

Elkhart Lake Intel® Converged Security Engine (Intel® CSE) 15.40 Firmware Bring Up

User Guide - NDA

March 2021

Revision 1.3

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.

A "Mission Critical Application" is any application in which failure of the Intel Product could result, directly or indirectly, in personal injury or death. SHOULD YOU PURCHASE OR USE INTEL'S PRODUCTS FOR ANY SUCH MISSION CRITICAL APPLICATION, YOU SHALL INDEMNIFY AND HOLD INTEL AND ITS SUBSIDIARIES, SUBCONTRACTORS AND AFFILIATES, AND THE DIRECTORS, OFFICERS, AND EMPLOYEES OF EACH, HARMLESS AGAINST ALL CLAIMS COSTS, DAMAGES, AND EXPENSES AND REASONABLE ATTORNEYS' FEES ARISING OUT OF, DIRECTLY OR INDIRECTLY, ANY CLAIM OF PRODUCT LIABILITY, PERSONAL INJURY, OR DEATH ARISING IN ANY WAY OUT OF SUCH MISSION CRITICAL APPLICATION, WHETHER OR NOT INTEL OR ITS SUBCONTRACTOR WAS NEGLIGENT IN THE DESIGN, MANUFACTURE, OR WARNING OF THE INTEL PRODUCT OR ANY OF ITS PARTS.

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.

Copies of documents which have an order number and are referenced in this document, or other Intel literature, may be obtained by calling 1-800-548-4725, or go to: <http://www.intel.com/design/literature.htm%20>

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.

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.

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

Copyright © 2021, Intel Corporation. All rights reserved.

Contents

1	Introduction.....	5
1.1	Purpose and Scope of this Document	5
1.2	Acronyms and Definitions	6
1.2.1	General.....	6
1.2.2	Intel® Converged Security Engine.....	8
1.2.3	System States and Power Management.....	9
2	Image Creation: Intel® Flash Image Tool.....	10
2.1	Start Intel® FIT.....	10
2.1.1	Intel® FIT Initial Screen Layout	10
2.1.2	Build Settings	16
2.1.3	Flash Layout Tab	18
2.1.4	Flash Settings Tab	23
2.1.5	Intel® ME Kernel Tab	31
2.1.6	Platform Protection Tab.....	35
2.1.7	Integrated Clock Controller Tab.....	42
2.1.8	Networking & Connectivity Tab.....	47
2.1.9	Internal PCH Buses Tab.....	48
2.1.10	Power Tab	51
2.1.11	Debug Tab.....	53
2.1.12	Compute Die Straps.....	58
2.1.13	Flex I/O Tab	61
2.1.14	GPIO Tab	69
2.1.15	Download and Execute Tab.....	88
2.1.16	Firmware Update Image Build Tab	90
2.2	Build Image in Intel® FIT.....	93
3	Programming SPI Flash Devices and Checking Firmware Status.....	95
3.1	Flash Burner/Programmer.....	95
3.2	Flash Programming Tool (Intel® FPT)	95
3.2.1	Intel® FPT Windows* Version.....	95
3.3	Common Bring Up Issues and Troubleshooting Table	96



Revision History

Revision Number	Description	Revision Date
1.3	<ul style="list-style-type: none">Removed the DnX chapter. For details about DnX image creation requirements and dependencies, refer to the Platform Flash Tool DnX user guide available in the Intel® CSE kit	March 2021
1.2	<ul style="list-style-type: none">Updated Build SettingsRenamed CPU straps to Compute Die StrapsRemoved Camera Tab from Intel® FIT UIUpdated Flash Layout – Intel® SI sub-partitionUpdated default setting for Intel® PTT RSA1K stateUpdated settings for Networking and Connectivity TabRemoved SMBUS Link Configuration from Internal PCH BusesUpdated default values in Flex I/O Tab	January 2021
1.1	<ul style="list-style-type: none">Aligned to Beta Intel® FIT tool 15.40.0.2066	August 2020
1.0	<ul style="list-style-type: none">Updated signing tool value in the build settingsRemoved Intel® Precise Touch and Stylus TabRemoved BTG S3 Optimization parameterUpdated the default value for Thermal Power ReportingUpdated USB3 and USB2 Port Configurations	May 2020
0.9	<ul style="list-style-type: none">Added a note regarding the numbering for Flex I/O USB3 ConfigurationsAdded Descriptor Configuration and Exclusion Ranges in the Platform Protection TabAdded SMx Support to Intel® PTT Configuration	April 2020
0.86	<ul style="list-style-type: none">Updated AcronymsRemoved EC settingsRemoved Camera IPU settings	April 2020
0.85	<ul style="list-style-type: none">Rewrote document.Aligned to EHL PoR with FW boot from SPI onlyAdded Intel® FIT Initial screen layoutAdded details for Intel® FIT Build settingsUpdated all of Intel® FIT settings in the tabs.	March 2020
0.7	<ul style="list-style-type: none">Removed iUNIT configurationRemoved Software re-binding Enabled configuration from flash componentsremoved OEM and Platforms IDs from Flash settingsUpdated Post Manufacturing Lock configurationsUpdated TPM over SPI Bus configurationRemoved ISH sectionRemoved ISH image from Firmware Update configurationsRemoved iUNIT image from Firmware Update configurations	August 2019
0.6	<ul style="list-style-type: none">First Release	January 2019

1 Introduction

1.1 Purpose and Scope of this Document

This document covers the Intel® Converged Security Engine Firmware (Intel® CSE) 15.40 bring up procedure. Intel® CSE is tied to essential platform functionality — this dependency cannot be avoided for engineering reasons.

