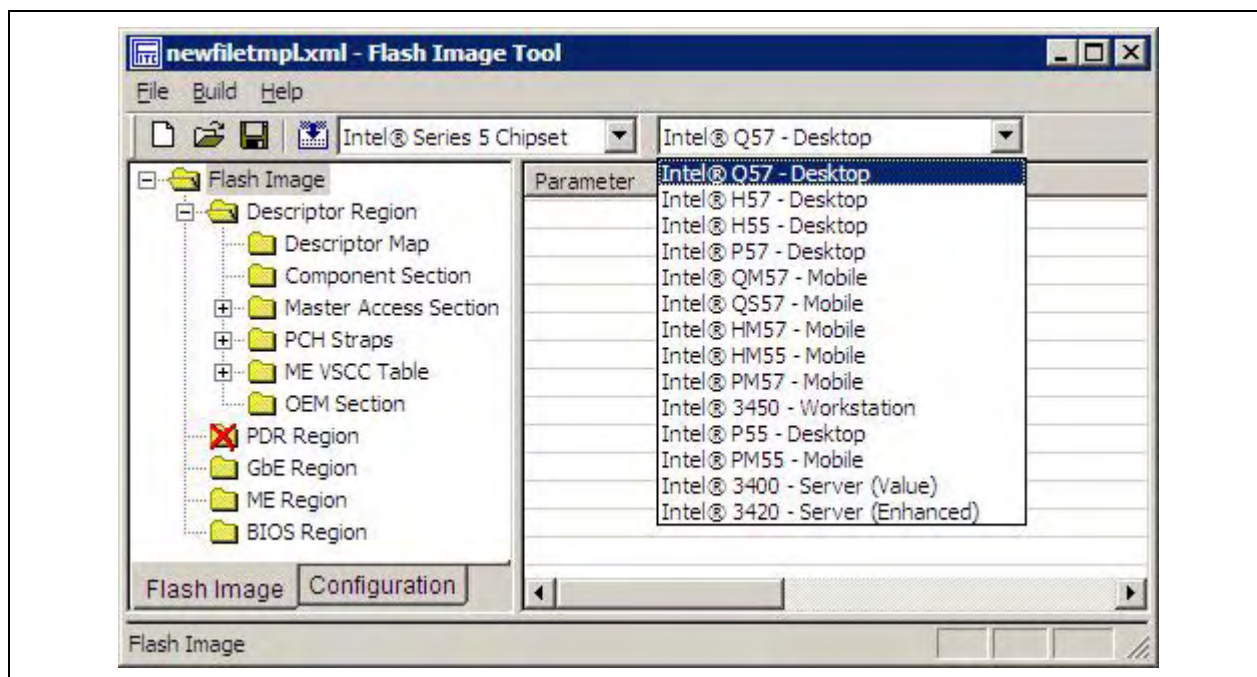
Note: Selecting the Platform SKU needs to be done after the ME region has been loaded to ensure that the proper firmware settings are loaded into FITc.

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, PM57, HM57 and HM55.



Bring Up Process — All Platforms

5.2.7 Set Up BIOS Region

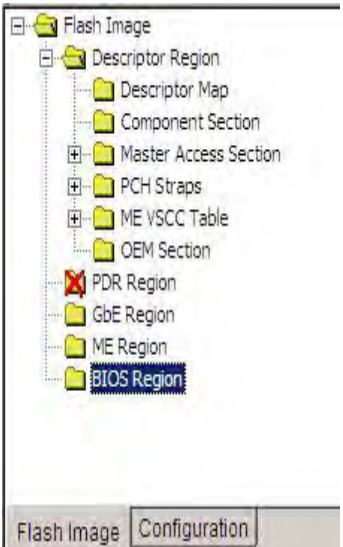
All parameters in this section are color-coded as per the key below.

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 5.2.2, page 34) and switch to the BIOS subdirectory. Choose the desktop or mobile BIOS binary image. See Section 4 page 23. For all other platforms point this parameter to the appropriate BIOS image.



5.2.8 Set Up Descriptor and SPI Flash Device(s)

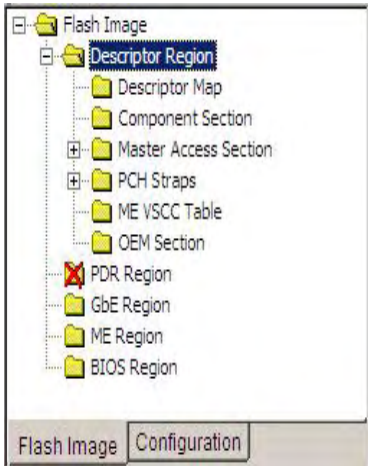
All parameters in this section are color-coded as per the key below.

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.

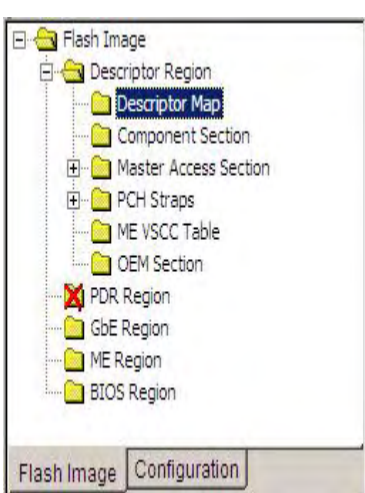
1. On the navigation tree to the left, select the **Flash Image** tab. Select **Flash Image | Descriptor Region**. Set the parameters in the **Descriptor Region** section as shown in the table below.

Location	Parameter	Default	Comments
	Descriptor region length	0h	Leave this at zero. Allows FIT to auto-size the descriptor region length.

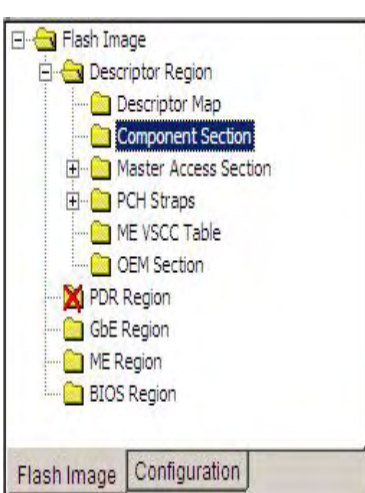


Bring Up Process — All Platforms

- 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
	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	

- 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
	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	



Bring Up Process — All Platforms

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 .

- 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
	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.



Bring Up Process — All Platforms

- 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
	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.

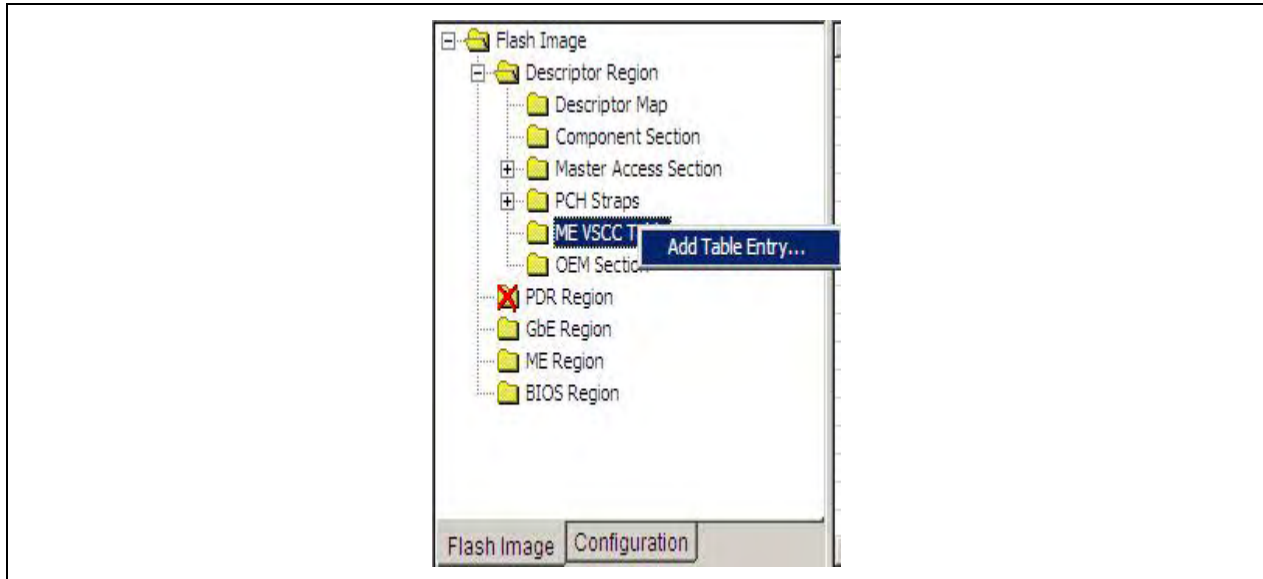
- On the navigation tree to the left, select the **Flash Image** tab. Select **Flash Image | Descriptor Region | Master Access Section | GbE LAN**. Set the parameters in the **GbE LAN** section as shown in the table below.

Location	Parameter	Default	Comments
	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.



Bring Up Process — All Platforms

- 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**.



- 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.

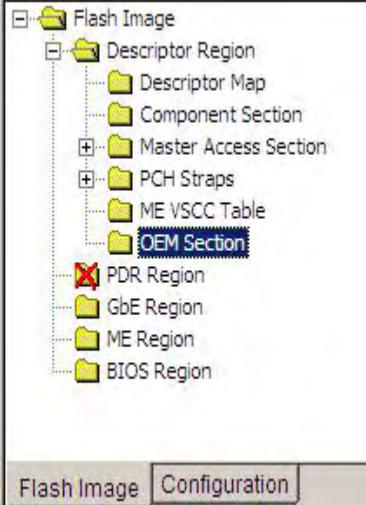
Note: These VSCC Table setting are specifically for the Desktop and Mobile CRB platforms. Refer to the manufacturer specifications for your SPI flash part for proper setting information.

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 .



Bring Up Process — All Platforms

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
	Binary input file		



5.2.9 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.

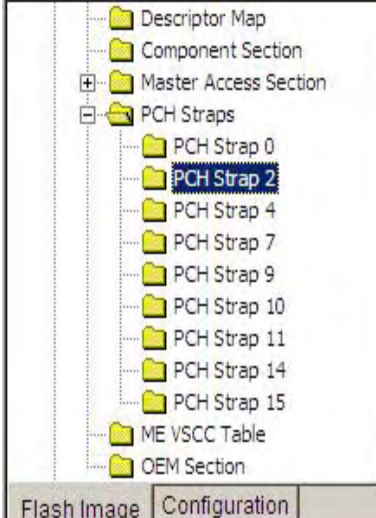
1. On the navigation tree to the left, select the **Flash Image** tab. Select **Flash Image | Descriptor Region | PCH Straps | PCH Strap 0**. Set the parameters in the **PCH Strap 0** section as shown in the table below.

Location	Parameter	Default	Comments
	BIOS Boot Block Size	64KB	Sets BIOS Boot Block Size
	Intel® Anti-Theft Technology Data Protection Disable	false	true = DT is disabled. false = DT is enabled. Does not override DT disable by hard strap (PCH GPIOxx), fuse, or SATA disable.
	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

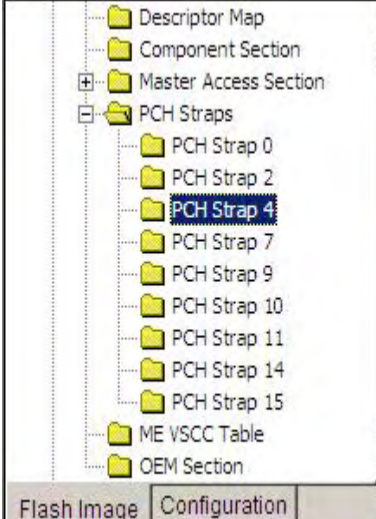


Bring Up Process — All Platforms

- 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.

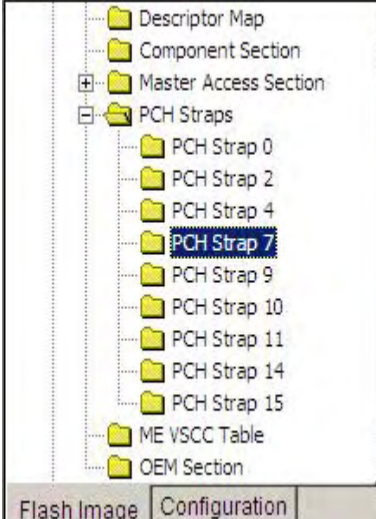
- On the navigation tree to the left, select the **Flash Image** tab. Select **Flash Image | Descriptor Region | PCH Straps | PCH Strap 4**. Set the parameters in the **PCH Strap 4** section as shown in the table below.

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.

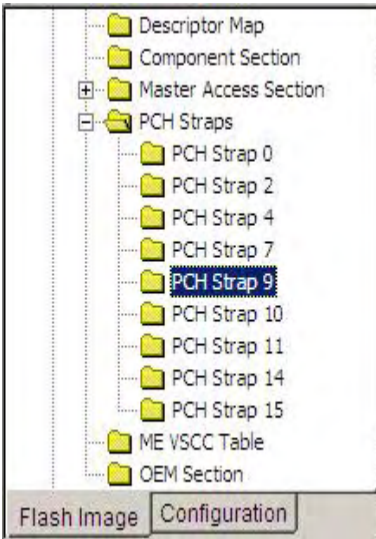


Bring Up Process — All Platforms

- 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
	Intel® ME SMBus Subsystem Vendor & Device ID for ASF2	0	Intel® ME SMBus Subsystem Vendor & Device ID for ASF2

- 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.

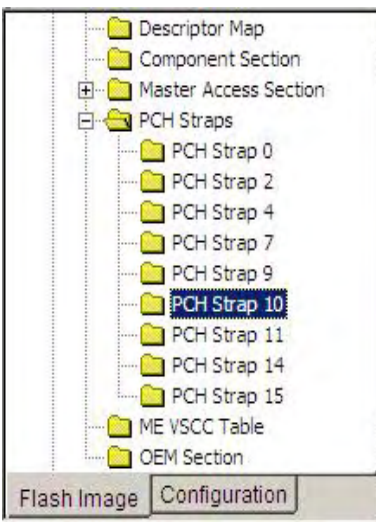
Location	Parameter	Default	Comments
	Intel® PHY Over PCI Express Enable (PHY_PCIE_EN)	true	true = Intel LAN is present false = Third-party LAN is present
	Intel® PHY PCIe Port Select (PHY_PCIEPORSEL)	101:Port 6	Only necessary if Intel LAN is present. 000 = Port 1 001 = Port 2 010 = Port 3 011 = Port 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.
	PCIe Lane Reversal 2	false	This parameter must reflect platform topology.
	PCIe Lane Reversal 1	false	This parameter must reflect platform topology.



Bring Up Process — All Platforms

Location	Parameter	Default	Comments
	PCIe Port Configuration 2	00: 4x1 Ports 5-8 (x1)	<p>Desktop CRB values - 00: 4x1 Ports 5-8 (x1)</p> <p>Mobile CRB values - 10: 2x2 Port 5 (x2), Port 7 (x2), Ports 6, 8 (disabled).</p> <p>This parameter must reflect platform topology.</p>
	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
	ME boot from flash	false	This option is read-only until an Intel ME Firmware binary image is loaded. See Section 5.2.5
	ME MDDD Enable	false	<p>true = Enable MDDD logging</p> <p>false = Disable MDDD logging</p>
	ME MDDD Address	0x00	<p>MDDD Address</p> <p>Set this to a value of '0x38' for MDDD logging.</p>
	ICC OEM Config Select	0	<p>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.</p> <p>SPI flash binary images across multiple board designs are expected to contain the same block of clock control parameters, up to 8 sets total.</p>



Bring Up Process — All Platforms

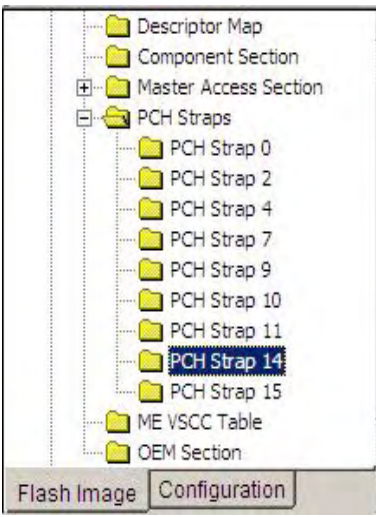
- On the navigation tree to the left, select the **Flash Image** tab. Select **Flash Image | Descriptor Region | PCH Straps | PCH Strap 11**. Set the parameters in the **PCH Strap 11** section as shown in the table below.

Location	Parameter	Default	Comments
	SMLink1 I2C Address Enable	true	<i>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.</i> 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	<i>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.</i> 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.



Bring Up Process — All Platforms

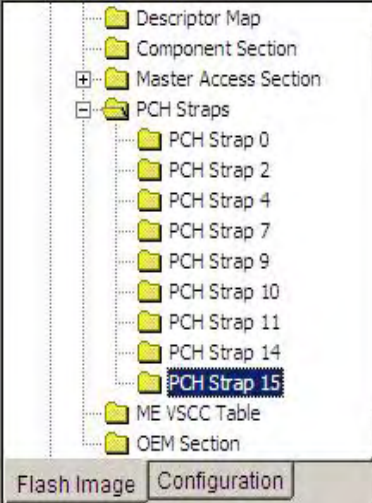
- On the navigation tree to the left, select the **Flash Image** tab. Select **Flash Image | Descriptor Region | PCH Straps | PCH Strap 14**. Set the parameters in the **PCH Strap 14** section as shown in the table below.