Note: All CSE Manufacturing Tools within Intel® CSE 15.40 EHL kit are referring to the prefix ME (e.g. MEInfo, MEManuf, etc.). This prefix is being used to keep aligned with other Intel® CSME projects.

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

- **[required]** Descriptor region — Contains sizing information for all other SPI Flash image regions, SPI settings (including Vendor Specific Configuration - or VSCC - tables, SPI device parameters), and region access permissions.
- **[required]** BIOS region — Contains firmware for the processor (or host).
- **[required]** Intel® CSE FW region — Contains firmware for the Intel® Converged Security Engine.

For more details on SPI Flash layout, refer to the Appendix A in this document and the SPI Programming Guide in this kit. Once the SPI Flash image is built, it will be programmed to the target 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® CSE FW is operating as expected.

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

This document makes only the following limited assumptions regarding hardware:

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



1.2 Acronyms and Definitions

1.2.1 General

Acronym/Term	Definition
AR	Anti-Replay
BCLK	Base Clock
BIOS	Basic Input Output System
BIST	Built-in-Self-Test
BSP	Bootstrap Processor
BSSB	Boundary Scan Side-Band
DbC	Debug Class
DCI	Direct Connect Interface
DIMM	Dual In-line Memory Module
DnX	Download and Execute
EC	Embedded Controller
EDS	External Design Specification
EOM	End Of Manufacturing
eSPI	Extended Serial Peripheral Interface
FPF	Field Programmable Fuses
FuSa	Functional Safety
FW	Firmware
GbE	Gigabit Ethernet
GBST	Guided Built in Self Test
GPIO	General Peripheral Input Output
GuC	Generic Micro-Controller
HDCP	High-Bandwidth Digital Content Protection
HECI	Host Embedded Controller Interface (aka Intel® MEI)
IDLM	Intel Device License Module

Acronym/Term	Definition
IFWI	Integrated Firmware Image
Intel® AMT	Intel® Active Management Technology
Intel® CSE	Intel® Converged Security Engine
Intel® FPT	Intel® Flash Programming Tool
Intel® ICCS	Intel® Integrated Clock Controller Service
Intel® MEI	Intel® Management Engine Interface (renamed from HECI)
Intel® PTT	Intel® Platform Trusted Technology
INTEL® SI	Intel® Safety Island
INTEL® SIC	Intel® Safety Island Configuration
IUP	Independent Updateable Partition
LAN	Local Area Network
MCP	Multi-Chip Package (Central Processing Unit / Platform Controller Hub)
MCTP	Management Component Transport Protocol
NVM	Non-Volatile Memory
OEM KM	OEM Key Manifest
OS	Operating System
PAVP	Protected Audio and Video Path
PCH	Platform Controller Hub
PCI	Peripheral Component Interconnect
PCIe*	Peripheral Component Interconnect Express
PDR	Platform Descriptor Region
Intel® PFT	Intel® Platform Flash Tool
PHY	Physical Layer (Networking)
PMC	Power Management Controller
PRTC	Protected Real Time Clock
RPMC	Replay Protection Monotonic Counter
RTC	Real Time Clock
SMBus	System Management Bus
SPI Flash	Flash Serial Peripheral Interface Flash



Acronym/Term	Definition
TPM	Trusted Platform Module
VSCC	Vendor Specific Configuration

1.2.2 Intel® Converged Security Engine

Acronym/Term	Definition
Agent	Software that runs on a client PC with OS running
Host or Host CPU	The processor that is running the operating system. This is different than the management processor running the Intel® CSE
Host Service / Application	An application that is running on the host CPU
INF	An information file (.inf) used by Microsoft* operating systems that supports the Plug & Play feature. When installing a driver, this file provides the OS the necessary information about driver filenames, driver components, and supported hardware.
Intel® MEI	Intel® Management Engine Interface. Interface between the Management Engine and the Host system
Intel® MEI driver	Intel® CSE host driver that runs on the host and interfaces between ISV Agents and the Intel® CSE HW.
Intel® CSE	Intel® Converged Security Engine: The embedded processor residing in the chipset MCP
NVM	Non-Volatile Memory: A type of memory that will retain its contents even if power is removed. In the Intel® CSE current implementation, this is achieved using a FLASH memory device.
System States	Operating System power states such as S0. See detailed definitions in System States and Power Management section.
Un-configured state	The state of the Intel® CSE Firmware when it leaves the OEM factory. At this stage the Intel® CSE Firmware is not functional and must be configured.

1.2.3 System States and Power Management

Acronym/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.
CM0	Intel® CSE firmware power state where all hardware power planes are activated. The host power state is S0.
CM0-PG	Core Well Powered; Intel® CSE Well Powered; (Intel® CSE core not consuming power) DRAM available.
CM3-PG	An Intel® CSE Firmware power state where no power is applied to the Intel® CSE subsystem. (Intel® CSE firmware is shut down).
OS Hibernate	System state where the OS state is saved on the hard drive
S0	A system state where power is applied to all HW devices and the system is running normally.
S1, S2, S3	A system state where the host CPU is halted but power remains available to the memory system (memory is in self-refresh mode).
S4	A system state where the host CPU and memory are not active.
S5	A system state where all power to the host system is off, however the power cord (and/or battery in mobile designs) is still connected.
Shut Down	Equivalent to the S5 state.
Snooze Mode	Intel® CSE activities are mostly suspended to save power. The Intel® CSE monitors HW activities and can restore its activities depending on the HW event.
Standby	System state where the OS state is saved in memory and resumed from the memory when mouse/keyboard is clicked.
Sx	All S states which are different than S0.



2 Image Creation: Intel® Flash Image Tool

Intel® Flash Image Tool (Intel® FIT) can be used to generate a full SPI Flash binary image with Descriptor, BIOS, and Intel® CSE Regions. Additionally, it can be used to create a simple image containing only the Intel® CSE Region only for use with custom SPI Flash binary image assembly solutions. Use the steps shown in following sections.

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

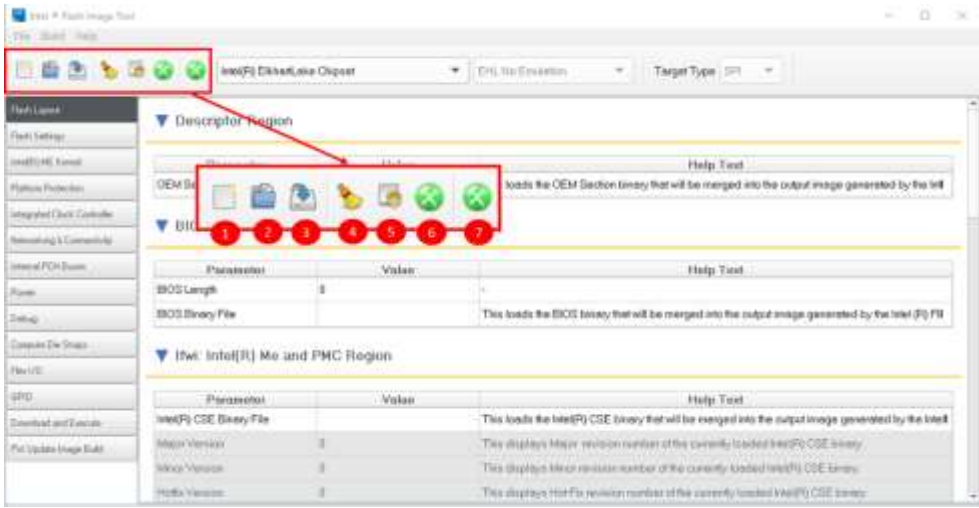
Note: Intel® Flash Image Tool (Intel® FIT) may be updated throughout the release cycles. As a general rule, please make sure to use the tools, images and other content from the same kit and refrain from using different version tools.

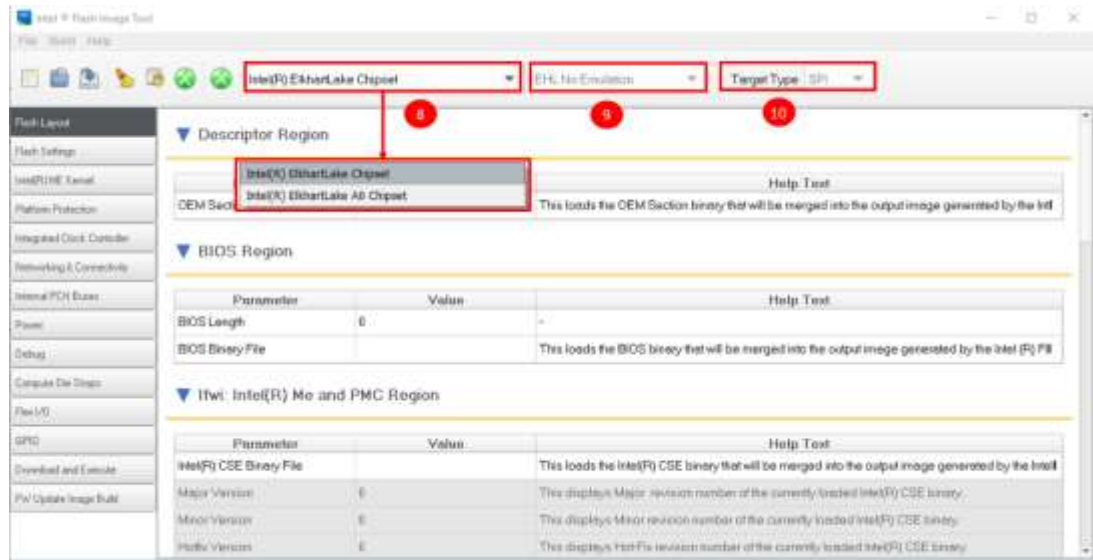
2.1 Start Intel® FIT

Invoke Intel® Flash Image Tool. Using Explorer*, navigate to **[root]\Tools\System Tools\Flash Image Tool**. Verify that the directory contents are correct. Double-click **FIT.exe**.