Location	Parameter	Default	Comments
	VE Enabled	true	<ul style="list-style-type: none"> This option is read-only and automatically be set to 'false' when Braidwood is set to Permanently disabled under Configuration / Feature.
	VE Boot From Flash	false	<ul style="list-style-type: none"> This option is read-only and will determine if VE boots from onboard ROM or the SPI flash.
	Braidwood Technology SSD Enabled	true	<ul style="list-style-type: none"> This option determines if Braidwood support for Solid State Devices (SSD) is enabled. <p>True = Enabled False = Disabled</p> <p>Note: Since SSD functionality is not currently supported, this settings is ignored by Braidwood firmware.</p>
	Braidwood Technology NVMHCI Enabled	true	<ul style="list-style-type: none"> This option determines if Braidwood support for Solid State Devices (NVMHCI) is enabled. <p>True = Enabled False = Disabled</p>



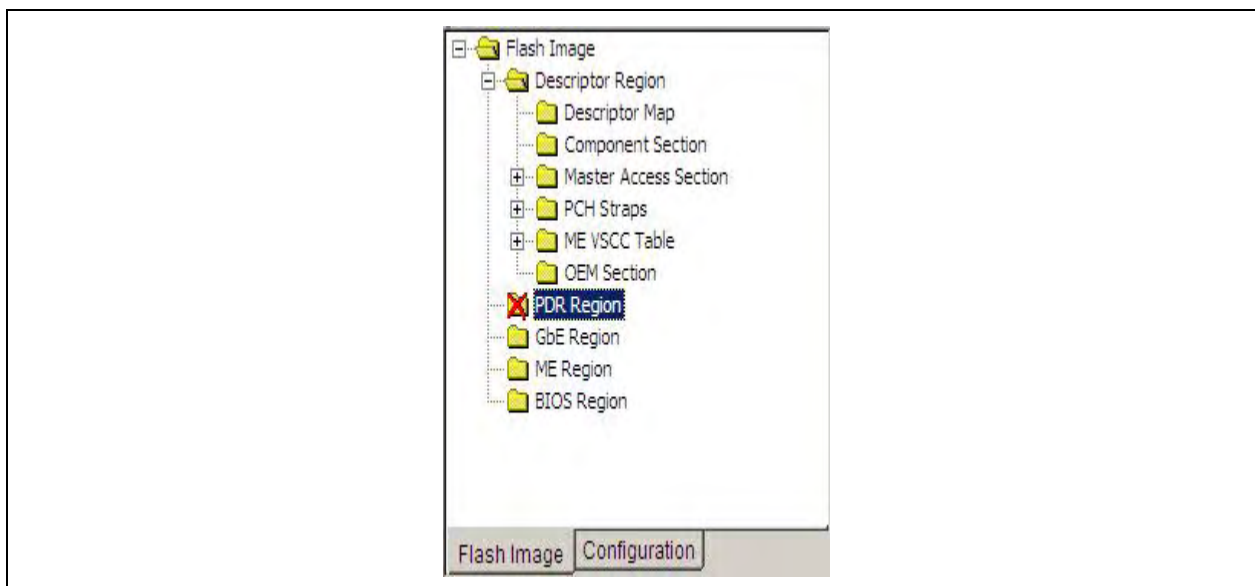
Bring Up Process — All Platforms

9. 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.

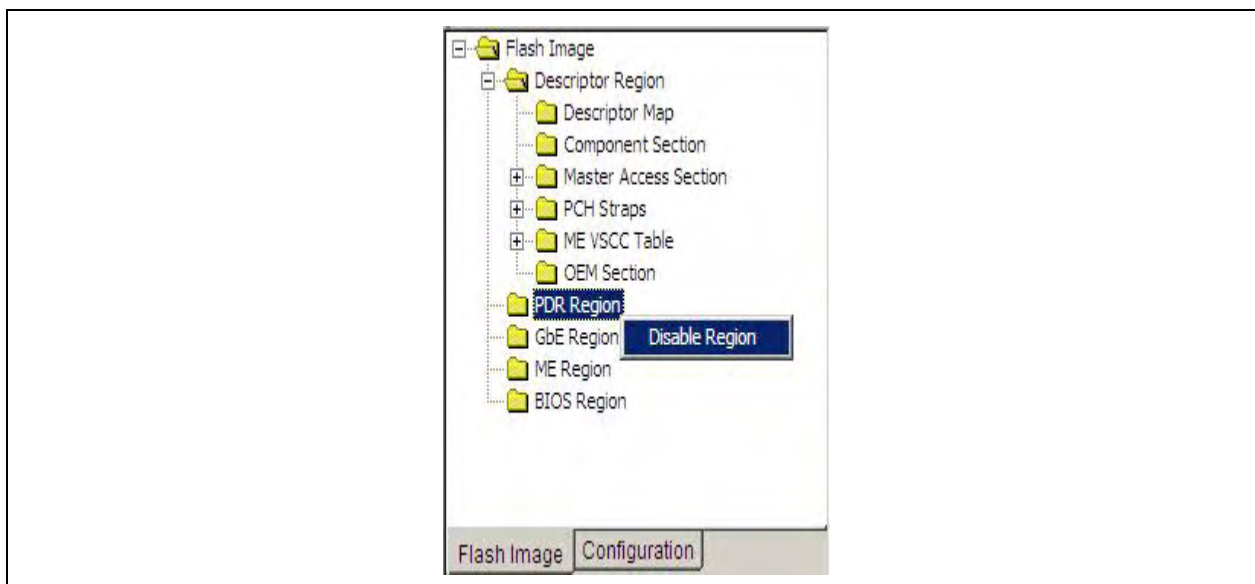
Location	Parameter	Default	Comments
	t209 Timing	1ms	t209 minimum timing value
	Intel® Integrated LAN Enable	true	Enables / Disables the Intel® Integrated LAN.

5.2.10 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.





5.2.11 Configuration Parameters

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

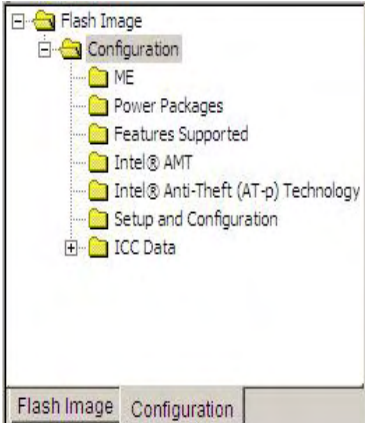
Note: ME region should be loaded before modifying any of the Configuration Parameters. Any Configuration Parameter data modified before the ME Regions is loaded will be lost.

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.

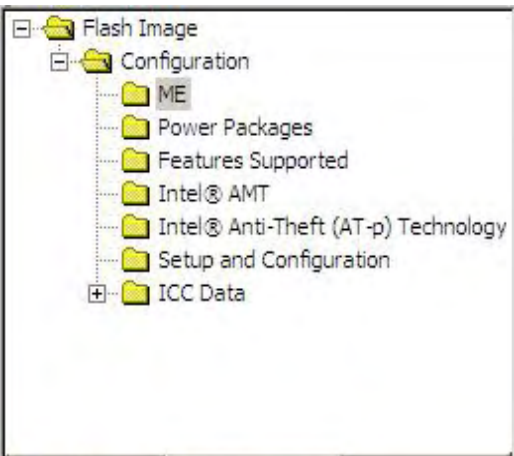
1. On the navigation tree to the left, select the **Configuration** tab. Select **Configuration** as shown below.

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



Bring Up Process — All Platforms

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

Location																													
																													
	Parameter	Default	Comments																										
<table><thead><tr><th>Parameter</th><th>Value</th></tr></thead><tbody><tr><td>Local FWU Override Counter</td><td>1</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>BIOS Reflash Capable</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>Debug Si Features</td><td>0x00000000</td></tr><tr><td>Prod Si Features</td><td>0x00000000</td></tr></tbody></table>	Parameter	Value	Local FWU Override Counter	1	Local FWU Override Qualifier	0	FW Update OEM ID	00000000-0000-0000-0000-000000000000	ME State on Flash Desc OVR	false	BIOS Reflash Capable	false	LAN Power Well Config	3	WLAN Power Well Config	0x80	M3 Power Rails Availability	true	HECI ME Region Unlockable	true	Sub System Vendor ID	0x0000	Debug Si Features	0x00000000	Prod Si Features	0x00000000	Local FWU Override Counter	1	This parameter overrides the MEBx settings for local firmware update. This value is configurable between -1 and 255 . (See Appendix C.1)
	Parameter	Value																											
	Local FWU Override Counter	1																											
	Local FWU Override Qualifier	0																											
	FW Update OEM ID	00000000-0000-0000-0000-000000000000																											
ME State on Flash Desc OVR	false																												
BIOS Reflash Capable	false																												
LAN Power Well Config	3																												
WLAN Power Well Config	0x80																												
M3 Power Rails Availability	true																												
HECI ME Region Unlockable	true																												
Sub System Vendor ID	0x0000																												
Debug Si Features	0x00000000																												
Prod Si Features	0x00000000																												
	Local Firmware Override Qualifier	0	This parameter determines behavior for local firmware updates. (See Appendix C.1)																										
	FW Update OEM ID	00000000-0000-0000-0000-000000000000	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.																										
	ME State on Flash Desc OVR	false	This parameter controls ME behavior for Descriptor Override (GPIO33). (See Appendix C.2)																										
	BIOS Reflash Capable	false																											



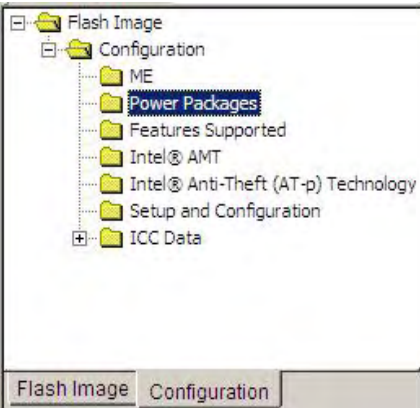
Bring Up Process — All Platforms

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
	Sub System Vendor ID	0x0000	This ID allows OEMs the ability to test boards using Manufacturing Test Permits.
	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)



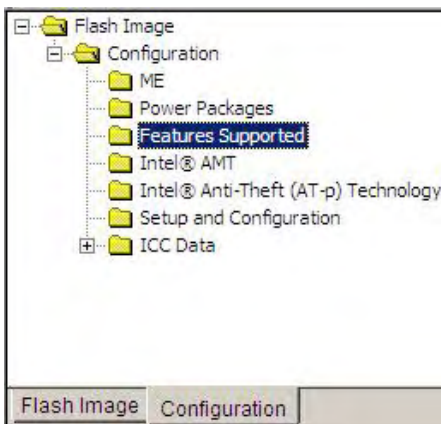
Bring Up Process — All Platforms

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

Location			
	Parameter	Default	Comments
Desktop Power Packages	Power Pkg 1 Supported (Desktop: On in S0)	true	This parameter configures ME for S0 operation only.
	Power Pkg 2 Supported (Desktop: ON in S0, ME Wake in S3, S4-5)	true	This parameter configures ME for operation in S0 and ME Wake in S3, S4 and S5.
	Default Power Package	1	This parameter determines the default Power Package used by firmware image.
Mobile Power Packages	Power Pkg 1 Supported (Mobile: On in S0)	true	This parameter configures ME for S0 operation only.
	Power Pkg 2 Supported (Mobile: On in S0, ME Wake in S3, S4-5 (AC only))	true	This parameter configures ME for operation in S0 and ME Wake in S3, S4 and S5.
	Default Power Package	1	This parameter determines the default Power Package used by firmware image.



- 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																																																												
			<p>These options control the availability / visibility of firmware features.</p> <p>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.</p>																																																												
<table><tr><th>Parameter</th><th>Value</th></tr><tr><td>Enable Intel® Standard Manageability; Disable Intel® AMT</td><td>No</td></tr><tr><td>Manageability Application Permanently Disabled?</td><td>No</td></tr><tr><td>PAVP 1.5 Permanently Disabled?</td><td>No</td></tr><tr><td>Intel® QST Permanently Disabled?</td><td>No</td></tr><tr><td>Intel® Identity Protection Technology Permanently Disabled?</td><td>Yes</td></tr><tr><td>Intel® Remote Wake Technology Permanently Disabled?</td><td>Yes</td></tr><tr><td>KVM Permanently Disabled?</td><td>No</td></tr><tr><td>Braidwood Technology Permanently Disabled?</td><td>No</td></tr><tr><td>TLS Permanently Disabled?</td><td>No</td></tr><tr><td> </td><td> </td></tr><tr><td>Manageability Application Enable/Disable</td><td>Enabled</td></tr><tr><td>PAVP 1.5 Enable/Disable</td><td>Enabled</td></tr><tr><td>Intel® QST Enable/Disable</td><td>Enabled</td></tr><tr><td>Intel® Identity Protection Technology Enable/Disable</td><td>Disabled</td></tr><tr><td>Intel® Remote Wake Technology Enable/Disable</td><td>Disabled</td></tr></table>	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	Braidwood Technology Permanently Disabled?	No	TLS Permanently Disabled?	No			Manageability Application Enable/Disable	Enabled	PAVP 1.5 Enable/Disable	Enabled	Intel® QST Enable/Disable	Enabled	Intel® Identity Protection Technology Enable/Disable	Disabled	Intel® Remote Wake Technology Enable/Disable	Disabled	<table><tr><td>Enable Intel® Standard Manageability; Disable Intel® AMT</td><td>No</td><td rowspan="9"><p>Note: Setting any of these options to 'Yes' will permanently disable that specific feature.</p><p>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</p></td></tr><tr><td>Intel® Manageability Application Permanently Disabled?</td><td>No</td></tr><tr><td>PAVP 1.5 Permanently Disabled?</td><td>No</td></tr><tr><td>Intel® QST Permanently Disabled?</td><td>No</td></tr><tr><td>Sentry Peak Permanently Disabled?</td><td>Yes</td></tr><tr><td>Intel® Remote Wake Technology Permanently Disabled?</td><td>No</td></tr><tr><td>KVM Permanently Disabled?</td><td>No</td></tr><tr><td>Braidwood Technology Permanently Disabled?</td><td>No</td></tr><tr><td>TLS Permanently Disabled?</td><td>No</td></tr><tr><td>Intel® Manageability Application Enable / Disable</td><td>Enabled</td><td rowspan="5"><p>ME Application State – This determines the state that an OEM would ship a specific ME Application</p><p>– 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</p></td></tr><tr><td>PAVP 1.5 Enable / Disable</td><td>Enabled</td></tr><tr><td>Intel® QST Enable / Disable</td><td>Enabled</td></tr><tr><td>Sentry Peak Enable / Disable</td><td>Enabled</td></tr><tr><td>Intel® Remote Wake Technology Enable / Disable</td><td>Enabled</td></tr></table>	Enable Intel® Standard Manageability; Disable Intel® AMT	No	<p>Note: Setting any of these options to 'Yes' will permanently disable that specific feature.</p> <p>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</p>	Intel® Manageability Application Permanently Disabled?	No	PAVP 1.5 Permanently Disabled?	No	Intel® QST Permanently Disabled?	No	Sentry Peak Permanently Disabled?	Yes	Intel® Remote Wake Technology Permanently Disabled?	No	KVM Permanently Disabled?	No	Braidwood Technology Permanently Disabled?	No	TLS Permanently Disabled?	No	Intel® Manageability Application Enable / Disable	Enabled	<p>ME Application State – This determines the state that an OEM would ship a specific ME Application</p> <p>– 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</p>	PAVP 1.5 Enable / Disable	Enabled	Intel® QST Enable / Disable	Enabled	Sentry Peak Enable / Disable	Enabled	Intel® Remote Wake Technology Enable / Disable	Enabled
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																																																														
Braidwood Technology Permanently Disabled?	No																																																														
TLS Permanently Disabled?	No																																																														
Manageability Application Enable/Disable	Enabled																																																														
PAVP 1.5 Enable/Disable	Enabled																																																														
Intel® QST Enable/Disable	Enabled																																																														
Intel® Identity Protection Technology Enable/Disable	Disabled																																																														
Intel® Remote Wake Technology Enable/Disable	Disabled																																																														
Enable Intel® Standard Manageability; Disable Intel® AMT	No	<p>Note: Setting any of these options to 'Yes' will permanently disable that specific feature.</p> <p>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</p>																																																													
Intel® Manageability Application Permanently Disabled?	No																																																														
PAVP 1.5 Permanently Disabled?	No																																																														
Intel® QST Permanently Disabled?	No																																																														
Sentry Peak Permanently Disabled?	Yes																																																														
Intel® Remote Wake Technology Permanently Disabled?	No																																																														
KVM Permanently Disabled?	No																																																														
Braidwood Technology Permanently Disabled?	No																																																														
TLS Permanently Disabled?	No																																																														
Intel® Manageability Application Enable / Disable	Enabled	<p>ME Application State – This determines the state that an OEM would ship a specific ME Application</p> <p>– 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</p>																																																													
PAVP 1.5 Enable / Disable	Enabled																																																														
Intel® QST Enable / Disable	Enabled																																																														
Sentry Peak Enable / Disable	Enabled																																																														
Intel® Remote Wake Technology Enable / Disable	Enabled																																																														

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

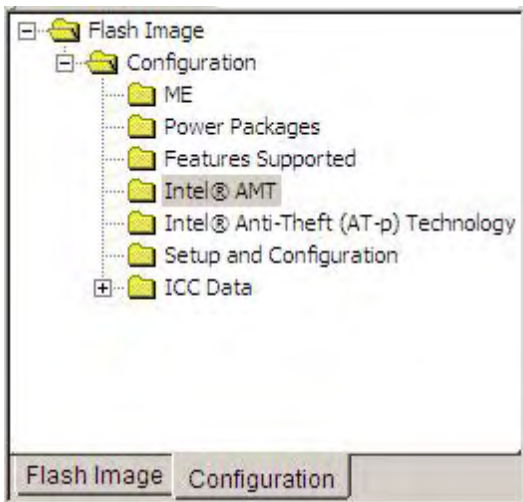
The "Shipping state" sub section (the lower sub section)

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.



Bring Up Process — All Platforms

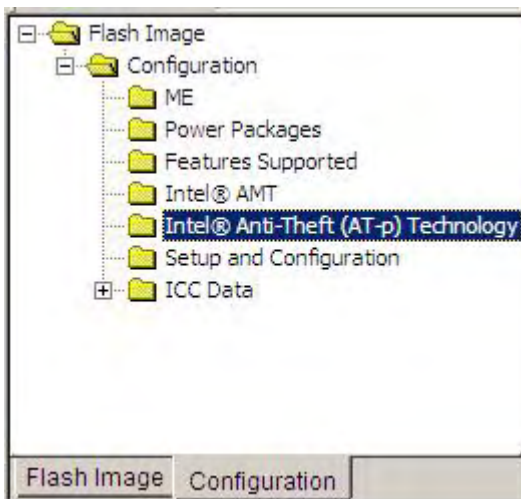
- On the navigation tree to the left, select the **Configuration** tab. Select **Intel® AMT** as shown below.

Location																																
		Parameter	Default	Comments																												
<table><tr><th>Parameter</th><th>Value</th></tr><tr><td>Intel® AMT Ping Response Enabled</td><td>true</td></tr><tr><td>VLAN</td><td>0</td></tr><tr><td>Boot into BIOS Setup Capable</td><td>false</td></tr><tr><td>Pause during BIOS Boot Capable</td><td>false</td></tr><tr><td>HostIf IDER Enabled</td><td>true</td></tr><tr><td>HostIf SOL Enabled</td><td>true</td></tr><tr><td>Idle Timeout - Manageability Engine</td><td>1</td></tr><tr><td>Full Test Counter</td><td>8</td></tr><tr><td>KVM Host I/F Enabled</td><td>11b Enabled</td></tr><tr><td>KVM Opt-In PTNI Editable Policy</td><td>11b Enabled</td></tr><tr><td>KVM Opt-In Enabled Policy</td><td>11b Enabled</td></tr><tr><td>USBr EHCI 1 Enabled</td><td>11b Enabled</td></tr><tr><td>USBr EHCI 2 Enabled</td><td>00b Not Set</td></tr></table>		Parameter	Value	Intel® AMT Ping Response Enabled	true	VLAN	0	Boot into BIOS Setup Capable	false	Pause during BIOS Boot Capable	false	HostIf IDER Enabled	true	HostIf SOL Enabled	true	Idle Timeout - Manageability Engine	1	Full Test Counter	8	KVM Host I/F Enabled	11b Enabled	KVM Opt-In PTNI Editable Policy	11b Enabled	KVM Opt-In Enabled Policy	11b Enabled	USBr EHCI 1 Enabled	11b Enabled	USBr EHCI 2 Enabled	00b Not Set			
Parameter	Value																															
Intel® AMT Ping Response Enabled	true																															
VLAN	0																															
Boot into BIOS Setup Capable	false																															
Pause during BIOS Boot Capable	false																															
HostIf IDER Enabled	true																															
HostIf SOL Enabled	true																															
Idle Timeout - Manageability Engine	1																															
Full Test Counter	8																															
KVM Host I/F Enabled	11b Enabled																															
KVM Opt-In PTNI Editable Policy	11b Enabled																															
KVM Opt-In Enabled Policy	11b Enabled																															
USBr EHCI 1 Enabled	11b Enabled																															
USBr EHCI 2 Enabled	00b Not Set																															
		Intel® AMT Ping Response Enabled	true																													
		VLAN	0																													
		Boot into BIOS Setup Capable	false																													
		Pause during BIOS Boot Capable	false																													
		HostIf IDER Enabled	true																													
		HostIf SOL Enabled	true																													
		Idle Timeout – Manageability Engine	1																													
		Full Test Counter	8																													
		KVM Host I/F Enabled	11b Enabled																													
		KVM Opt-In PTNI Editable Policy	11b Enabled																													
		KVM Opt-In Enabled Policy	11b Enabled																													
		USBr EHCI 1 Enabled	11b Enabled																													
		USBr EHCI 2 Enabled	10b Disabled																													



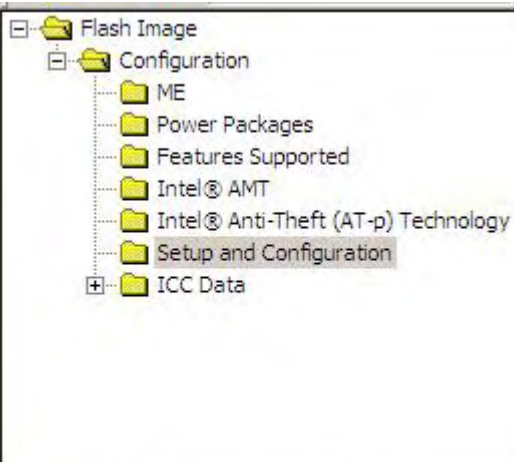
Bring Up Process — All Platforms

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

Location												
		Parameter	Default	Comments								
<table><tr><td>Allow Unsigned Assert Stolen</td><td>false</td></tr><tr><td> </td><td> </td></tr><tr><td> </td><td> </td></tr><tr><td> </td><td> </td></tr></table>		Allow Unsigned Assert Stolen	false							Allow Unsigned Assert Stolen	false	
Allow Unsigned Assert Stolen	false											

Bring Up Process — All Platforms

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

Location																																							
																																							
<div>Flash Image Configuration</div>	Parameter	Default	Comments																																				
<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>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>Remote Connectivity Service Capability</td><td>true</td></tr><tr><td>Remote Connectivity Service Enabler Id</td><td>00000000-0000-0000-0000-000000000000</td></tr><tr><td>Remote Connectivity Service Enabler Name</td><td></td></tr><tr><td>RCS HW Button</td><td>0x01</td></tr><tr><td>Hash 0 Active</td><td>false</td></tr><tr><td>Hash 0 Friendly Name</td><td></td></tr><tr><td>Hash 0 Stream</td><td></td></tr><tr><td>Hash 1 Active</td><td>false</td></tr><tr><td>Hash 1 Friendly Name</td><td></td></tr><tr><td>Hash 1 Stream</td><td></td></tr></table>	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 Connectivity Service Capability	true	Remote Connectivity Service Enabler Id	00000000-0000-0000-0000-000000000000	Remote Connectivity Service Enabler Name		RCS HW Button	0x01	Hash 0 Active	false	Hash 0 Friendly Name		Hash 0 Stream		Hash 1 Active	false	Hash 1 Friendly Name		Hash 1 Stream		ODM ID used by Intel® Upgrade Service	0x00000000	
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 Connectivity Service Capability	true																																						
Remote Connectivity Service Enabler Id	00000000-0000-0000-0000-000000000000																																						
Remote Connectivity Service Enabler Name																																							
RCS HW Button	0x01																																						
Hash 0 Active	false																																						
Hash 0 Friendly Name																																							
Hash 0 Stream																																							
Hash 1 Active	false																																						
Hash 1 Friendly Name																																							
Hash 1 Stream																																							
	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																																						
	Config Server FQDN																																						
	Remote Connectivity Service Capability	true																																					
	Remote Connectivity Service Enabler Id	0	This value must be programmed with your OEM specific Id if you enable RCS in your image.																																				



Bring Up Process — All Platforms

Location			
	Remote Connectivity Service Enabler Name		This value must be programmed with your OEM specific RCS Enabler name.
	RCS HW Button	0x01	
	Hash 0 Active	true	(See Appendix O)
	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	
	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	



Bring Up Process — All Platforms

Location			
	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	false	
	Hash 5 Friendly Name		
	Hash 5 Stream		
	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	
	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		



Bring Up Process — All Platforms

Location			
	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	
	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		



Bring Up Process — All Platforms

Location			
	Hash 22 Active	false	
	Hash 22 Friendly Name		
	Hash 22 Stream		



5.2.12 Program Clock Control Parameters

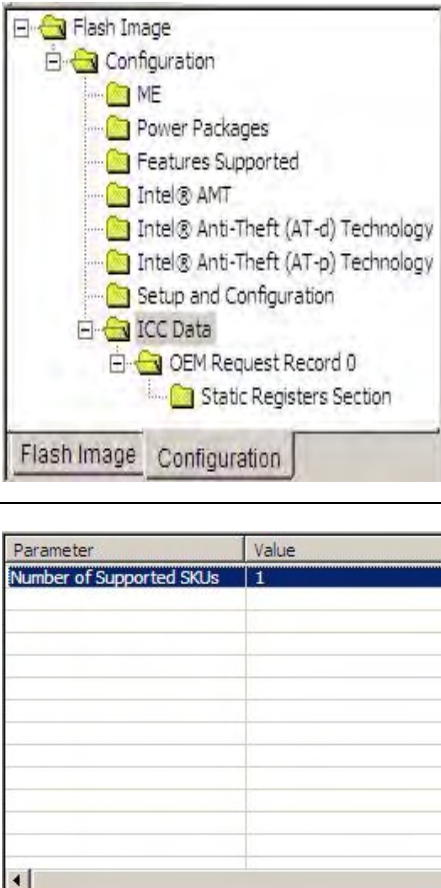
All parameters in this section are color-coded as per the key below.

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.

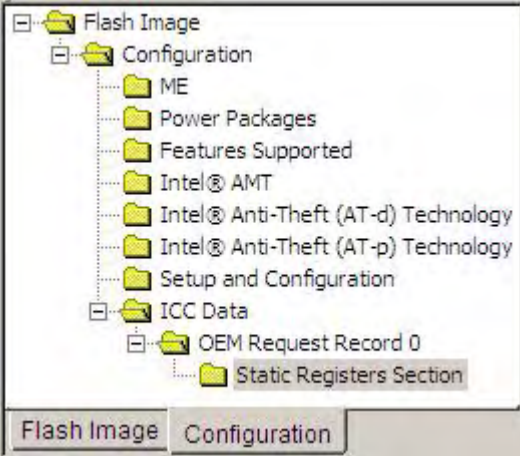

1. On the navigation tree to the left, select the **Configuration** tab. Select **Flash Image | Configuration | ICC Data**. Set the parameters in the **ICC Data** section as shown in the table below.

Location	Parameter	Default	Comments
	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.



Bring Up Process — All Platforms

- 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
	FCSS	0x00000344	Turn off unsupported clock output on CLKOUTFLEX2 and CLKOUTFLEX1. Thus: <ul style="list-style-type: none">F3SS = 000b = 48 MHzF2SS = 011b = 14.31818 MHzF1SS = 100b = Disabled (DC logic '0')F0SS = 100b = Disabled (DC logic '0') See Section A.2.1 for further details
	OCKEN	0x1FFF0F8F	See Section A.2.2 for further details
	IBEN	0x00000000	See Section A.2.3 for further details
	PM1	0x00000013	Set this value to 0x00000011. Allows VBIOS and Integrated Graphics Device driver to power manage DIV1S (see A.2.4, page 102). This setting is also safe for processors without Integrated Graphics. This is accomplished by: SSC1DSEN = 11b DIV1NSDSEN = 0b See Section A.2.4 for further details
	PM2	0x00000000	See Section A.2.5 for further details



Bring Up Process — All Platforms

Location	Parameter	Default	Comments																																																																				
<table><tr><th>Parameter</th><th>Value</th></tr><tr><td>SEBP1</td><td>0x00009999</td></tr><tr><td>F3SLC</td><td>100b = Default Slew rate setting (~1.4V/ns for a TBD inch trace at double load)</td></tr><tr><td>F3SDLSR</td><td>1b = 17 Ohms for double load usage</td></tr><tr><td>F2SLC</td><td>100b = Default Slew rate setting (~1.4V/ns for a TBD inch trace at double load)</td></tr><tr><td>F2SDLSR</td><td>1b = 17 Ohms for double load usage</td></tr><tr><td>F1SLC</td><td>100b = Default Slew rate setting (~1.4V/ns for a TBD inch trace at double load)</td></tr><tr><td>F1SDLSR</td><td>1b = 17 Ohms for double load usage</td></tr><tr><td>F0SLC</td><td>100b = Default Slew rate setting (~1.4V/ns for a TBD inch trace at double load)</td></tr><tr><td>F0SDLSR</td><td>1b = 17 Ohms for double load usage</td></tr><tr><td>SEBP2</td><td>0x00099999</td></tr><tr><td>PCI4SLC</td><td>100b = Default Slew rate setting (~1.4V/ns for a TBD inch trace at double load)</td></tr><tr><td>PCI4SDLSR</td><td>1b = 17 Ohms for double load usage</td></tr><tr><td>PCI3SLC</td><td>100b = Default Slew rate setting (~1.4V/ns for a TBD inch trace at double load)</td></tr><tr><td>PCI3SDLSR</td><td>1b = 17 Ohms for double load usage</td></tr><tr><td>PCI2SLC</td><td>100b = Default Slew rate setting (~1.4V/ns for a TBD inch trace at double load)</td></tr><tr><td>PCI2SDLSR</td><td>1b = 17 Ohms for double load usage</td></tr><tr><td>PCI1SLC</td><td>100b = Default Slew rate setting (~1.4V/ns for a TBD inch trace at double load)</td></tr><tr><td>PCI1SDLSR</td><td>1b = 17 Ohms for double load usage</td></tr><tr><td>PCI0SLC</td><td>100b = Default Slew rate setting (~1.4V/ns for a TBD inch trace at double load)</td></tr><tr><td>PCI0SDLSR</td><td>1b = 17 Ohms for double load usage</td></tr><tr><td>PMSRCCLK1</td><td>0x76543210</td></tr><tr><td>CRQSEL_SRC7</td><td>0111b = SRC7CLKRQ#/GPIO46 controls CLKOUT_SRC7</td></tr><tr><td>CRQSEL_SRC6</td><td>0110b = SRC6CLKRQ#/GPIO45 controls CLKOUT_SRC6</td></tr><tr><td>CRQSEL_SRC5</td><td>0101b = SRC5CLKRQ#/GPIO44 controls CLKOUT_SRC5</td></tr><tr><td>CRQSEL_SRC4</td><td>0100b = SRC4CLKRQ#/GPIO26 controls CLKOUT_SRC4</td></tr><tr><td>CRQSEL_SRC3</td><td>0011b = SRC3CLKRQ#/GPIO25 controls CLKOUT_SRC3</td></tr><tr><td>CRQSEL_SRC2</td><td>0010b = SRC2CLKRQ#/GPIO20 controls CLKOUT_SRC2</td></tr><tr><td>CRQSEL_SRC1</td><td>0001b = SRC1CLKRQ#/GPIO18 controls CLKOUT_SRC1</td></tr><tr><td>CRQSEL_SRC0</td><td>0000b = SRC0CLKRQ#/GPIO73 controls CLKOUT_SRC0</td></tr><tr><td>PMSRCCLK2</td><td>0x00000F98</td></tr><tr><td>CRQSEL_SRC8</td><td>1111b = Disable dynamic control of CLKOUT_SRC8</td></tr><tr><td>CRQSEL_PEGB</td><td>1001b = SRC9CLKRQ#/PEG_B_CLKRQ#/GPIO56 controls CLKOUT_PEG_B</td></tr><tr><td>CRQSEL_PEGA</td><td>1000b = SRC8CLKRQ#/PEG_A_CLKRQ#/GPIO47 controls CLKOUT_PEG_A</td></tr></table>	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	CRQSEL_SRC7	0111b = SRC7CLKRQ#/GPIO46 controls CLKOUT_SRC7	CRQSEL_SRC6	0110b = SRC6CLKRQ#/GPIO45 controls CLKOUT_SRC6	CRQSEL_SRC5	0101b = SRC5CLKRQ#/GPIO44 controls CLKOUT_SRC5	CRQSEL_SRC4	0100b = SRC4CLKRQ#/GPIO26 controls CLKOUT_SRC4	CRQSEL_SRC3	0011b = SRC3CLKRQ#/GPIO25 controls CLKOUT_SRC3	CRQSEL_SRC2	0010b = SRC2CLKRQ#/GPIO20 controls CLKOUT_SRC2	CRQSEL_SRC1	0001b = SRC1CLKRQ#/GPIO18 controls CLKOUT_SRC1	CRQSEL_SRC0	0000b = SRC0CLKRQ#/GPIO73 controls CLKOUT_SRC0	PMSRCCLK2	0x00000F98	CRQSEL_SRC8	1111b = Disable dynamic control of CLKOUT_SRC8	CRQSEL_PEGB	1001b = SRC9CLKRQ#/PEG_B_CLKRQ#/GPIO56 controls CLKOUT_PEG_B	CRQSEL_PEGA	1000b = SRC8CLKRQ#/PEG_A_CLKRQ#/GPIO47 controls CLKOUT_PEG_A	SEBP1	0x00009999	See Section A.2.6 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																																																																					
	CRQSEL_SRC7	0111b = SRC7CLKRQ#/GPIO46 controls CLKOUT_SRC7																																																																					
	CRQSEL_SRC6	0110b = SRC6CLKRQ#/GPIO45 controls CLKOUT_SRC6																																																																					
	CRQSEL_SRC5	0101b = SRC5CLKRQ#/GPIO44 controls CLKOUT_SRC5																																																																					
	CRQSEL_SRC4	0100b = SRC4CLKRQ#/GPIO26 controls CLKOUT_SRC4																																																																					
	CRQSEL_SRC3	0011b = SRC3CLKRQ#/GPIO25 controls CLKOUT_SRC3																																																																					
	CRQSEL_SRC2	0010b = SRC2CLKRQ#/GPIO20 controls CLKOUT_SRC2																																																																					
	CRQSEL_SRC1	0001b = SRC1CLKRQ#/GPIO18 controls CLKOUT_SRC1																																																																					
	CRQSEL_SRC0	0000b = SRC0CLKRQ#/GPIO73 controls CLKOUT_SRC0																																																																					
	PMSRCCLK2	0x00000F98																																																																					
	CRQSEL_SRC8	1111b = Disable dynamic control of CLKOUT_SRC8																																																																					
	CRQSEL_PEGB	1001b = SRC9CLKRQ#/PEG_B_CLKRQ#/GPIO56 controls CLKOUT_PEG_B																																																																					
	CRQSEL_PEGA	1000b = SRC8CLKRQ#/PEG_A_CLKRQ#/GPIO47 controls CLKOUT_PEG_A																																																																					
		SEBP2	0x00099999	See Section A.2.7 for further details																																																																			
		PMSRCCLK1	0xFFFFFFFF	See Section A.2.8 for further details																																																																			
		PMSRCCLK1	0x00000FFF	See Section A.2.9 for further details																																																																			

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 **97**).

- 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:



Bring Up Process — All Platforms

Table 5-1. High Impact Clock Control Parameters

Clock Output Pin	XML Symbol and Bit Offsets	Default	Description
CLKOUT_FLEX3	FCSS[14:12]	000b	<p>FLEXCLK3 Source Select (F3SS): Selects the source of clock to be driven out on CLKOUTFLEX3.</p> <p>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</p> <p><i>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.</i></p>
CLKOUT_FLEX3	SEBP1[12]	1b	<p>FLEXCLK3 Single/Double Load Series Resistance (F3SDLR): Sets programmable series resistance for CLKOUTFLEX3.</p> <p>0b = 25 Ohms for single load usage 1b = 17 Ohms for double load usage</p>
CLKOUT_FLEX2	FCSS[10:8]	000b	<p>FLEXCLK2 Source Select (F2SS): Selects the source of clock to be driven out on CLKOUTFLEX2.</p> <p>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</p>
CLKOUT_FLEX2	SEBP1[8]	1b	<p>FLEXCLK2 Single/Double Load Series Resistance (F2SDLR): Sets programmable series resistance for CLKOUTFLEX2.</p> <p>0b = 25 Ohms for single load usage 1b = 17 Ohms for double load usage</p>
CLKOUT_FLEX1	FCSS[6:4]	011b	<p>FLEXCLK1 Source Select (F1SS): Selects the source of clock to be driven out on CLKOUTFLEX1.</p> <p>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</p>



Bring Up Process — All Platforms

Clock Output Pin	XML Symbol and Bit Offsets	Default	Description
			<i>Note: These clock select settings only take effect when this muxed FLEXCLK/GPIO pin is configured for FLEXCLK native usage. Refer to the <i>Ibex Peak EDS</i> for configuration of GPIO vs. native usage.</i>
CLKOUT_FLEX1	SEBP1[4]	1b	FLEXCLK1 Single/Double Load Series Resistance (F1SDLR): 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 (FOSS): 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 <i>Note: These clock select settings only take effect when this muxed FLEXCLK/GPIO pin is configured for FLEXCLK native usage. Refer to the <i>Ibex Peak EDS</i> for configuration of GPIO vs. native usage.</i>
CLKOUT_FLEX0	SEBP1[0]	1b	FLEXCLK0 Single/Double Load Series Resistance (F0SDLR): 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 (PCI4SDLR): 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 (PCI3SDLR): 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 (PCI2SDLR): Sets programmable series resistance for CLKOUT_PCI2. 0b = 25 Ohms for single load usage 1b = 17 Ohms for double load usage



Bring Up Process — All Platforms

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



5.2.13 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.

5.2.14 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 5.2.2, page 34)

5.3 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.

5.4 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 5.2.2, page 34) where your generated SPI flash binary images are saved. It is assumed that this image file is named **outimage.bin**.



Bring Up Process — All Platforms

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.

5.5 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 CTRL-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.