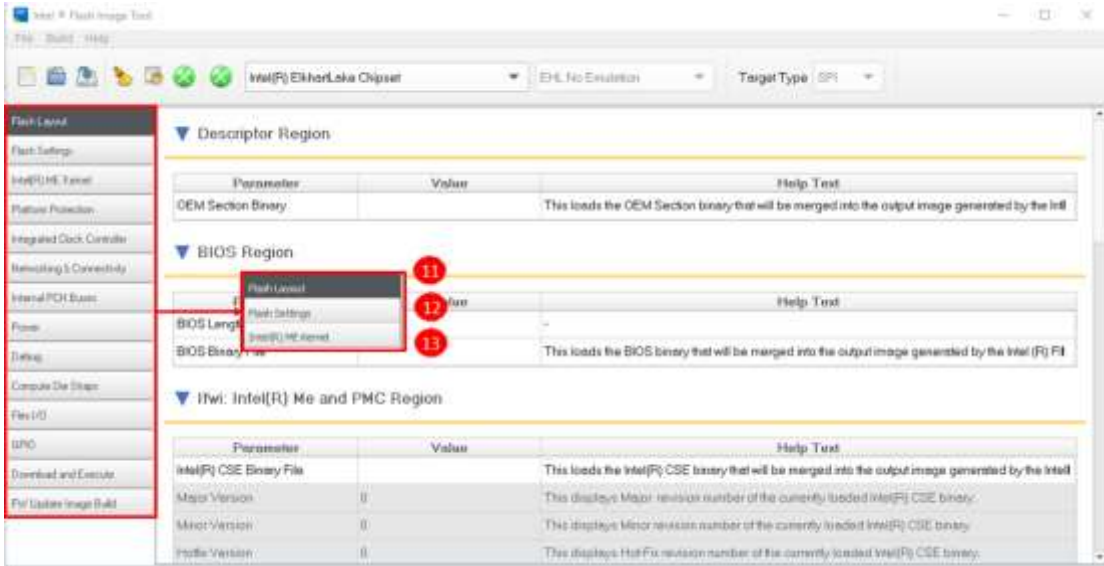
2.1.1 Intel® FIT Initial Screen Layout

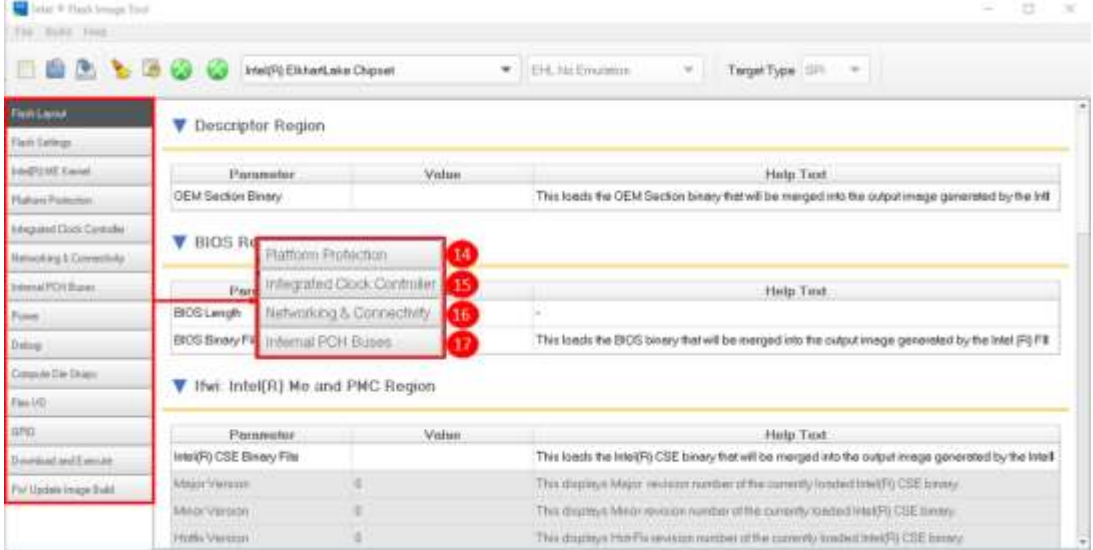
See the table below with details on all settings shown in the initial Intel® FIT screen layout.

Initial Screen Layout		
#	Label	Contents
		
1	New	This button labeled 'New' on rollover allows opening of a new session with default values

Initial Screen Layout		
#	Label	Contents
2	Open	This button labeled 'Open' on rollover allows opening of an xml or bin file
3	Save	This button labeled 'Save' on rollover allows saving of xml file
4	Clear Console	This button labeled 'Clear Console' clears the console area
5	Build Settings	This button labeled 'Build Settings' brings up the build settings popup Window
6	Build Image	This button labeled 'Build Image' on rollover allows build of the image
7	Build Image for FWUpdate	This button labeled 'Build Image for FWUpdate allows the user to build separate firmware update binaries.
		
8	Drop Down Selector	This drop down allows selection of platform
9	Drop Down Selector	This drop down allows selection of SKU within platform selected
10	Indicator	This displays the type of Boot Media Target based on FW being used