5.5.1 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 4.2, page 24).
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 5.2.2, page 34) 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
```

5.5.2 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 4.2, page 24).
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 5.2.2, page 34) 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
```



6 Intel® Remote PC Assist Technology (RPAT)

- **This section is only applicable if Intel® Remote PC Assist Technology is to be configured on the target platform. If not, please skip this section and continue with the next section.**
- This section describes the soft straps that need to be set to enable Intel® RPAT.
- Note that there are two options for Intel® RPAT which are for Consumer and vPro system
- 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.

Intel® RPAT platform consists of hardware components equal to vPro systems. The exception is that the consumer product does not need the ME voltage regulator as it has M0 support only.

The Intel® RPAT Consumer /Business FW configurations guide will be based on the bring up instructions in sections 5.1 to 5.2 (including) for an AMT system, In order to reduce mistakes you'll be required to follow some of the sections as describe above and then change specific parameters for your technology of choice: **Changes are marked in RED. Below is step by step procedure.**

6.1 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:

6.1.1 Intel® RPAT Consumer Bring Up

Please Follow sections 5.1 – 5.2.1 as describe above (Assemble the SPI Flash Binary Image, Set Up the Build Environment).

6.1.2 Selecting Intel® RPAT Consumer Platform SKU

As describe in section 5.2.2 Use the SKU Manager drop down box to select the appropriate platform type for your specific chipset.



Intel® Remote PC Assist Technology (RPAT)

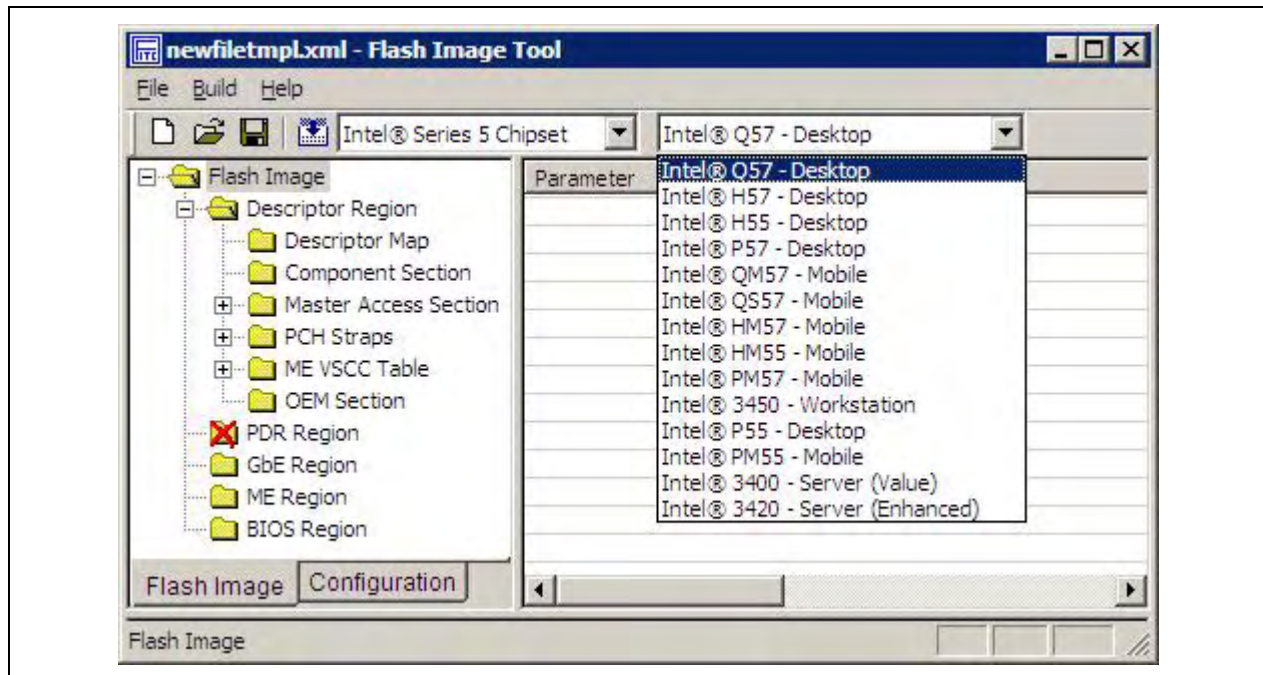
This new feature allows testing how firmware behaves with SKU'd HW using Super-SKU Ibex Peak.

- 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 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**

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.

6.1.3 Intel® RPAT Consumer bring up continued

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



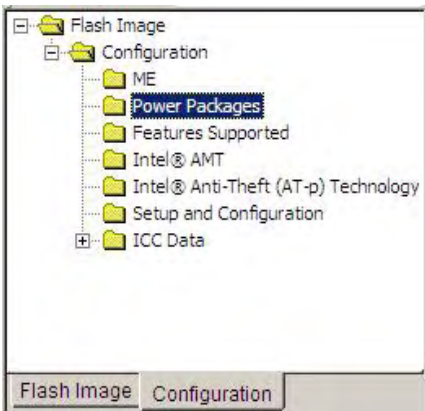
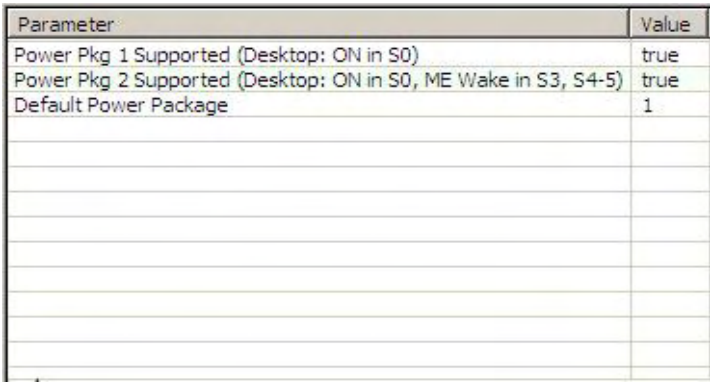
6.1.4 Intel® RPat Consumer Configuration Parameters

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

Follow section 2.2.11 Configuration Parameters describe above for an AMT system, these will use as a baseline, and then you must change the specific parameters (below) in order to configure Intel® RPat consumer FW.

Changes are marked in RED, and followed by screenshots.

1. On the navigation tree to the left, select the **Configuration** tab. Select **Power Packages** as shown below, please make sure the below configuration (only S0 support in RPat consumer SKU's both Desktop and Mobile).

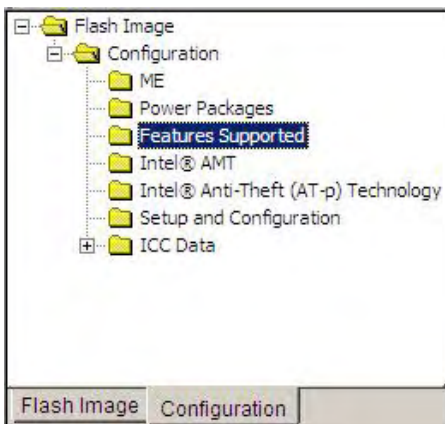
Location	Parameter	Default	Comments
	Power Pkg 1 Supported (Desktop: On in S0)	true	This parameter configures ME for S0 operation only.
Desktop Power Packages 	Power Pkg 2 Supported (Desktop: On in S0, ME Wake in S3, S4-5)	true	This parameter configures ME for operation in S0 and ME Wake in S3, S4 and S5.
	Default Power Package	1	This parameter determines the default Power Package used by firmware image.

Location			
Mobile Power Packages	Power Pkg 1 Supported (Mobile: On in S0)	true	This parameter configures ME for S0 operation only.
	Power Pkg 2 Supported (Mobile: ON in S0, ME Wake in S3, S4-5 (AC only))	true	
	Default Power Package	1	

2. On the navigation tree to the left, select the **Configuration** tab. Select **Features Supported** as shown below, the configurations below are basically already set according to each SKU.
- In order to have Intel® RPAT enabled Intel® Manageability Application both settings must be configure as below (in RED)
 - * In case **Intel® Identity Protection Technology** is being supported you will need to set the: "Intel® Identity Protection Technology Permanently Disabled" option to No?
 - ** **Intel® Remote Wake Technology** will be supported in Intel RPAT consumer on Desktop SKUs only.



Intel® Remote PC Assist Technology (RPAT)

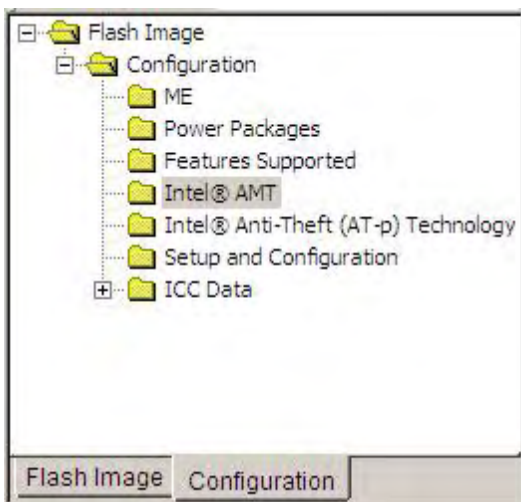
Location	Parameter	Default	Comments																																																									
			<p>These options control the availability / visibility of firmware features.</p> <p>In instances where a specific feature is configurable in the MEBx disabling it through the 'Features Supported' section will hide / disable that specific feature in the MEBx.</p>																																																									
<table><tr><th>Parameter</th><th>Value</th></tr><tr><td>Enable Intel® Standard Manageability; Disable Intel® AMT</td><td>No</td></tr><tr><td>Manageability Application Permanently Disabled?</td><td>No</td></tr><tr><td>PAVP 1.5 Permanently Disabled?</td><td>No</td></tr><tr><td>Intel® QST Permanently Disabled?</td><td>No</td></tr><tr><td>Intel® Identity Protection Technology Permanently Disabled?</td><td>Yes</td></tr><tr><td>Intel® Remote Wake Technology Permanently Disabled?</td><td>Yes</td></tr><tr><td>KVM Permanently Disabled?</td><td>No</td></tr><tr><td>Braidwood Technology Permanently Disabled?</td><td>No</td></tr><tr><td>TLS Permanently Disabled?</td><td>No</td></tr><tr><td>Manageability Application Enable/Disable</td><td>Enabled</td></tr><tr><td>PAVP 1.5 Enable/Disable</td><td>Enabled</td></tr><tr><td>Intel® QST Enable/Disable</td><td>Enabled</td></tr><tr><td>Intel® Identity Protection Technology Enable/Disable</td><td>Disabled</td></tr><tr><td>Intel® Remote Wake Technology Enable/Disable</td><td>Disabled</td></tr></table>	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	Braidwood Technology Permanently Disabled?	No	TLS Permanently Disabled?	No	Manageability Application Enable/Disable	Enabled	PAVP 1.5 Enable/Disable	Enabled	Intel® QST Enable/Disable	Enabled	Intel® Identity Protection Technology Enable/Disable	Disabled	Intel® Remote Wake Technology Enable/Disable	Disabled	<table><tr><td>Enable Intel® Standard Manageability; Disable Intel® AMT</td><td>No</td></tr><tr><td>Intel® Manageability Application Permanently Disabled?</td><td>No</td></tr><tr><td>PAVP 1.5 Permanently Disabled?</td><td>No</td></tr><tr><td>Intel® QST Permanently Disabled?</td><td>No</td></tr><tr><td>Intel® Identity Protection Technology Permanently Disabled?</td><td>Yes</td></tr><tr><td>Intel® Remote Wake Technology Permanently Disabled?</td><td>No</td></tr><tr><td>KVM Permanently Disabled?</td><td>No</td></tr><tr><td>Braidwood Technology Permanently Disabled?</td><td>No</td></tr><tr><td>TLS Permanently Disabled?</td><td>No</td></tr><tr><td>Intel® Manageability Application Enable / Disable</td><td>Enabled</td></tr><tr><td>PAVP 1.5 Enable / Disable</td><td>Enabled</td></tr><tr><td>Intel® QST Enable / Disable</td><td>Enabled</td></tr><tr><td>Intel® Identity Protection Technology Enable / Disable</td><td>Enabled</td></tr><tr><td>Intel® Remote Wake Technology Enable / Disable</td><td>Enabled</td></tr></table>	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?	No	KVM Permanently Disabled?	No	Braidwood Technology Permanently Disabled?	No	TLS Permanently Disabled?	No	Intel® Manageability Application Enable / Disable	Enabled	PAVP 1.5 Enable / Disable	Enabled	Intel® QST Enable / Disable	Enabled	Intel® Identity Protection Technology Enable / Disable	Enabled	Intel® Remote Wake Technology Enable / Disable	Enabled	<p>Note: Setting any of these options to 'Yes' will permanently disable that specific feature.</p> <p>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</p>
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																																																											
Braidwood Technology Permanently Disabled?	No																																																											
TLS Permanently Disabled?	No																																																											
Manageability Application Enable/Disable	Enabled																																																											
PAVP 1.5 Enable/Disable	Enabled																																																											
Intel® QST Enable/Disable	Enabled																																																											
Intel® Identity Protection Technology Enable/Disable	Disabled																																																											
Intel® Remote Wake Technology Enable/Disable	Disabled																																																											
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?	No																																																											
KVM Permanently Disabled?	No																																																											
Braidwood Technology Permanently Disabled?	No																																																											
TLS Permanently Disabled?	No																																																											
Intel® Manageability Application Enable / Disable	Enabled																																																											
PAVP 1.5 Enable / Disable	Enabled																																																											
Intel® QST Enable / Disable	Enabled																																																											
Intel® Identity Protection Technology Enable / Disable	Enabled																																																											
Intel® Remote Wake Technology Enable / Disable	Enabled																																																											
<p>This section is divided into two sub sections separated by a blank row:</p> <p>Permanently disabled sub section (top section)</p> <p>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</p> <p>The "Shipping state" sub section (the lower sub section)</p> <p>This determines the state that an OEM would ship a specific ME Application.</p> <p>This state (enabled /disabled) can be later changed through available interfaces such as MEBx / USB / Agent / Management Console etc.</p>																																																												



Intel® Remote PC Assist Technology (RPAT)

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

- In order to have Intel® RPAT enabled settings must be configure as below (in RED)

Location																															
																															
<table><tr><th>Parameter</th><th>Value</th></tr><tr><td>Intel® AMT Ping Response Enabled</td><td>true</td></tr><tr><td>VLAN</td><td>0</td></tr><tr><td>Boot into BIOS Setup Capable</td><td>true</td></tr><tr><td>Pause during BIOS Boot Capable</td><td>true</td></tr><tr><td>HostIf IDER Enabled</td><td>true</td></tr><tr><td>HostIf SOL Enabled</td><td>true</td></tr><tr><td>Idle Timeout - Manageability Engine</td><td>1</td></tr><tr><td>Full Test Counter</td><td>8</td></tr><tr><td>KVM Host I/F Enabled</td><td>11b Enabled</td></tr><tr><td>KVM Opt-In PTNI Editable Policy</td><td>11b Enabled</td></tr><tr><td>KVM Opt-In Enabled Policy</td><td>11b Enabled</td></tr><tr><td>USBr EHCI 1 Enabled</td><td>11b Enabled</td></tr><tr><td>USBr EHCI 2 Enabled</td><td>10b Disabled</td></tr></table>	Parameter	Value	Intel® AMT Ping Response Enabled	true	VLAN	0	Boot into BIOS Setup Capable	true	Pause during BIOS Boot Capable	true	HostIf IDER Enabled	true	HostIf SOL Enabled	true	Idle Timeout - Manageability Engine	1	Full Test Counter	8	KVM Host I/F Enabled	11b Enabled	KVM Opt-In PTNI Editable Policy	11b Enabled	KVM Opt-In Enabled Policy	11b Enabled	USBr EHCI 1 Enabled	11b Enabled	USBr EHCI 2 Enabled	10b Disabled			
Parameter	Value																														
Intel® AMT Ping Response Enabled	true																														
VLAN	0																														
Boot into BIOS Setup Capable	true																														
Pause during BIOS Boot Capable	true																														
HostIf IDER Enabled	true																														
HostIf SOL Enabled	true																														
Idle Timeout - Manageability Engine	1																														
Full Test Counter	8																														
KVM Host I/F Enabled	11b Enabled																														
KVM Opt-In PTNI Editable Policy	11b Enabled																														
KVM Opt-In Enabled Policy	11b Enabled																														
USBr EHCI 1 Enabled	11b Enabled																														
USBr EHCI 2 Enabled	10b Disabled																														
	Parameter	Default	Comments																												
	Intel® AMT Ping Response Enabled	true																													
	VLAN	0																													
	Boot into BIOS Setup Capable	true																													
	Pause during BIOS Boot Capable	true																													
	HostIf IDER Enabled	true																													
	HostIf SOL Enabled	true																													
	Idle Timeout – Manageability Engine	1																													
	Full Test Counter	8																													
	KVM Host I/F Enabled	11b Enabled																													
	KVM Opt-In PTNI Editable Policy	11b Enabled																													
	KVM Opt-In Enabled Policy	11b Enabled																													
	USBr EHCI 1 Enabled	11b Enabled																													



Intel® Remote PC Assist Technology (RPAT)

Location			
	USB 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																																							
<div><div>Flash Image</div><div><div>Configuration</div><div>ME</div><div>Power Packages</div><div>Features Supported</div><div>Intel® AMT</div><div>Intel® Anti-Theft (AT-p) Technology</div><div>Setup and Configuration</div><div>ICC Data</div></div></div> <div><div>Flash Image</div><div>Configuration</div></div>																																							
	Parameter	Default	Comments																																				
<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>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>Remote Connectivity Service Capability</td><td>true</td></tr><tr><td>Remote Connectivity Service Enabler Id</td><td>00000000-0000-0000-0000-000000000000</td></tr><tr><td>Remote Connectivity Service Enabler Name</td><td></td></tr><tr><td>RCS HW Button</td><td>0x01</td></tr><tr><td>Hash 0 Active</td><td>false</td></tr><tr><td>Hash 0 Friendly Name</td><td></td></tr><tr><td>Hash 0 Stream</td><td></td></tr><tr><td>Hash 1 Active</td><td>false</td></tr><tr><td>Hash 1 Friendly Name</td><td></td></tr><tr><td>Hash 1 Stream</td><td></td></tr></table>	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 Connectivity Service Capability	true	Remote Connectivity Service Enabler Id	00000000-0000-0000-0000-000000000000	Remote Connectivity Service Enabler Name		RCS HW Button	0x01	Hash 0 Active	false	Hash 0 Friendly Name		Hash 0 Stream		Hash 1 Active	false	Hash 1 Friendly Name		Hash 1 Stream		ODM ID used by Intel® Upgrade Service	0x00000000	
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 Connectivity Service Capability	true																																						
Remote Connectivity Service Enabler Id	00000000-0000-0000-0000-000000000000																																						
Remote Connectivity Service Enabler Name																																							
RCS HW Button	0x01																																						
Hash 0 Active	false																																						
Hash 0 Friendly Name																																							
Hash 0 Stream																																							
Hash 1 Active	false																																						
Hash 1 Friendly Name																																							
Hash 1 Stream																																							
	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																																						
	Config Server FQDN																																						



Intel® Remote PC Assist Technology (RPAT)

Location			
	Remote Connectivity Service Capability	true	Specifies if the platform allows configuration of Remote Connectivity Service (Remote PC Assist Service) capability or not. When the value is "true", the platform will have RPAS (formally known as Remote Connectivity service) be enabled on the system and it can start an RPAT session if triggered to do so by MEBX or BIOS.
	Remote Connectivity Service Enabler Id	0	This value must be programmed with your OEM specific Id if you enable RCS in your image.
	Remote Connectivity Service Enabler Name		This value must be programmed with your OEM specific RCS Enabler name.
	RCS 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
	Hash 0 Active	true	(See Appendix C.5)



Intel® Remote PC Assist Technology (RPAT)

Location			
	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	
	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	

6.1.5 Intel® RPAT Consumer bring up cont..

Follow instructions in sections 5.2.12 – 5.5.2 (including) as describe above.