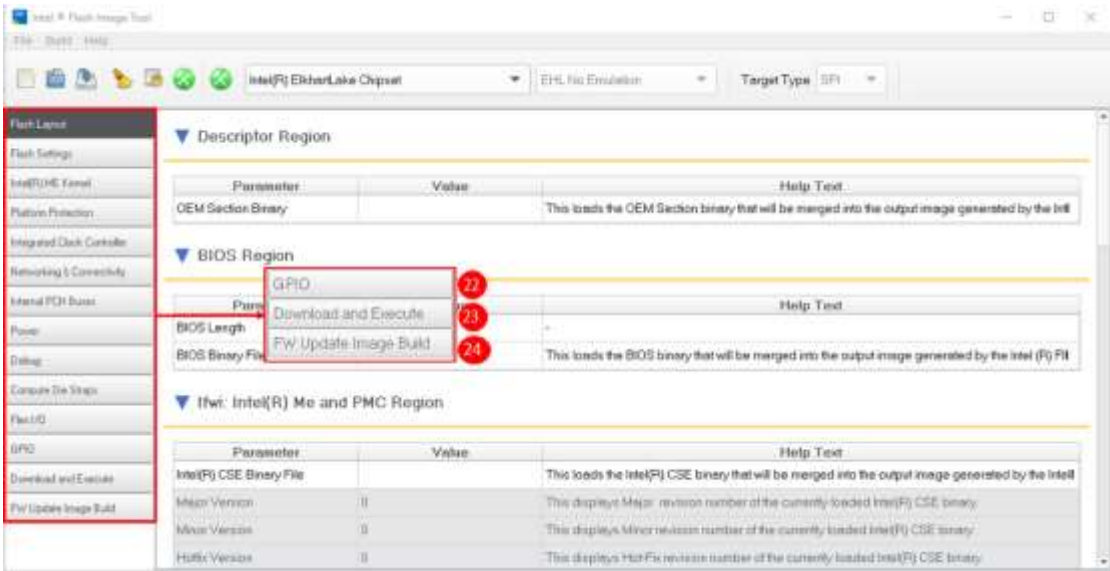


Initial Screen Layout		
#	Label	Contents
		
11	Flash Layout Tab	<ul style="list-style-type: none"> • Descriptor Region • BIOS Region • Intel® CSE and PMC Region • Sub-partitions • PDR
12	Flash Settings Tab	<ul style="list-style-type: none"> • Flash Components • Host CPU/ BIOS Master Access • Intel® CSE Master Access • Flash Configuration • Legacy VSCC Table - VSCC Entries • BIOS Configuration • FPF Configuration • RPMC Configuration
13	Intel® ME Kernel Tab	<ul style="list-style-type: none"> • Intel® ME Firmware Update • Image Identification • Firmware Diagnostics • End of Manufacturing Configuration • Intel® CSE Boot Configuration • Intel® ME Measured Boot Configuration • Intel® CSE Assisted Boot Configuration

Initial Screen Layout		
#	Label	Contents
		
14	Platform Protection Tab	<ul style="list-style-type: none"> Content Protection Graphics uController Hash Key Configuration for Bootguard Descriptor Configuration Exclusion Ranges Boot Guard Configuration Intel® PTT Configuration TPM Over SPI Bus Configuration FuSa Configuration
15	Integrated Clock Controller Tab	<ul style="list-style-type: none"> Integrated Clock Controller Policies
16	Networking & Connectivity Tab	<ul style="list-style-type: none"> Gigabit and Time Sensitive Networking Configuration
17	Internal PCH Buses Tab	<ul style="list-style-type: none"> PCH Timer Configuration eSPI Configuration



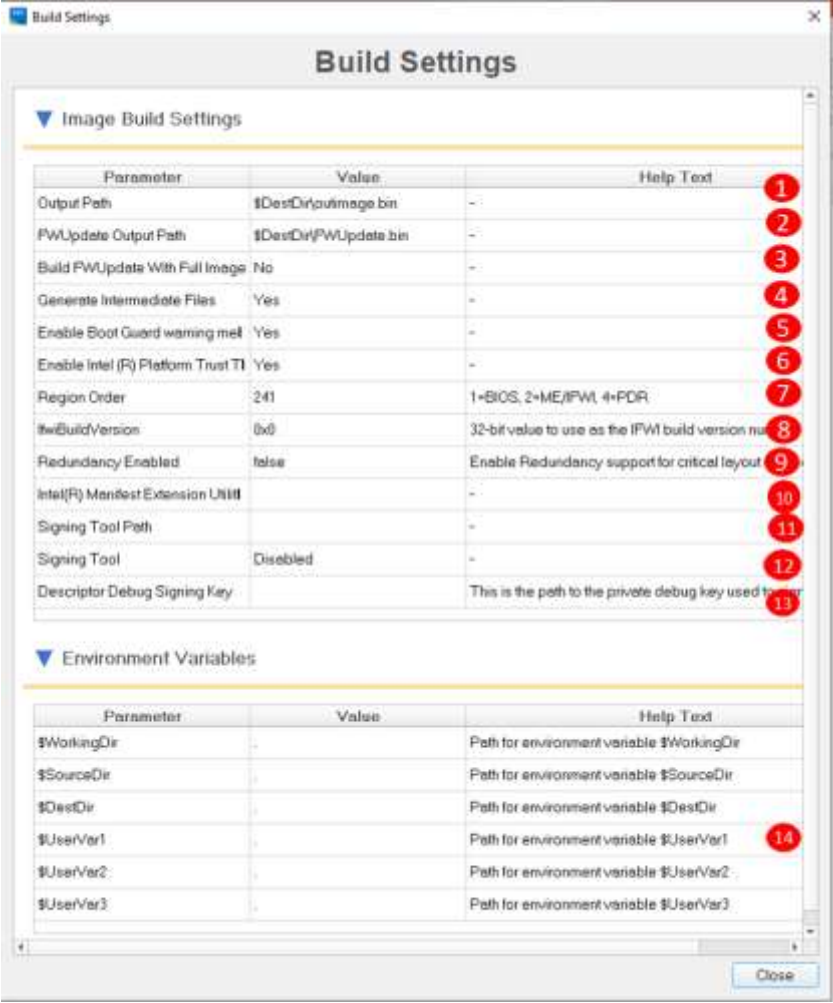
Initial Screen Layout		
#	Label	Contents
18	Power Tab	<ul style="list-style-type: none"> Platform Power PCH Thermal Reporting
19	Debug Tab	<ul style="list-style-type: none"> IDLM Delayed Authentication Mode Configuration Intel® Trace Hub Technology Intel® ME Firmware Debugging Overrides Direct Connection Interface Configuration eSPI Feature Overrides Early USB DBC over Type-A Configuration TRC Emulation
20	CPU Straps Tab	<ul style="list-style-type: none"> Compute Die Straps
21	Flex I/O Tab	<ul style="list-style-type: none"> PCIe Lane Reversal Configuration PCIe Port Configuration PCIe Multi VC Port Configuration SATA / PCIe Combo Port Configuration USB3 Port Configuration USB2 Port Configuration UFS Port Configuration M.2 Pullup Configuration Power Delivery (PD) Controller Configuration