6.2 Intel® RPAT Business Firmware Bringup Process

In order to bring up an RPAT- business supported platform the following stages **must** be addressed – detailed description that includes screen shots located below.

Remark: RPAT – business is enabled on a vPro platform after AMT was configured correctly (see the relevant sections in this guide regarding the correct bring up of AMT).

6.2.1 Intel® RPAT Business Bring Up

Please Follow sections 5.1 – 5.2.1 as describe above (Assemble the SPI Flash Binary Image, Set Up the Build Environment).

6.2.2 Selecting Intel® RPAT Business Platform SKU

As describe in section 5.2.2 Use the SKU Manager drop down box to select the appropriate platform type for your specific chipset.

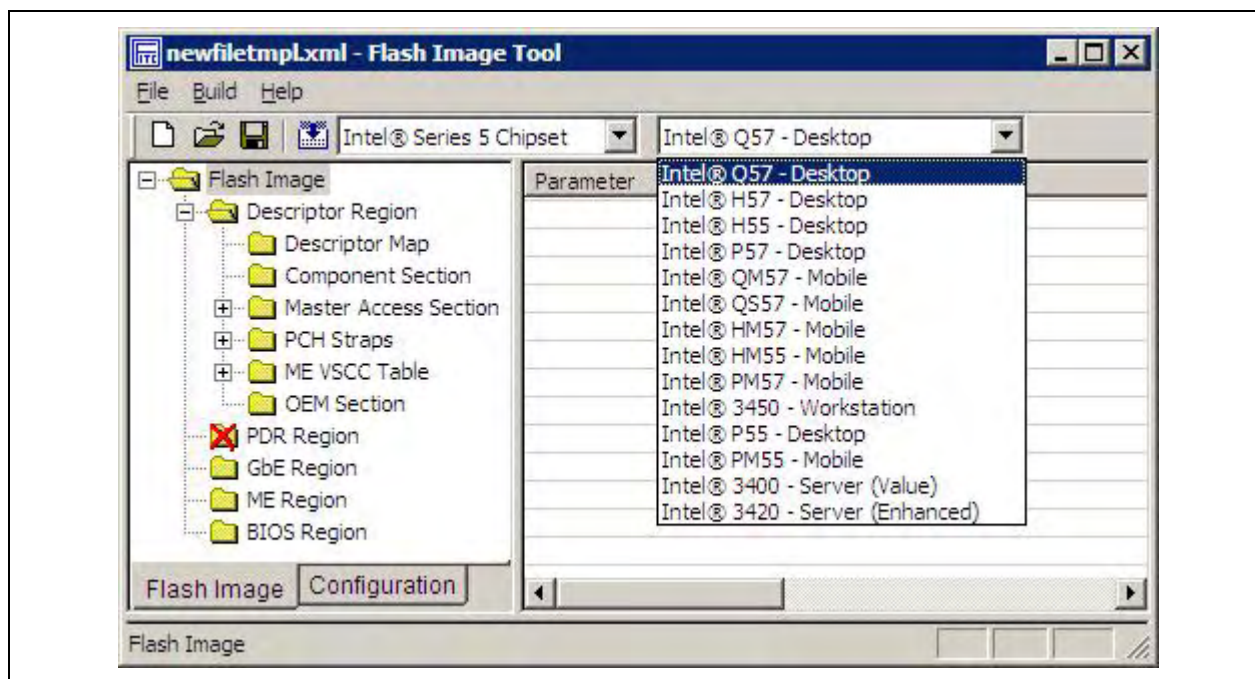
This new feature allows testing how firmware behaves with SKU'd HW using Super-SKU Ibex Peak.

- 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 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.

6.2.3 Intel® RPat Business bring-up continued

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

6.2.4 Intel® RPat Business Configuration Parameters

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

Follow section 2.2.11 Configuration Parameters describe above for an AMT system, these will use as a baseline, and then you must change the specific parameters (below) in order to configure Intel® RPat consumer FW.

Changes are marked in RED, and followed by screenshots.

1. **Set the "Default Power Package" to 2 in the** Power package tab.
2. Set the AMT tab configuration according to the desired settings
3. Set RCS "Remote Connectivity Service Capability"
4. Set "Remote Connectivity Service Enabler Id"
5. Remote Connectivity Service Enabler Name
6. Set RCS HW Button



Intel® Remote PC Assist Technology (RPAT)

- 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).

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

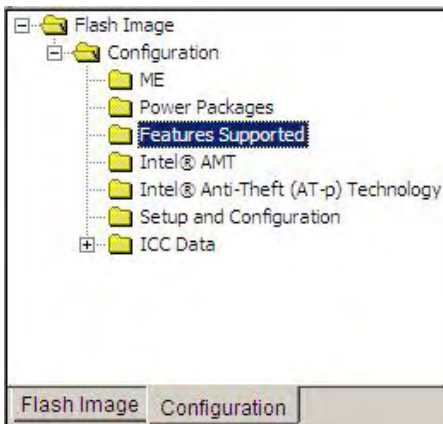


Intel® Remote PC Assist Technology (RPAT)

6. On the navigation tree to the left, select the **Configuration** tab. Select **Features Supported** as shown below, the configurations below are basically already set according to each SKU.
 - In order to have Intel® RPAT enabled Intel® Manageability Application both settings must be configure as below (in RED)
 - * In case Intel® Identity Protection Technology is being supported you will need to set the: "Intel® Identity Protection Technology Permanently Disabled" option to No?



Intel® Remote PC Assist Technology (RPAT)

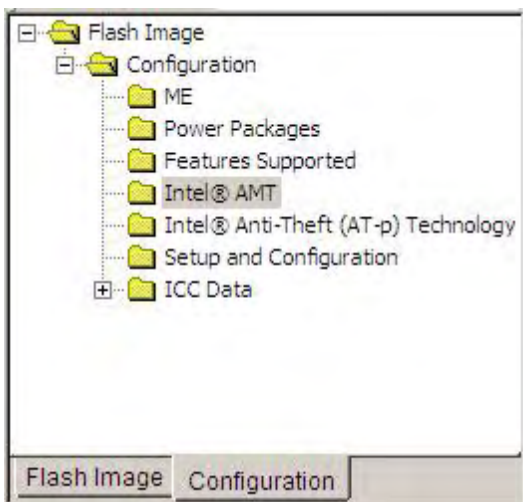
Location	Parameter	Default	Comments																																																									
			<p>These options control the availability / visibility of firmware features.</p> <p>In instances where a specific feature is configurable in the MEBx disabling it through the 'Features Supported' section will hide / disable that specific feature in the MEBx.</p>																																																									
<table><tr><th>Parameter</th><th>Value</th></tr><tr><td>Enable Intel® Standard Manageability; Disable Intel® AMT</td><td>No</td></tr><tr><td>Manageability Application Permanently Disabled?</td><td>No</td></tr><tr><td>PAVP 1.5 Permanently Disabled?</td><td>No</td></tr><tr><td>Intel® QST Permanently Disabled?</td><td>No</td></tr><tr><td>Intel® Identity Protection Technology Permanently Disabled?</td><td>Yes</td></tr><tr><td>Intel® Remote Wake Technology Permanently Disabled?</td><td>Yes</td></tr><tr><td>KVM Permanently Disabled?</td><td>No</td></tr><tr><td>Braidwood Technology Permanently Disabled?</td><td>No</td></tr><tr><td>TLS Permanently Disabled?</td><td>No</td></tr><tr><td>Manageability Application Enable/Disable</td><td>Enabled</td></tr><tr><td>PAVP 1.5 Enable/Disable</td><td>Enabled</td></tr><tr><td>Intel® QST Enable/Disable</td><td>Enabled</td></tr><tr><td>Intel® Identity Protection Technology Enable/Disable</td><td>Disabled</td></tr><tr><td>Intel® Remote Wake Technology Enable/Disable</td><td>Disabled</td></tr></table>	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	Braidwood Technology Permanently Disabled?	No	TLS Permanently Disabled?	No	Manageability Application Enable/Disable	Enabled	PAVP 1.5 Enable/Disable	Enabled	Intel® QST Enable/Disable	Enabled	Intel® Identity Protection Technology Enable/Disable	Disabled	Intel® Remote Wake Technology Enable/Disable	Disabled	<table><tr><td>Enable Intel® Standard Manageability; Disable Intel® AMT</td><td>No</td></tr><tr><td>Intel® Manageability Application Permanently Disabled?</td><td>No</td></tr><tr><td>PAVP 1.5 Permanently Disabled?</td><td>No</td></tr><tr><td>Intel® QST Permanently Disabled?</td><td>No</td></tr><tr><td>Intel® Identity Protection Technology Permanently Disabled? *(see note above)</td><td>Yes</td></tr><tr><td>Intel® Remote Wake Technology Permanently Disabled?</td><td>No</td></tr><tr><td>KVM Permanently Disabled?</td><td>No</td></tr><tr><td>Braidwood Technology Permanently Disabled?</td><td>No</td></tr><tr><td>TLS Permanently Disabled?</td><td>No</td></tr><tr><td>Intel® Manageability Application Enable / Disable</td><td>Enabled</td></tr><tr><td>PAVP 1.5 Enable / Disable</td><td>Enabled</td></tr><tr><td>Intel® QST Enable / Disable</td><td>Enabled</td></tr><tr><td>Intel® Identity Protection Technology Enable / Disable</td><td>Enabled</td></tr><tr><td>Intel® Remote Wake Technology Enable / Disable</td><td>Enabled</td></tr></table>	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? *(see note above)	Yes	Intel® Remote Wake Technology Permanently Disabled?	No	KVM Permanently Disabled?	No	Braidwood Technology Permanently Disabled?	No	TLS Permanently Disabled?	No	Intel® Manageability Application Enable / Disable	Enabled	PAVP 1.5 Enable / Disable	Enabled	Intel® QST Enable / Disable	Enabled	Intel® Identity Protection Technology Enable / Disable	Enabled	Intel® Remote Wake Technology Enable / Disable	Enabled	<p>Note: Setting any of these options to 'Yes' will permanently disable that specific feature.</p> <p>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</p>
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																																																											
Braidwood Technology Permanently Disabled?	No																																																											
TLS Permanently Disabled?	No																																																											
Manageability Application Enable/Disable	Enabled																																																											
PAVP 1.5 Enable/Disable	Enabled																																																											
Intel® QST Enable/Disable	Enabled																																																											
Intel® Identity Protection Technology Enable/Disable	Disabled																																																											
Intel® Remote Wake Technology Enable/Disable	Disabled																																																											
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? *(see note above)	Yes																																																											
Intel® Remote Wake Technology Permanently Disabled?	No																																																											
KVM Permanently Disabled?	No																																																											
Braidwood Technology Permanently Disabled?	No																																																											
TLS Permanently Disabled?	No																																																											
Intel® Manageability Application Enable / Disable	Enabled																																																											
PAVP 1.5 Enable / Disable	Enabled																																																											
Intel® QST Enable / Disable	Enabled																																																											
Intel® Identity Protection Technology Enable / Disable	Enabled																																																											
Intel® Remote Wake Technology Enable / Disable	Enabled																																																											
<p>This section is divided into two sub sections separated by a blank row:</p> <p>Permanently disabled sub section (top section)</p> <p>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</p> <p>The "Shipping state" sub section (the lower sub section)</p> <p>This determines the state that an OEM would ship a specific ME Application.</p> <p>This state (enabled /disabled) can be later changed through available interfaces such as MEBx / USB / Agent / Management Console etc.</p>			<p>ME Application State</p> <p>– This determines the state that an OEM would ship a specific ME Application</p> <p>– 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</p>																																																									



Intel® Remote PC Assist Technology (RPAT)

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

- In order to have Intel® RPAT enabled settings must be configure as below (in RED)

Location																																
		Parameter	Default	Comments																												
<table><tr><th>Parameter</th><th>Value</th></tr><tr><td>Intel® AMT Ping Response Enabled</td><td>true</td></tr><tr><td>VLAN</td><td>0</td></tr><tr><td>Boot into BIOS Setup Capable</td><td>true</td></tr><tr><td>Pause during BIOS Boot Capable</td><td>true</td></tr><tr><td>HostIf IDER Enabled</td><td>true</td></tr><tr><td>HostIf SOL Enabled</td><td>true</td></tr><tr><td>Idle Timeout - Manageability Engine</td><td>1</td></tr><tr><td>Full Test Counter</td><td>8</td></tr><tr><td>KVM Host I/F Enabled</td><td>11b Enabled</td></tr><tr><td>KVM Opt-In PTNI Editable Policy</td><td>11b Enabled</td></tr><tr><td>KVM Opt-In Enabled Policy</td><td>11b Enabled</td></tr><tr><td>USBr EHCI 1 Enabled</td><td>11b Enabled</td></tr><tr><td>USBr EHCI 2 Enabled</td><td>10b Disabled</td></tr></table>		Parameter	Value	Intel® AMT Ping Response Enabled	true	VLAN	0	Boot into BIOS Setup Capable	true	Pause during BIOS Boot Capable	true	HostIf IDER Enabled	true	HostIf SOL Enabled	true	Idle Timeout - Manageability Engine	1	Full Test Counter	8	KVM Host I/F Enabled	11b Enabled	KVM Opt-In PTNI Editable Policy	11b Enabled	KVM Opt-In Enabled Policy	11b Enabled	USBr EHCI 1 Enabled	11b Enabled	USBr EHCI 2 Enabled	10b Disabled	Intel® AMT Ping Response Enabled	true	
Parameter	Value																															
Intel® AMT Ping Response Enabled	true																															
VLAN	0																															
Boot into BIOS Setup Capable	true																															
Pause during BIOS Boot Capable	true																															
HostIf IDER Enabled	true																															
HostIf SOL Enabled	true																															
Idle Timeout - Manageability Engine	1																															
Full Test Counter	8																															
KVM Host I/F Enabled	11b Enabled																															
KVM Opt-In PTNI Editable Policy	11b Enabled																															
KVM Opt-In Enabled Policy	11b Enabled																															
USBr EHCI 1 Enabled	11b Enabled																															
USBr EHCI 2 Enabled	10b Disabled																															
		VLAN	0																													
		Boot into BIOS Setup Capable	true																													
		Pause during BIOS Boot Capable	true																													
		HostIf IDER Enabled	true																													
		HostIf SOL Enabled	true																													
		Idle Timeout – Manageability Engine	1																													
		Full Test Counter	8																													
		KVM Host I/F Enabled	11b Enabled																													
		KVM Opt-In PTNI Editable Policy	11b Enabled																													
		KVM Opt-In Enabled Policy	11b Enabled																													
		USBr EHCI 1 Enabled	11b Enabled																													



Intel® Remote PC Assist Technology (RPAT)

Location			
	USB [®] EHCI 2 Enabled	10b Disabled	

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

Location																																							
<div><div>Flash Image</div><div><div>Configuration</div><div>ME</div><div>Power Packages</div><div>Features Supported</div><div>Intel® AMT</div><div>Intel® Anti-Theft (AT-p) Technology</div><div>Setup and Configuration</div><div>ICC Data</div></div></div> <div><div>Flash Image</div><div>Configuration</div></div>	Parameter	Default	Comments																																				
<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>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>Remote Connectivity Service Capability</td><td>true</td></tr><tr><td>Remote Connectivity Service Enabler Id</td><td>00000000-0000-0000-0000-000000000000</td></tr><tr><td>Remote Connectivity Service Enabler Name</td><td></td></tr><tr><td>RCS HW Button</td><td>0x01</td></tr><tr><td>Hash 0 Active</td><td>false</td></tr><tr><td>Hash 0 Friendly Name</td><td></td></tr><tr><td>Hash 0 Stream</td><td></td></tr><tr><td>Hash 1 Active</td><td>false</td></tr><tr><td>Hash 1 Friendly Name</td><td></td></tr><tr><td>Hash 1 Stream</td><td></td></tr></table>	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 Connectivity Service Capability	true	Remote Connectivity Service Enabler Id	00000000-0000-0000-0000-000000000000	Remote Connectivity Service Enabler Name		RCS HW Button	0x01	Hash 0 Active	false	Hash 0 Friendly Name		Hash 0 Stream		Hash 1 Active	false	Hash 1 Friendly Name		Hash 1 Stream		ODM ID used by Intel® Upgrade Service	0x00000000	
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 Connectivity Service Capability	true																																						
Remote Connectivity Service Enabler Id	00000000-0000-0000-0000-000000000000																																						
Remote Connectivity Service Enabler Name																																							
RCS HW Button	0x01																																						
Hash 0 Active	false																																						
Hash 0 Friendly Name																																							
Hash 0 Stream																																							
Hash 1 Active	false																																						
Hash 1 Friendly Name																																							
Hash 1 Stream																																							
	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																																						
	Config Server FQDN																																						



Intel® Remote PC Assist Technology (RPAT)

Location			
	Remote Connectivity Service Capability	true	Specifies if the platform allows configuration of Remote Connectivity Service (Remote PC Assist Service) capability or not. When the value is "true", the platform will have RPAS (formally known as Remote Connectivity service) be enabled on the system and it can start an RPAT session if triggered to do so by MEBX or BIOS.
	Remote Connectivity Service Enabler Id	0	This value must be programmed with your OEM specific Id if you enable RCS in your image.
	Remote Connectivity Service Enabler Name		This value must be programmed with your OEM specific RCS Enabler name.
	RCS 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
	Hash 0 Active	true	(See Appendix C.5)



Intel® Remote PC Assist Technology (RPAT)

Location			
	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	
	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	

6.2.5 Intel® RPAT Bussines bring up continued

Follow instructions in sections 5.2.12 – 5.5.2 (including) as describe above.