Initial Screen Layout		
#	Label	Contents
		
22	GPIO Tab	<ul style="list-style-type: none"> GPIO VCCIO Voltage Control
23	Download and Execute	<ul style="list-style-type: none"> DnX Image DnX Fuses
24	FW Update Image Build	<ul style="list-style-type: none"> ME Image PMC Image OEM KM Image PCHC Image INTEL® SI Image and Configuration file FuSa Image
	Console Window Area	Displays opening messages, log file entries, and build activity messages



2.1.2 Build Settings

Click on The Build Button in the top menu bar, select build settings option. The table below provides details for all the displayed settings.

Build Settings			
#	Parameter	Default Value	Values
			
1	Output Path	Same folder as Intel® FIT tool	Double click to the right of outimage.bin and click to get browse button to specify path and name of file to create for the build
2	FWUpdate Output Path	Same folder as Intel® FIT tool	Double click to the right of FWUpdate.bin and click to get browse button to specify path and name of file to create for the build
3	Build FWUpdate With Full Image	No	Yes/No

Build Settings			
#	Parameter	Default Value	Values
4	Generate Intermediate Files	Yes	Yes/No
5	Enable Boot Guard warning message at build time	Yes	Yes/No
6	Enable Intel® Platform Trust Technology warning message at build time	Yes	Yes/No
7	Region Order	53241	
8	IFWI Build Version		32-bit value to use as the IFWI build version number.
9	Redundancy Enabled	false	This setting enabled Redundancy support for critical layout components
10	Intel® Manifest Extension Utility Path		
11	Signing Tool Path		
12	Signing Tool	Disabled	
13	Descriptor Debug Signing Key		Path to the private debug key used to sign the descriptor, while public key hash of it is included in the OEM hash manifest. This setting is operative only when FDV is enabled.
14	Environment Variables		\$WorkingDir and \$DestDir can be left at the default `.` Click on \$SourceDir Value field and type in path where the Image Components are located for the CSE kit



2.1.3 Flash Layout Tab

Click on Flash Layout in the left tabs' menu. All regions are expanded by default. See the table below.

Flash Layout Tab											
<div> <div>▼ Descriptor Region</div> <table> <tr> <th>Parameter</th><th>Value</th><th>Help Text</th></tr> <tr> <td>OEM Section Binary</td><td></td><td>This loads the OEM Section binary that will be merged into the output</td></tr> </table> </div>			Parameter	Value	Help Text	OEM Section Binary		This loads the OEM Section binary that will be merged into the output			
Parameter	Value	Help Text									
OEM Section Binary		This loads the OEM Section binary that will be merged into the output									
#	Parameter	Settings									
1	OEM Section Binary This loads the OEM Section binary that will be merged into the output image generated by the Intel® FIT tool.	OEM Binary (optional)									
<div> <div>▼ BIOS Region</div> <table> <tr> <th>Parameter</th><th>Value</th><th>Help Text</th></tr> <tr> <td>Length</td><td>0</td><td>-</td></tr> <tr> <td>BIOS Binary File</td><td></td><td>This loads the BIOS binary that will be merged into the output image</td></tr> </table> </div>			Parameter	Value	Help Text	Length	0	-	BIOS Binary File		This loads the BIOS binary that will be merged into the output image
Parameter	Value	Help Text									
Length	0	-									
BIOS Binary File		This loads the BIOS binary that will be merged into the output image									
#	Parameter	Settings									
2	BIOS Region										
	Length -This displays the length of the BIOS binary. Note: This value will be automatically populated by Intel® FIT during image build.										
	BIOS Binary File Navigate to path to load bios.rom file. This loads the BIOS binary that will be merged into the output image generated by the Intel® FIT tool.	biosimage.bin									

Flash Layout Tab		
<div> <div>▼ Ifwi: Intel(R) Me and Pmc Region</div> <div>3</div> </div>		
Parameter	Value	
Intel(R) ME Binary File		This loads the Intel(R) ME binary that will be merged into the
Major Version	0	This displays Major revision number of the currently loaded
Minor Version	0	This displays Minor revision number of the currently loaded
Hotfix Version	0	This displays Hot-Fix revision number of the currently loaded
Build Version	0	This displays Build version number of the currently loaded
Chipset Initialization Version		This displays the current Chipset Initialization version contain
Chipset Initialization Binary		This loads the Chipset Initialization binary that will be merged
ChipsetInit Override Version		This displays the version of the Chipset Initialization Binary ove
PMC Binary File		This loads the PMC binary that will be merged into the output
PMC Length	0x30000	-
Version		-

#	Parameter	Settings
3	Intel® ME and PMC Region	
	Intel® ME Binary File Navigate to your Source Directory and switch to the CSE subdirectory. Choose the appropriate Intel CSE Firmware binary image. This loads the Intel® CSE binary that will be merged into the into the output image generated by the Intel® FIT tool. Note: You may choose to build the Intel® CSE Region only. To do so, the Number of Flash Components in Flash Settings> Flash Components must be set to 0. Note: If loading cse_image.bin file, check that the ME region is enabled in the tool before building the image.	cse_image.bin
	Major Version - This displays Major revision number of the currently loaded Intel® CSE binary.	
	Minor Version - This displays Minor revision number of the currently loaded Intel® CSE binary.	
	Hotfix Version - This displays Hot-Fix revision number of the currently loaded Intel® CSE binary.	
	Build Version - This displays Build version number of the currently loaded Intel® CSE binary.	
	Chipset Initialization Version - This displays the current Chipset Initialization version contained in the currently loaded Intel® CSE binary.	



Flash Layout Tab														
	<p>Chipset Initialization Binary - This loads the Chipset Initialization binary that will be merged into the output image generated by the Intel® FIT. If specified, this will override the version contained in the Intel® CSE binary.</p> <p>Note: When BIOS passes new Chipset Initialization settings to CSE, a Global Reset is initiated (only required on the first boot, subsequent boots will not incur a global reset). This allows for the new settings to be stored in the CSE Region and programmed into the PCH. This global reset can be avoided by loading the proper chipset initialization binary into the CSE Region when building the image that aligns with the values in BIOS. The Chipset Initialization Binary will be included in BIOS RC package. If BIOS contains an older version of Chipset Initialization settings, CSE will be updated at boot with the older settings regardless of any newer settings being present in firmware. In order to avoid this problem and the additional Global Reset customers should ensure that both BIOS and CSE are updated with same Chipset Initialization binary.</p>	Chipset.bin (Mandatory)												
	ChipsetInit Override Version - This displays the version of the Chipset Initialization Binary override if specified.													
	PMC Binary File - This loads the PMC binary that will be merged into the output image generated by the Intel® FIT tool.	PMC.bin												
	<p>PMC Length - This displays the length of the PMC binary.</p> <p>Note: This value will be automatically populated by Intel® FIT during image build.</p>													
	Version - This displays the version of PMC													
<div> <div>▼ PCH Configuration Sub-Partition</div> <div>4</div> <table> <thead> <tr> <th>Parameter</th><th>Value</th><th></th></tr> </thead> <tbody> <tr> <td>PCH Configuration File</td><td></td><td>This loads the PCH Configuration binary that will be merged in</td></tr> <tr> <td>Version</td><td></td><td>-</td></tr> <tr> <td>Length</td><td>0x1000</td><td>-</td></tr> </tbody> </table> </div>			Parameter	Value		PCH Configuration File		This loads the PCH Configuration binary that will be merged in	Version		-	Length	0x1000	-
Parameter	Value													
PCH Configuration File		This loads the PCH Configuration binary that will be merged in												
Version		-												
Length	0x1000	-												
#	Parameter	Settings												
4	PCH Configuration Sub-Partition													
	<p>PCH Configuration File</p> <p>This loads the PCH Configuration binary that will be merged into the output image generated by the Intel® FIT tool.</p>	PCHC.bin												
	Version - This displays the version number of the PCHC Configuration Sub-Partition													

Flash Layout Tab

Length - This displays the length of the PCH Configuration Sub-Partition.

Note: This value will be automatically populated by Intel® FIT during image build.

ISI FW Sub-Partition

5

Parameter	Value	Help Text
ISI FW File		This loads the ISI FW binary that will be merged into the output image generated by Intel® FIT tool.
Length	0x40000	-
ISI Configuration File		Path of ISI configuration binary

#	Parameter	Settings
5	INTEL® SI FW Sub-Partition	
	INTEL® SI FW File This loads the INTEL® SI FW binary that will be merged into the output image generated by the Intel® FIT tool.	INTEL® SI.bin
	Length - This displays the length of the INTEL® SI FW Sub-Partition. Note: This value will be automatically populated by Intel® FIT during image build.	
	INTEL® SI Configuration File This loads the INTEL® SI Configuration binary that will be merged into the output image generated by Intel® FIT tool	

FuSa Proof Test Configuration Sub-Partition

6

Parameter	Value	Help Text
FuSa Proof Test Configuration I		This loads the FuSa Proof Test Configuration binary that will be merged i
FuSa Proof Test Version		-
FuSa Proof Test Length	0x8000	-

#	Parameter	Settings
6	Fusa Proof Test Configuration Sub-Partition This loads the Fusa Proof Test Configuration binary that will be merged in the output image generated by the Intel® FIT tool. Note: Used to enable FuSa safety standards.	
	Fusa Proof Test Configuration File Navigate to path to load FuSa.bin file. This loads the FuSa Configuration binary.	FuSa.bin (Optional)
	Version - This displays the version number of the Fusa Proof Test Configuration Sub-Partition	



Flash Layout Tab														
	<p>Length - This displays the length of the Fusa Proof Test Configuration Sub-Partition.</p> <p>Note: This value will be automatically populated by Intel® FIT during image build.</p>													
<div> <div>PDR Region</div> <div>7</div> <table> <tr> <th>Parameter</th><th>Value</th><th>Help</th></tr> <tr> <td>Length</td><td>0</td><td></td></tr> <tr> <td>PDR Binary File</td><td></td><td>This loads the Platform Data region binary that i</td></tr> <tr> <td>PDR Region Enable</td><td>Disabled</td><td>This option allows the user to enable or disable</td></tr> </table> </div>			Parameter	Value	Help	Length	0		PDR Binary File		This loads the Platform Data region binary that i	PDR Region Enable	Disabled	This option allows the user to enable or disable
Parameter	Value	Help												
Length	0													
PDR Binary File		This loads the Platform Data region binary that i												
PDR Region Enable	Disabled	This option allows the user to enable or disable												
#	Parameter	Settings												
7	<p>PDR Region - This loads the Platform Data region binary that will be merged into the output image generated by the Intel® FIT tool.</p>													
	<p>Length Region is disabled by default. Displays Region size information when Binary input file is specified.</p>													
	<p>PDR Binary File Navigate to path to load pdrimage.bin file if required and available. This loads the Platform Data region binary that will be merged into the output image generated by the Intel® FIT tool.</p>	PDR.bin (Optional)												
	<p>PDR Region Enable Values: Enabled/Disabled - This option allows the user to enable or disable the Platform Data Region. Note: If loading PDR.bin file, check that the PDR region is enabled in tool before building image.</p>	Disabled												

2.1.4 Flash Settings Tab

Click on Flash Settings in the left tabs' menu. All regions are expanded by default. See the table below.