7 Consumer SKU Intel® Identity Protection (Sentry Peak)

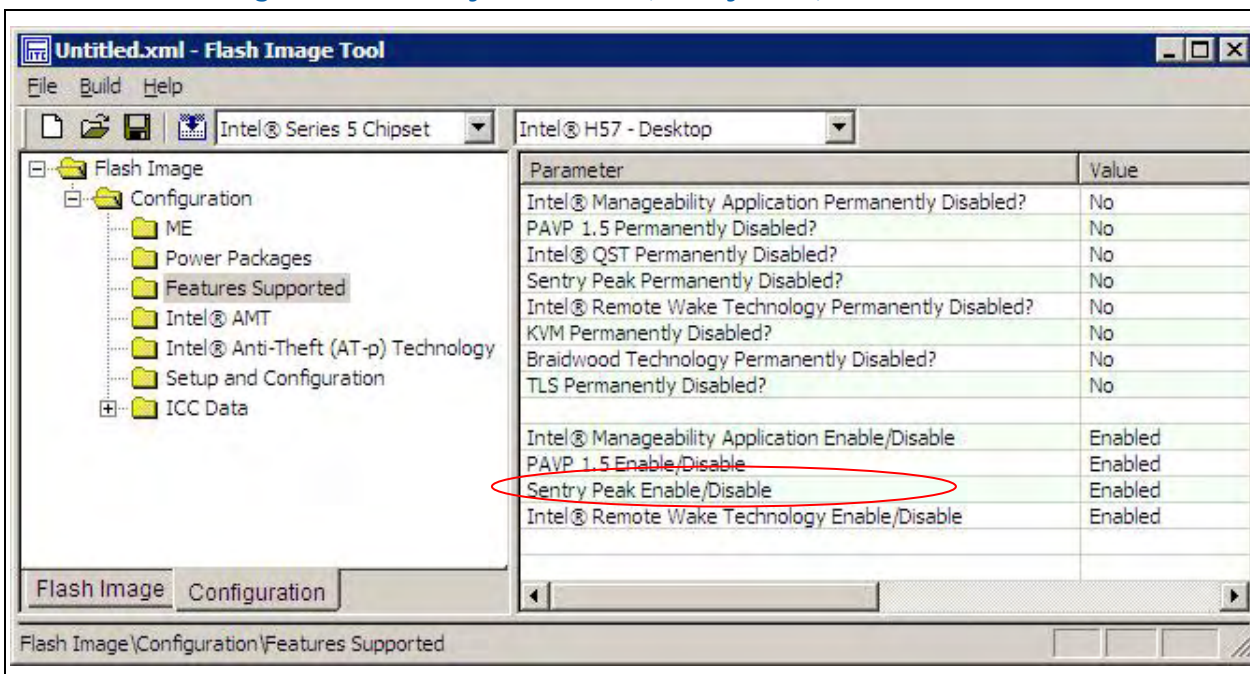
7.1 Intel® Identity Protection (Sentry Peak) Configuration:

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

The settings below cover H57, H55, HM57 and PM55 SKU platforms.

1. To enable Intel® Identity Protection (Sentry Peak):
 - a. Set the Sentry Peak Enable / Disable option to '**Enabled**' as shown below.
 - b. If enabled, this feature can be disabled in MEBx.

Table 7-1. Enabling Intel® Identity Protection (Sentry Peak)



Parameter	Value
Intel® Manageability Application Permanently Disabled?	No
PAVP 1.5 Permanently Disabled?	No
Intel® QST Permanently Disabled?	No
Sentry Peak Permanently Disabled?	No
Intel® Remote Wake Technology Permanently Disabled?	No
KVM Permanently Disabled?	No
Braidwood Technology Permanently Disabled?	No
TLS Permanently Disabled?	No
Intel® Manageability Application Enable/Disable	Enabled
PAVP 1.5 Enable/Disable	Enabled
Sentry Peak Enable/Disable	Enabled
Intel® Remote Wake Technology Enable/Disable	Enabled

7.2 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



Consumer SKU Intel® Identity Protection (Sentry Peak)

the tools and documents provided in the latest kit release should supersede any version available from any other source.

7.2.1 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 Sentry Peak Enablement field. Verify pass/fail criteria.	MEInfoWin.EXE	Intel IPT: Status Version

7.2.2 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:

- Boot to DOS shell
- Navigate to the directory containing MEInfo.exe
- Execute MEInfo.exe from the command prompt
- 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

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



Consumer SKU Intel® Identity Protection (Sentry Peak)

7.2.3 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

7.2.3.1 Example 1: Execute MEInfoWin without any parameters

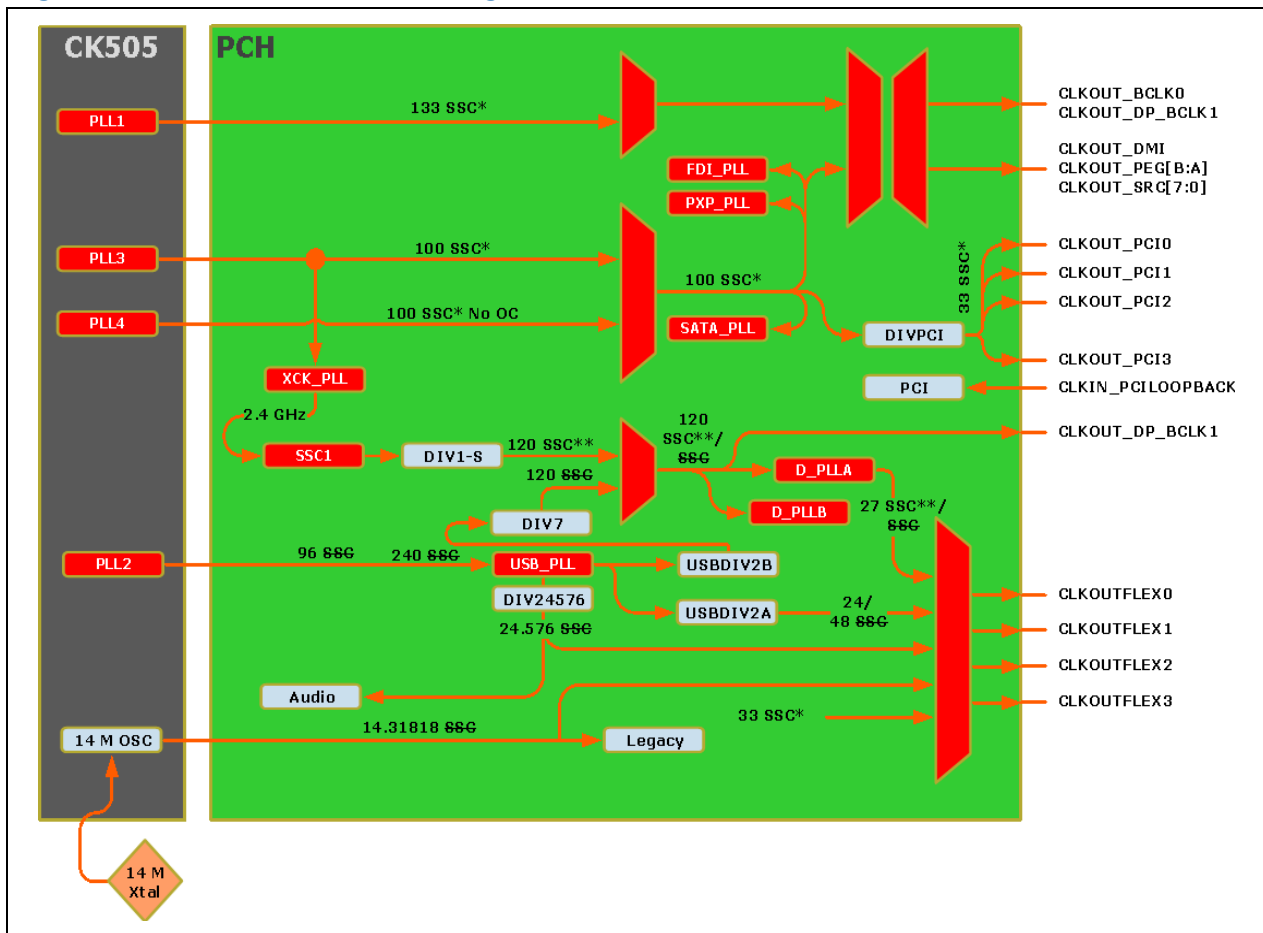
- Boot to Microsoft Windows
- Ensure that LMS and ME Drivers are installed
- Navigate to the folder containing MEInfoWin.exe
- Execute MEInfo.exe by double clicking its icon
- The following are examples of executing MEInfo.
- MEInfo will output many lines of data. In order to verify that Intel IPT is 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 7-1. Ibex Peak Buffer Through Mode Architecture



Only 14.31818 MHz and 48 MHz outputs from CLKOUTFLEX[3:0] are guaranteed.



Ibex Peak Clock Configuration

A.1 Functional Blocks

There are four spread modulators in the Ibex Peak, labeled as follows:

Table 7-2. 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 7-3. 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 CLKOUT_DP.
USBDIV1	Generates 96-MHz clock with no spread. Uses output of DIV5A. Supplies USB PLL.
USBDIV2A	Generates 24-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.



A.2.1 FCSS – Flex Clock Source Select

Flash Image Tool/ME FW Default: 0000 0344h

BTM Default: 00000304h

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

Flash Image Tool Configuration: Flash Image | Configuration | ICC Data | OEM Req.
Rec. Block | OEM Request Record [7:0] | Static Registers Section

Table 7-4. 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 <i>Ibex Peak EDS</i> for configuration of GPIO vs. native usage.
11:11	0h	Reserved (RSVD)
10:8	011b 0h	FLEXCLK2 Source Select (F3SS): Selects the source of clock to be driven out on CLKOUTFLEX2. 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 Reserved (RSVD)
7:7		
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') 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 <i>Ibex Peak EDS</i> 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



Ibex Peak Clock Configuration

Bits	Default	Description
		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 <i>Ibex Peak EDS</i> for configuration of GPIO vs. native usage.

A.2.2 OCKEN – Output Clock Enable

Flash Image Tool/ME FW Default: No changes from HW defaults

BTM Default: 1FFF0F8Fh

Description: This parameter controls enabling of output buffers

Flash Image Tool Configuration: Flash Image | Configuration | ICC Data | OEM Req. Rec. Block | OEM Request Record [7:0] | Static Registers Section

Table 7-5. 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 (CSIDPOCKEN): 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: Note that 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 PLEN[8]. When the ownership is under display control, the display logic side (not Intel ME Firmware) determines whether the output clock pin CLKOUT_DP_BCLK1 toggles or gated to low state.



Ibex Peak Clock Configuration

Bits	Default	Description
24	1b	<p>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.</p> <p>0b = Output clock is gated to low state</p> <p>1b = Output clock is enabled to toggle once its clock source has been initialized</p>
23:16	Ffh	<p>SRC 7:0 Output Clock Enable (SRC7OOCKEN): 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.</p> <p>0b = Corresponding output clock is gated to low state</p> <p>1b = Corresponding output clock is enabled to toggle once its clock source has been initialized (hot plug capable)</p>
15:12	0h	Reserved (RSVD)
11:7	1Fh	<p>PCICLK 4:0 Output Clock Enable (PCI4OOCKEN): Controls the enabling of PCI clock toggling. Each bit position controls the corresponding PCI output clock, e.g. bit 7 controls CLKOUT_PCIO. When any clock output is not used, it should be gated to low state to save power.</p> <p>0b = Corresponding output clock is gated to low state</p> <p>1b = Corresponding output clock is enabled to toggle once its clock source has been initialized</p> <p>A-stepping Note: This parameter has no effect and clock output is always enabled.</p> <p>B-stepping Note: Parameter behaves normally.</p>
6:4	0h	Reserved (RSVD)
3:0	Fh	<p>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.</p> <p>0b = Corresponding output clock is tri-stated (not driven)</p> <p>1b = Corresponding output clock is driven</p> <p>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.</p> <p>B-stepping Implementation: FLEXCLK 3:0 Output Clock Enable (PCI4OOCKEN): 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.</p> <p>0b = Corresponding output clock is gated to low state</p> <p>1b = Corresponding output clock is enabled to toggle once its clock source has been initialized</p> <p>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].</p>



Ibex Peak Clock Configuration

A.2.3 IBEN – Input Buffer Enable

Flash Image Tool/ME FW Default: No changes from HW defaults

BTM Default: 00000000h

Description: This parameter controls enabling of input buffers

Flash Image Tool Configuration: Flash Image | Configuration | ICC Data | OEM Req. Rec. Block | OEM Request Record [7:0] | Static Registers Section

Table 7-6. 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 (BCLKInCikBufDis): 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.2.4 PM1 – Power Management

Flash Image Tool/ME FW Default: No changes from HW defaults

Recommended Default: 0000 0011h

BTM Default: 00000000h

Description: This parameter controls power management features of clocks

Flash Image Tool Configuration: Flash Image | Configuration | ICC Data | OEM Req.
Rec. Block | OEM Request Record [7:0] | Static Registers Section

Table 7-7. Power Management Parameters

Bits	Default	Description
31:4	0h	Reserved (RSVD)
4	0b	<p>Dynamic SSC1 Shutdown Enable (SSC1DSEN): Enables dynamic power management of DIV1-S. 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 PLEN[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 (PLEN[9] is 1b). The following are logical combinations of this parameter field (MSB) and “Dynamic DIV1S Shutdown Enable” parameter field at PM1[0] (LSB).</p> <p>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.</p> <p>A-stepping Note: This parameter has no effect and the divider output is always enabled. B-stepping Note: Parameter behaves normally.</p>
3:2	0h	Reserved (RSVD)
1	0b	<p>Dynamic DIV1NS Shutdown Enable (DIV1NSDSEN): Enables dynamic power management of DIV1-NS.</p> <p>0b = Disable dynamic power management of DIV1-S 1b = Enable dynamic power management of DIV1-S</p> <p>A-stepping Note: This parameter has no effect and the divider output is always enabled. B-stepping Note: Parameter behaves normally.</p>
0	0b	<p>Dynamic DIV1S Shutdown Enable (DIV1SDSEN): Enables dynamic power management of DIV1-S (see Figure A.1, page 97).</p> <p>Do not configure this parameter field on its own. See “DIV1 Shutdown Enable” parameter field at PM1[4].</p>



Ibex Peak Clock Configuration

A.2.5 PM2 – Power Management

Flash Image Tool/ME FW Default: No changes from HW defaults

BTM Default: 00000000h

Description: This parameter controls power management features of clocks

Flash Image Tool Configuration: Flash Image | Configuration | ICC Data | OEM Req. Rec. Block | OEM Request Record [7:0] | Static Registers Section

Table 7-8. Power Management Parameters

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

A.2.6 SEBP1 – Single Ended Buffer Parameters

Flash Image Tool/ME FW Default: No changes from HW defaults

BTM Default: 00009999h

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 Req. Rec. Block | OEM Request Record [7:0] | Static Registers Section

Table 7-9. Single Ended Buffer Parameters

Bits	Default	Description
31:16	0h	Reserved (RSVD)
15:13	100b	<p>FLEXCLK3 Slew Rate Control (F3SLC): Controls slew rate for CLKOUTFLEX3.</p> <p>000b = Weakest slew rate setting (~0.6 V/ns for a TBD inch trace at double load)</p> <p>001b</p> <p>010b</p> <p>011b</p> <p>100b = Default Slew rate setting (~1.4V/ns for a TBD inch trace at double load)</p> <p>101b</p>



Ibex Peak Clock Configuration

Bits	Default	Description
		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. 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



Ibex Peak Clock Configuration

A.2.7 SEBP2 – Single Ended Buffer Parameters

Flash Image Tool/ME FW Default: No changes from HW defaults

BTM Default: 00099999h

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. Intel ME Firmware 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 Req. Rec. Block | OEM Request Record [7:0] | Static Registers Section

Table 7-10. 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 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



Ibex Peak Clock Configuration

Bits	Default	Description
		111b = Strongest slew rate setting (~2 V/ns for a TBD inch trace at double load)
8	1b	PCI1 Single/Double Load Series Resistance (PCI1SDLR) : 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 (PCI0SDLR) : 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)
0	1b	PCI4 Single/Double Load Series Resistance (PCI4SDLR) : Sets programmable series resistance for CLKOUT_PCI4. 0b = 25 Ohms for single load usage 1b = 17 Ohms for double load usage



Ibex Peak Clock Configuration

A.2.8 PMSRCCLK1 – SRC Power Management

Flash Image Tool/ME FW Default: FFFF FFFFh

BTM Default: 76543210h

Description: This parameter assigns dynamic CLKRQ# control of SRC clocks

Flash Image Tool Configuration: Unavailable

Table 7-11. SRC Power Management

Bits	Default	Description
31:28	0111b	<p>CLKRQ# Select for CLKOUT_SRC7 (CRQSELSRC7): Select external input CLKRQ# pin for dynamical control of CLKOUT_SRC7 output.</p> <p> 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 </p> <p>A-stepping Note: This parameter has no effect and the dynamic control CLKOUT_SRC7 output.</p> <p>B-stepping Note: Parameter behaves normally.</p>
27:24	0110b	<p>CLKRQ# Select for CLKOUT_SRC6 (CRQSELSRC6): Select external input CLKRQ# pin for dynamical control of CLKOUT_SRC6 output.</p> <p> 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 </p> <p>A-stepping Note: This parameter has no effect and the dynamic control CLKOUT_SRC6 output.</p> <p>B-stepping Note: Parameter behaves normally.</p>
23:20	0101b	<p>CLKRQ# Select for CLKOUT_SRC5 (CRQSELSRC5): Select external input CLKRQ# pin for dynamical control of CLKOUT_SRC5 output.</p> <p> 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 </p>



Ibex Peak Clock Configuration

Bits	Default	Description
		<p>1001b = SRC9CLKRQ#/PEG_B_CLKRQ#/GPIO56 controls CLKOUT_SRC5</p> <p>101xb = Reserved</p> <p>1110b = Reserved</p> <p>1111b = Disable dynamic control of CLKOUT_SRC5</p> <p>A-stepping Note: This parameter has no effect and the dynamic control CLKOUT_SRC5 output.</p> <p>B-stepping Note: Parameter behaves normally.</p>
19:16	0100b	<p>CLKRQ# Select for CLKOUT_SRC4 (CRQSELSRC4): Select external input CLKRQ# pin for dynamical control of CLKOUT_SRC4 output.</p> <p>0000b = SRC0CLKRQ#/GPIO73 controls CLKOUT_SRC4</p> <p>0001b = SRC1CLKRQ#/GPIO18 controls CLKOUT_SRC4</p> <p>0010b = SRC2CLKRQ#/GPIO20 controls CLKOUT_SRC4</p> <p>0011b = SRC3CLKRQ#/GPIO25 controls CLKOUT_SRC4</p> <p>0100b = SRC4CLKRQ#/GPIO26 controls CLKOUT_SRC4</p> <p>0101b = SRC5CLKRQ#/GPIO44 controls CLKOUT_SRC4</p> <p>0110b = SRC6CLKRQ#/GPIO45 controls CLKOUT_SRC4</p> <p>0111b = SRC7CLKRQ#/GPIO46 controls CLKOUT_SRC4</p> <p>1000b = SRC8CLKRQ#/PEG_A_CLKRQ#/GPIO47 controls CLKOUT_SRC4</p> <p>1001b = SRC9CLKRQ#/PEG_B_CLKRQ#/GPIO56 controls CLKOUT_SRC4</p> <p>101xb = Reserved</p> <p>1110b = Reserved</p> <p>1111b = Disable dynamic control of CLKOUT_SRC4</p> <p>A-stepping Note: This parameter has no effect and the dynamic control CLKOUT_SRC4 output.</p> <p>B-stepping Note: Parameter behaves normally.</p>
15:12	0011b	<p>CLKRQ# Select for CLKOUT_SRC3 (CRQSELSRC3): Select external input CLKRQ# pin for dynamical control of CLKOUT_SRC3 output.</p> <p>0000b = SRC0CLKRQ#/GPIO73 controls CLKOUT_SRC3</p> <p>0001b = SRC1CLKRQ#/GPIO18 controls CLKOUT_SRC3</p> <p>0010b = SRC2CLKRQ#/GPIO20 controls CLKOUT_SRC3</p> <p>0011b = SRC3CLKRQ#/GPIO25 controls CLKOUT_SRC3</p> <p>0100b = SRC4CLKRQ#/GPIO26 controls CLKOUT_SRC3</p> <p>0101b = SRC5CLKRQ#/GPIO44 controls CLKOUT_SRC3</p> <p>0110b = SRC6CLKRQ#/GPIO45 controls CLKOUT_SRC3</p> <p>0111b = SRC7CLKRQ#/GPIO46 controls CLKOUT_SRC3</p> <p>1000b = SRC8CLKRQ#/PEG_A_CLKRQ#/GPIO47 controls CLKOUT_SRC3</p> <p>1001b = SRC9CLKRQ#/PEG_B_CLKRQ#/GPIO56 controls CLKOUT_SRC3</p> <p>101xb = Reserved</p> <p>1110b = Reserved</p> <p>1111b = Disable dynamic control of CLKOUT_SRC3</p> <p>A-stepping Note: This parameter has no effect and the dynamic control CLKOUT_SRC3 output.</p> <p>B-stepping Note: Parameter behaves normally.</p>
11:8	0010b	<p>CLKRQ# Select for CLKOUT_SRC2 (CRQSELSRC2): Select external input CLKRQ# pin for dynamical control of CLKOUT_SRC2 output.</p> <p>0000b = SRC0CLKRQ#/GPIO73 controls CLKOUT_SRC2</p> <p>0001b = SRC1CLKRQ#/GPIO18 controls CLKOUT_SRC2</p> <p>0010b = SRC2CLKRQ#/GPIO20 controls CLKOUT_SRC2</p> <p>0011b = SRC3CLKRQ#/GPIO25 controls CLKOUT_SRC2</p> <p>0100b = SRC4CLKRQ#/GPIO26 controls CLKOUT_SRC2</p> <p>0101b = SRC5CLKRQ#/GPIO44 controls CLKOUT_SRC2</p> <p>0110b = SRC6CLKRQ#/GPIO45 controls CLKOUT_SRC2</p> <p>0111b = SRC7CLKRQ#/GPIO46 controls CLKOUT_SRC2</p> <p>1000b = SRC8CLKRQ#/PEG_A_CLKRQ#/GPIO47 controls CLKOUT_SRC2</p> <p>1001b = SRC9CLKRQ#/PEG_B_CLKRQ#/GPIO56 controls CLKOUT_SRC2</p> <p>101xb = Reserved</p> <p>1110b = Reserved</p> <p>1111b = Disable dynamic control of CLKOUT_SRC2</p>



Ibex Peak Clock Configuration

Bits	Default	Description
		<p>A-stepping Note: This parameter has no effect and the dynamic control CLKOUT_SRC2 output.</p> <p>B-stepping Note: Parameter behaves normally.</p>
7:4	0001b	<p>CLKRQ# Select for CLKOUT_SRC1 (CRQSELSRC1): Select external input CLKRQ# pin for dynamical control of CLKOUT_SRC1 output.</p> <p> 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 </p> <p>A-stepping Note: This parameter has no effect and the dynamic control CLKOUT_SRC1 output.</p> <p>B-stepping Note: Parameter behaves normally.</p>
3:0	0000b	<p>CLKRQ# Select for CLKOUT_SRC0 (CRQSELSRC0): Select external input CLKRQ# pin for dynamical control of CLKOUT_SRC0 output.</p> <p> 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 </p> <p>A-stepping Note: This parameter has no effect and the dynamic control CLKOUT_SRC0 output.</p> <p>B-stepping Note: Parameter behaves normally.</p>



A.2.9 PMSRCCLK2 – SRC Power Management

Flash Image Tool/ME FW Default: FFFF FFFFh

BTM Default: 00000F98h

Description: This parameter assigns dynamic CLKRQ# control of SRC clocks

Flash Image Tool Configuration: Unavailable

Table 7-12. SRC Power Management

Bits	Default	Description
31:12	0h	Reserved (RSVD)
11:8	1001b	<p>CLKRQ# Select for CLKOUT_SRC8 (CROSELSRC8): Select external input CLKRQ# pin for dynamical control of CLKOUT_SRC8 output.</p> <p> 0000b = SRC0CLKRQ#/GPIO73 controls CLKOUT_SRC8 0001b = SRC1CLKRQ#/GPIO18 controls CLKOUT_SRC8 0010b = SRC2CLKRQ#/GPIO20 controls CLKOUT_SRC8 0011b = SRC3CLKRQ#/GPIO25 controls CLKOUT_SRC8 0100b = SRC4CLKRQ#/GPIO26 controls CLKOUT_SRC8 0101b = SRC5CLKRQ#/GPIO44 controls CLKOUT_SRC8 0110b = SRC6CLKRQ#/GPIO45 controls CLKOUT_SRC8 0111b = SRC7CLKRQ#/GPIO46 controls CLKOUT_SRC8 1000b = SRC8CLKRQ#/PEG_A_CLKRQ#/GPIO47 controls CLKOUT_SRC8 1001b = SRC9CLKRQ#/PEG_B_CLKRQ#/GPIO56 controls CLKOUT_SRC8 101xb = Reserved 1110b = Reserved 1111b = Disable dynamic control of CLKOUT_SRC8 </p> <p>A-stepping Note: This parameter has no effect and the dynamic control CLKOUT_SRC8 output. B-stepping Note: Parameter behaves normally.</p>
7:4	1000b	<p>CLKRQ# Select for CLKOUT_PEG_B (CROSELPEGB): Select external input CLKRQ# pin for dynamical control of CLKOUT_PEG_B output.</p> <p> 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 </p> <p>A-stepping Note: This parameter has no effect and the dynamic control CLKOUT_PEG_B output. B-stepping Note: Parameter behaves normally.</p>
3:0	1111b	<p>CLKRQ# Select for CLKOUT_PEG_A (CROSELPEGA): Select external input CLKRQ# pin for dynamical control of CLKOUT_PEG_A output.</p> <p> 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 </p>



Ibex Peak Clock Configuration

Bits	Default	Description
		<p>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</p> <p>A-stepping Note: This parameter has no effect and the dynamic control CLKOUT_PEG_A output. B-stepping Note: Parameter behaves normally.</p>

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 Compliance Guide for ME Hardware, Intel*.

Figure 7-2. Configuration “A” — Desktop/Server/Workstation or Mobile

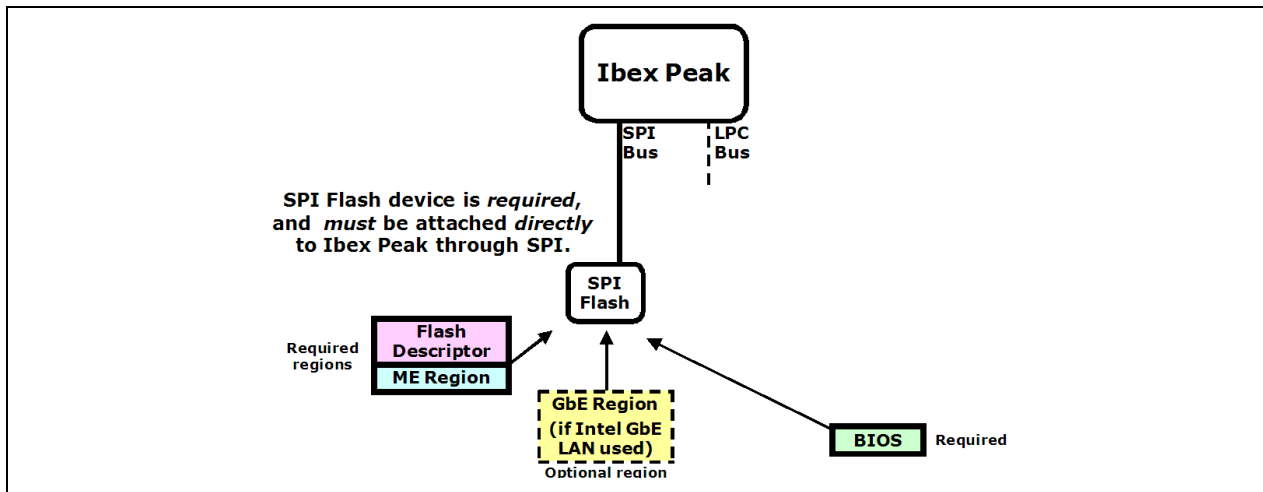
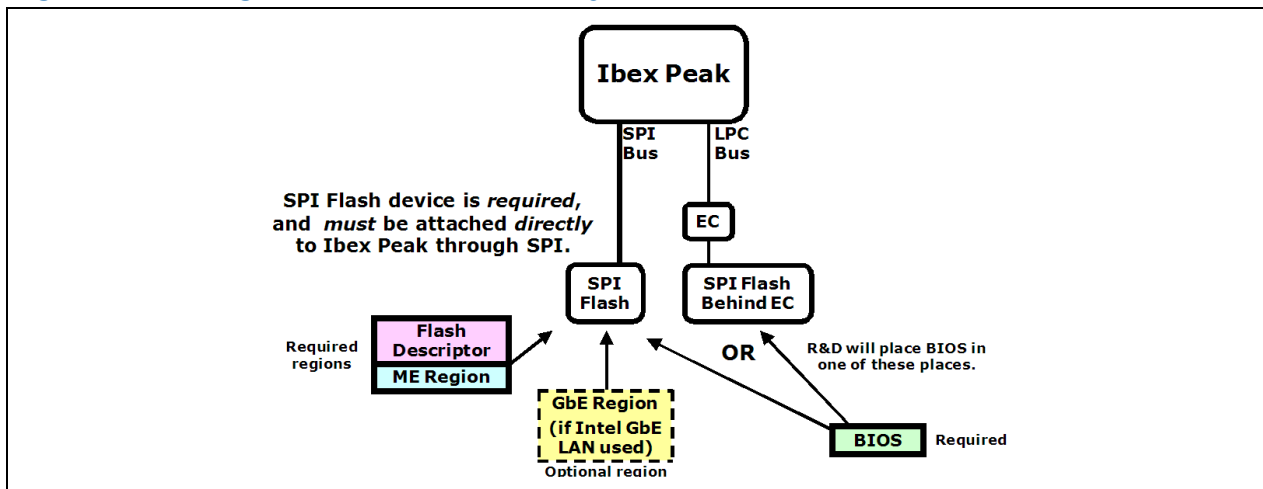


Figure 7-3. Configuration “B” — Mobile Only



Flash Configurations

Figure 7-4. Configuration “C” — Desktop/Server/Workstation Only

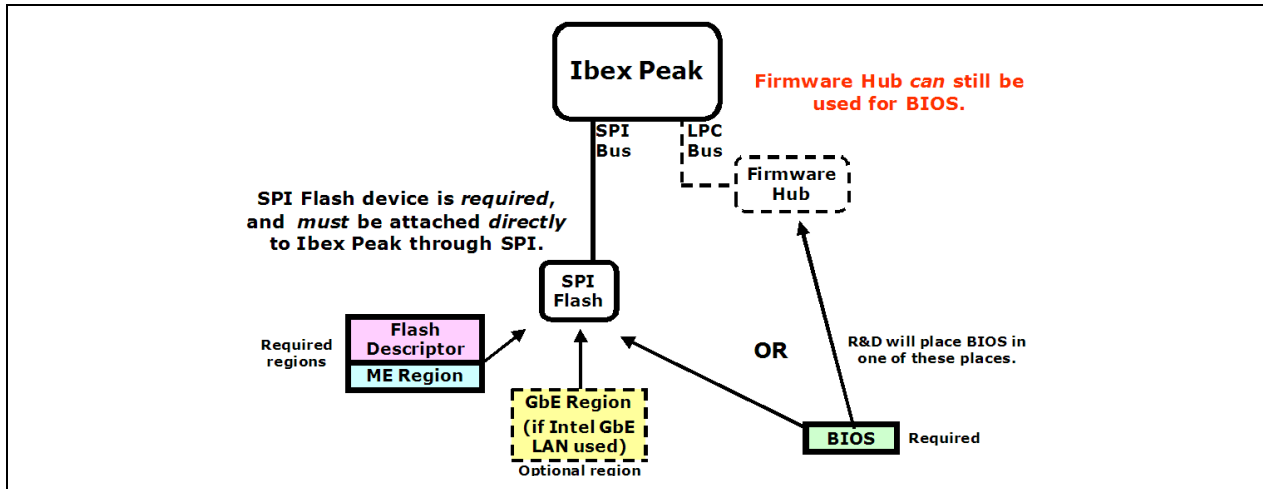
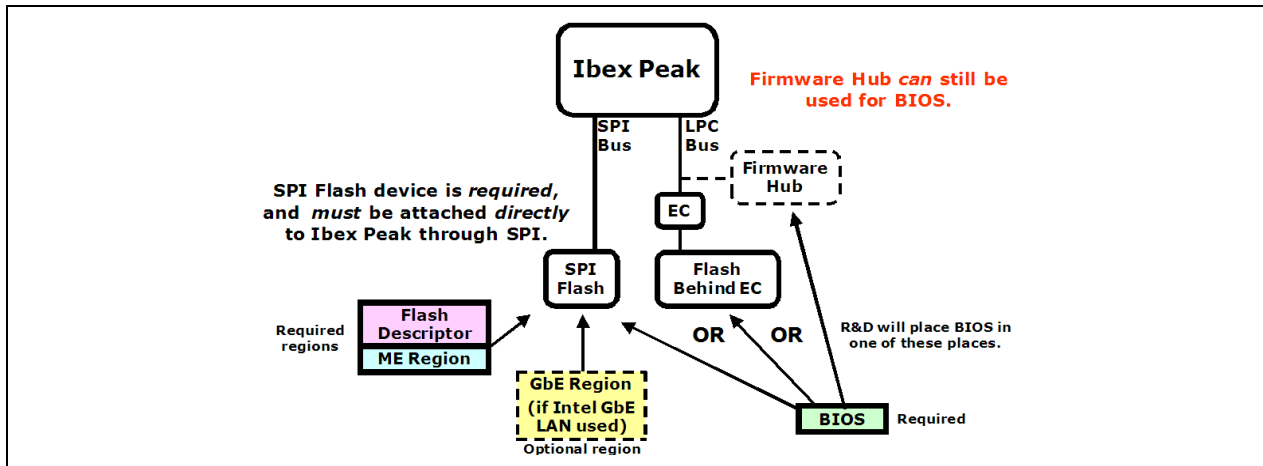


Figure 7-5. Configuration “D” — Mobile Only





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 7-13. 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 <u>NOT</u> Allowed	Local Firmware Updates <u>NOT</u> Allowed	Local Firmware Updates <u>NOT</u> Allowed
Local FWU Override Counter = -1 (minus one)	Local Firmware Updates Allowed	Local Firmware Updates <u>NOT</u> 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 enter 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.



Configuration Parameter Details

C.3 Si features parameters

These options allow for various debugging features.

Table 7-14. 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.



Configuration Parameter Details

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 7-15. 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
	Sentry Peak Permanently Disabled?	Yes
	Intel® Remote Wake Technology Permanently Disabled?	Yes
	KVM Permanently Disabled?	No
	Braidwood Technology Permanently Disabled?	No
	TLS Permanently Disabled?	No
	Intel® Manageability Application Enable / Disable	Enabled
	PAVP 1.5 Enable / Disable	Enabled
	Intel® QST Enable / Disable	Enabled
	Sentry Peak 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
	Sentry Peak Permanently Disabled?	No
	Intel® Remote Wake Technology Permanently Disabled?	No
	KVM Permanently Disabled?	No
	Braidwood Technology Permanently Disabled?	No
	TLS Permanently Disabled?	No
	Intel® Manageability Application Enable / Disable	Enabled
	PAVP 1.5 Enable / Disable	Enabled
	Intel® QST Enable / Disable	Enabled
	Sentry Peak 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
	Sentry Peak Permanently Disabled?	No
	Intel® Remote Wake Technology Permanently Disabled?	No
	KVM Permanently Disabled?	Yes



Configuration Parameter Details

SKU	Feature	Default Value
	Braidwood Technology Permanently Disabled?	Yes
	TLS Permanently Disabled?	No
	Intel® Manageability Application Enable / Disable	Enabled
	PAVP 1.5 Enable / Disable	Enabled
	Intel® QST Enable / Disable	Enabled
	Sentry Peak Enable / Disable	Enabled
	Intel® Remote Wake Technology Enable / Disable	Enabled
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
	Sentry Peak Permanently Disabled?	Yes
	Intel® Remote Wake Technology Permanently Disabled?	Yes
	KVM Permanently Disabled?	No
	Braidwood Technology Permanently Disabled?	No
	TLS Permanently Disabled?	No
	Intel® Manageability Application Enable / Disable	Enabled
	PAVP 1.5 Enable / Disable	Enabled
	Intel® QST Enable / Disable	Disabled
	Sentry Peak Enable / Disable	Disabled
	Intel® Remote Wake Technology Enable / Disable	Disabled
Intel® QS57	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
	Sentry Peak Permanently Disabled?	Yes
	Intel® Remote Wake Technology Permanently Disabled?	Yes
	KVM Permanently Disabled?	No
	Braidwood Technology Permanently Disabled?	No
	TLS Permanently Disabled?	No
	Intel® Manageability Application Enable / Disable	Enabled
	PAVP 1.5 Enable / Disable	Enabled
	Intel® QST Enable / Disable	Disabled
	Sentry Peak Enable / Disable	Disabled
	Intel® Remote Wake Technology Enable / Disable	Disabled
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
	Sentry Peak Permanently Disabled?	No
	Intel® Remote Wake Technology Permanently Disabled?	Yes
	KVM Permanently Disabled?	No



Configuration Parameter Details

SKU	Feature	Default Value
	Braidwood Technology Permanently Disabled?	No
	TLS Permanently Disabled?	No
	Intel® Manageability Application Enable / Disable	Enabled
	PAVP 1.5 Enable / Disable	Enabled
	Intel® QST Enable / Disable	Disabled
	Sentry Peak Enable / Disable	Enabled
	Intel® Remote Wake Technology Enable / Disable	Disabled
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
	Sentry Peak Permanently Disabled?	Yes
	Intel® Remote Wake Technology Permanently Disabled?	Yes
	KVM Permanently Disabled?	Yes
	Braidwood Technology Permanently Disabled?	Yes
	TLS Permanently Disabled?	Yes
	Intel® Manageability Application Enable / Disable	Disabled
	PAVP 1.5 Enable / Disable	Enabled
	Intel® QST Enable / Disable	Disabled
	Sentry Peak Enable / Disable	Disabled
	Intel® Remote Wake Technology Enable / Disable	Disabled
Intel® PM57	Enable Intel® Standard Manageability; Disable Intel® AMT	Yes
	Intel® Manageability Application Permanently Disabled?	No
	PAVP 1.5 Permanently Disabled?	Yes
	Intel® QST Permanently Disabled?	Yes
	Sentry Peak Permanently Disabled?	No
	Intel® Remote Wake Technology Permanently Disabled?	Yes
	KVM Permanently Disabled?	Yes
	Braidwood Technology Permanently Disabled?	No
	TLS Permanently Disabled?	No
	Intel® Manageability Application Enable / Disable	Enabled
	PAVP 1.5 Enable / Disable	Disabled
	Intel® QST Enable / Disable	Disabled
	Sentry Peak Enable / Disable	Enabled
	Intel® Remote Wake Technology Enable / Disable	Disabled
Intel® 3450	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
	Sentry Peak Permanently Disabled?	Yes
	Intel® Remote Wake Technology Permanently Disabled?	Yes
	KVM Permanently Disabled?	No



Configuration Parameter Details

SKU	Feature	Default Value
	Braidwood Technology Permanently Disabled?	No
	TLS Permanently Disabled?	No
	Intel® Manageability Application Enable / Disable	Enabled
	PAVP 1.5 Enable / Disable	Enabled
	Intel® QST Enable / Disable	Enabled
	Sentry Peak 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.

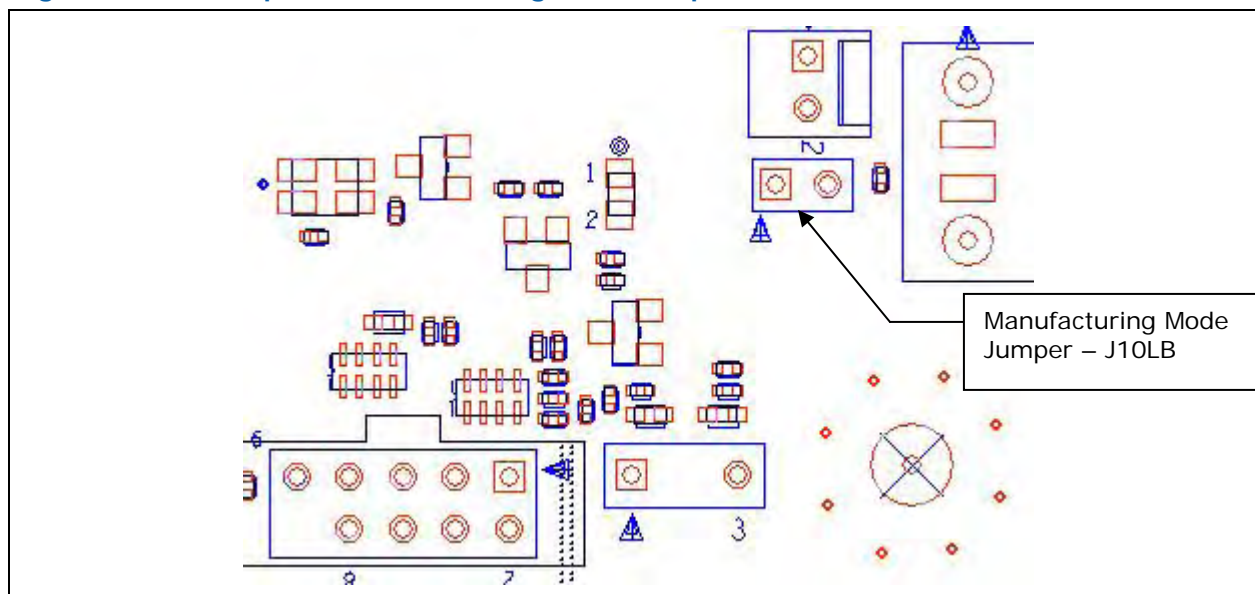
Hash 'x' Stream where 'x' represents one of the 22 possible Remote Configuration Hash entries designates the either the Raw Hash value or certificate file for that Hash entry.

Appendix D – Desktop CRB Information

D.6 Manufacturing Mode Jumper

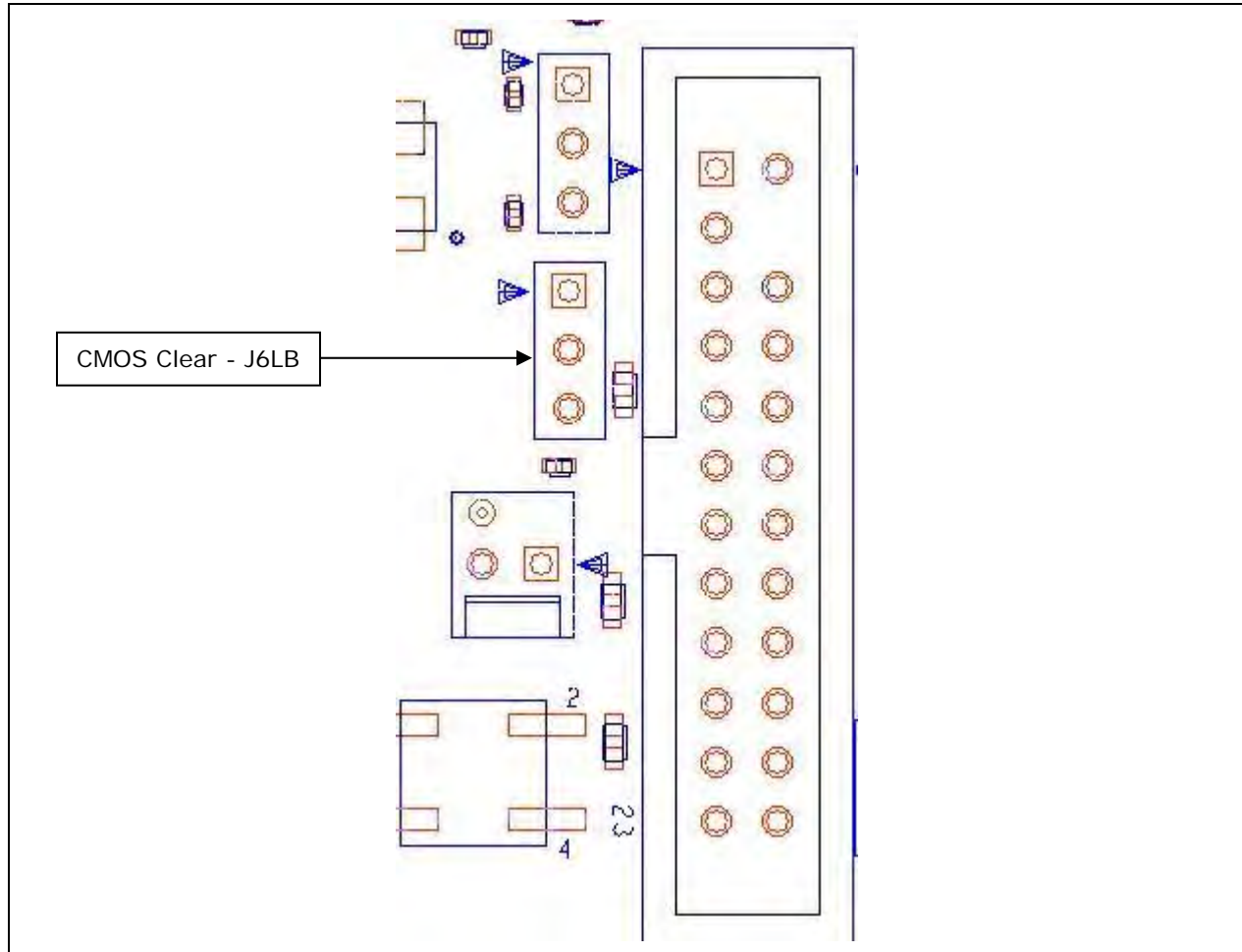
The Manufacturing Mode (Flash Override) jumper permits or denies CPU write access to the SPI flash devices at the hardware level. When this jumper is open, the CPU will not have write access to the flash (if those permissions are not present in firmware). Normally these permissions are set in the firmware 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 7-6. Desktop CRB Manufacturing Mode Jumper Location



D.7 CMOS Clear Jumper

Figure 7-7. Desktop CRB CMOS Clear Location

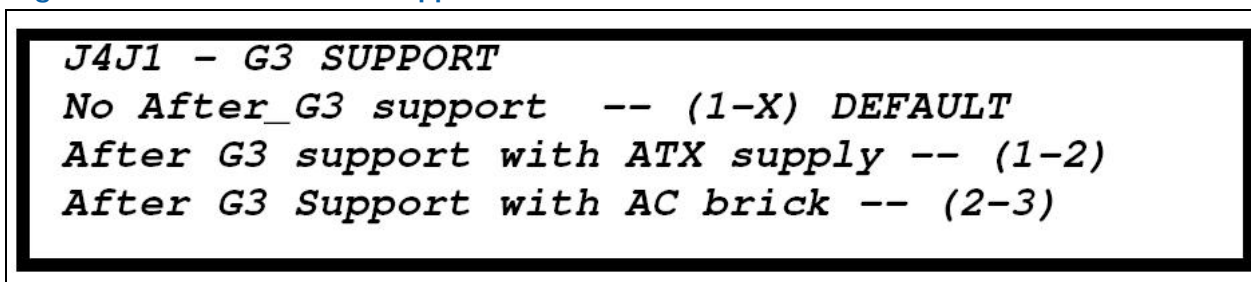


Appendix E – Mobile CRB Information

E.1 Redfort G3 Support

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

Figure 7-8. Redfort CRB G3 Support



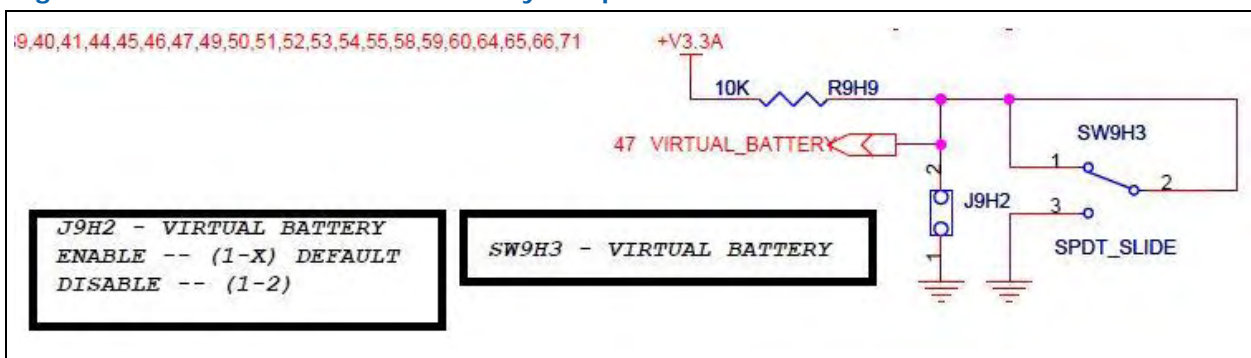
E.2 Redfort Virtual AC / DC Operation

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 7-9. Redfort CRB Virtual Battery Jumper

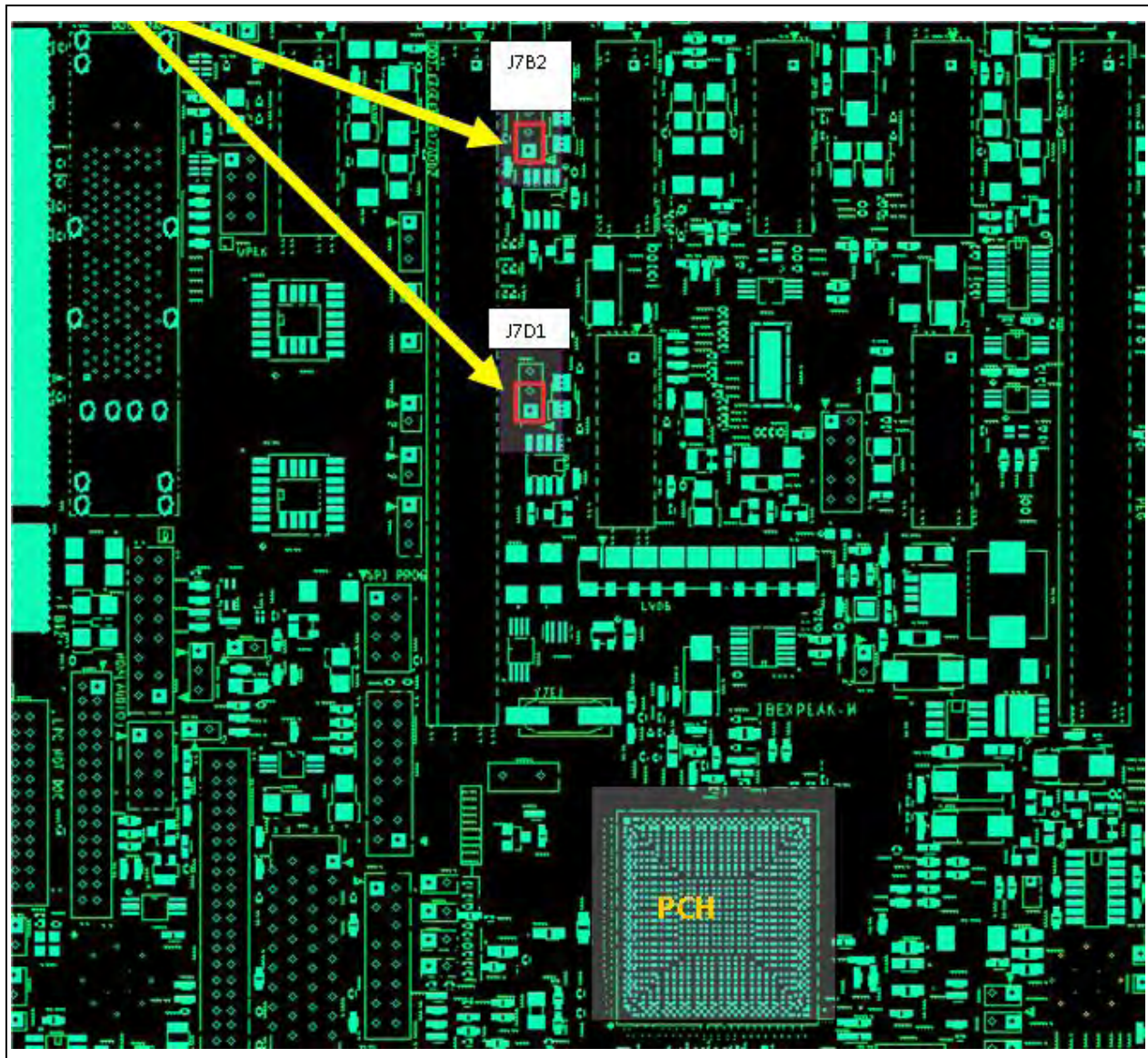


E.3 Redfort Virtual AC / DC Operation

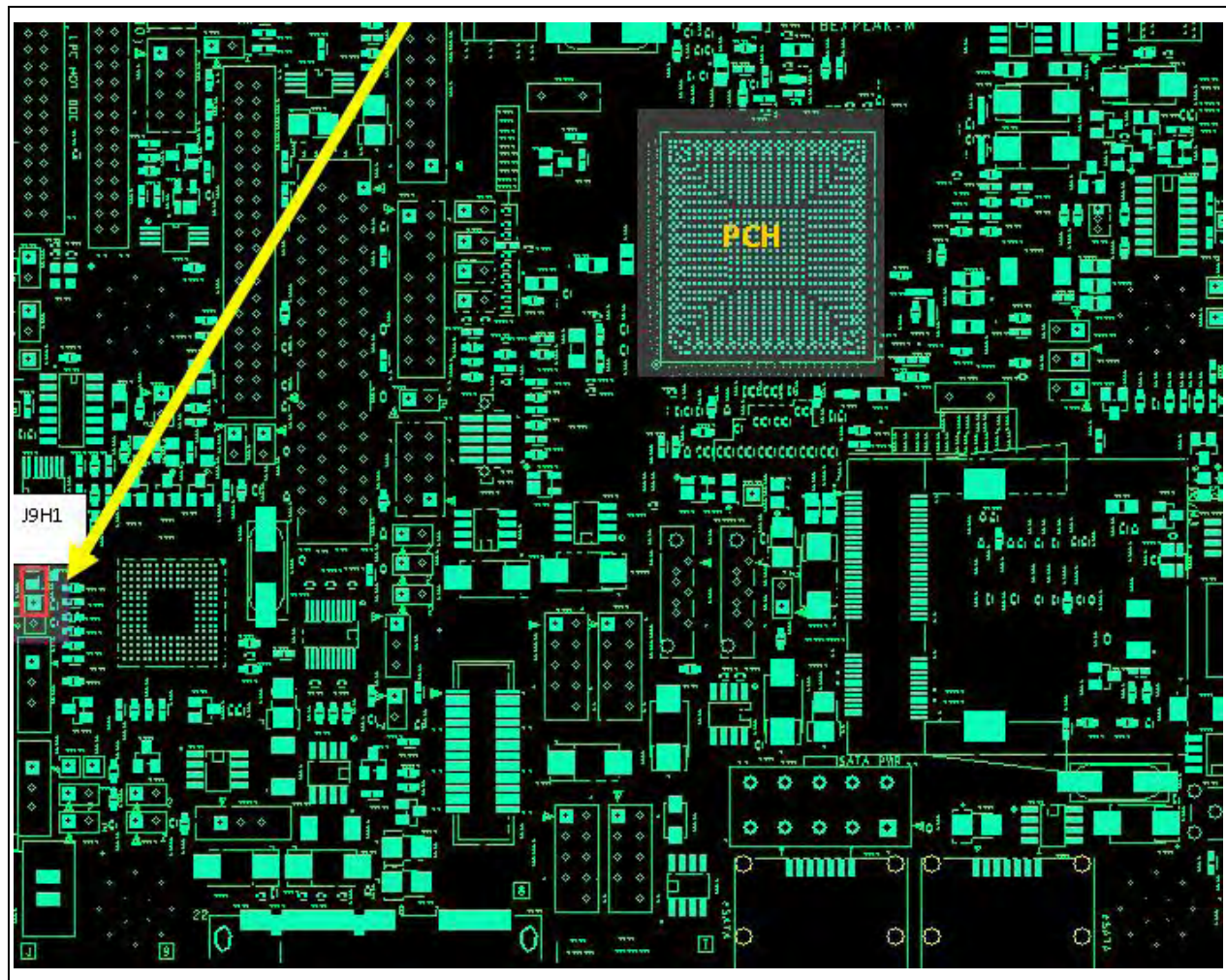
Make sure you are setting the jumpers correctly

- 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 7-10. Redfort ME WLAN Power Control Jumper settings



Mobile CRB Information





Appendix F – Basic Bring-up steps

F.4 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 7-11. 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.