Flash Settings Tab		
<div> <div>Flash Components</div> <div>1</div> </div>		
Parameter	Value	Help
Number of Flash Components	1	Specifies the number of Flash components that will be used.
Flash component 1 Size	16MB	This field identifies the size of the 1st Flash component.
Flash component 2 Size	8MB	This field identifies the size of the 2nd Flash component.
SPI Global Protected Range	0x0	Sets the default value of the Global Protected Range register.
SPI Idle to Deep Power Down Timeout Default Spec	0x5	SPI Idle to Deep Power Down Timeout Default Specification.
SPI Out of Order operation Enabled	Yes	When this setting is enabled priority operations may be performed out of order.
SPI Resume Hold-off Delay	8us	Specifies the time after the completion of a priority operation before the SPI controller resumes normal operation.
SPI Max write / erase Resume Delay	No Ceiling	This setting specifies the maximum value for the write/erase resume delay.
SPI Suspend / Resume Enabled	Yes	When this setting is enabled writes and erases may be suspended and resumed.

#	Parameter	Settings
1	Flash Components	
	Number of Flash Components Values: 0, 1, 2 - This setting configures the total number of flash components for the platform. Note: Choosing a selection of '0' part will cause the Intel® FIT tool to build an output image containing only the Intel® CSE region.	1
	Flash component 1 Size Values: 512KB, 1MB, 2MB, 4MB, 8MB, 16MB, 32MB, 64MB - This setting determines the size of Flash component 1 for the platform image.	32MB
	Flash component 2 Size Values: 512KB, 1MB, 2MB, 4MB, 8MB, 16MB, 32MB, 64MB - This setting determines the size of Flash component 2 for the platform image. Note: This setting is only applicable when the Number of Flash Components option is set to '2'.	Greyed Out
	SPI Global Protected Range - This sets the default value of the Global Protected Range register in the SPI Flash Controller.	0x0



Flash Settings Tab																	
	SPI Idle to Deep Power Down Timeout - This sets SPI Idle to Deep Power Down Timeout Default Specifies the time in microseconds that the Flash Controller waits after all activity is idle before commanding the flash devices to Deep Power down, time = 2^N microseconds.	0x5															
	SPI Out of Order operation Enabled - When this setting is enabled priority operations may be issued while waiting for write / erase operations to complete on the flash device. When this setting is disabled all write / erase type operations in order.	Yes															
	SPI Resume Hold-off Delay - This specifies the time after the completion of a pri_op before the flash controller sends the resume instruction. If a new pri_op is eligible to be issued prior to the end of this delay time then the pri_op is issued and the timer is reinitialized to tRHD. 3-bit field encodes count with range 0-7. tRHD = count * 2us.	8us															
	SPI Max write / erase Resume to Suspend intervals - This setting specifies the maximum value for the write and erase Resume to Suspend intervals.	No Ceiling															
	SPI Suspend / Resume Enabled - When this setting is enabled writes and erases may be suspended to allow a read to be issued on the flash device. When this setting is disabled no transaction will be allowed to the busy flash device.	Yes															
<div> <div>▼ Host CPU / BIOS Master Access</div> <div>2</div> </div> <table> <thead> <tr> <th>Parameter</th><th>Value</th><th></th></tr> </thead> <tbody> <tr> <td>Host CPU / BIOS Write Access Intel Recommended</td><td>0xFFFF</td><td>This setting determines write acc</td></tr> <tr> <td>Host CPU / BIOS Write Access Custom</td><td>0x0000</td><td>This setting determines write acc</td></tr> <tr> <td>Host CPU / BIOS Read Access Intel Recommended</td><td>0xFFFF</td><td>This setting determines read acc</td></tr> <tr> <td>Host CPU / BIOS Read Access Custom</td><td>0x0000</td><td>This setting determines read acc</td></tr> </tbody> </table>			Parameter	Value		Host CPU / BIOS Write Access Intel Recommended	0xFFFF	This setting determines write acc	Host CPU / BIOS Write Access Custom	0x0000	This setting determines write acc	Host CPU / BIOS Read Access Intel Recommended	0xFFFF	This setting determines read acc	Host CPU / BIOS Read Access Custom	0x0000	This setting determines read acc
Parameter	Value																
Host CPU / BIOS Write Access Intel Recommended	0xFFFF	This setting determines write acc															
Host CPU / BIOS Write Access Custom	0x0000	This setting determines write acc															
Host CPU / BIOS Read Access Intel Recommended	0xFFFF	This setting determines read acc															
Host CPU / BIOS Read Access Custom	0x0000	This setting determines read acc															
#	Parameter	Settings															
2	Host CPU/ BIOS Master Access	For more details on Region Access Control, refer to the SPI Programming guide															
	Host CPU / BIOS Write Access Intel Recommended Values: 0xFFFF, 0x000A, 0x001A, 0x010A, 0x011A - This setting determines write access control for the BIOS region. 0xFFFF = Debug/Manufacturing 0x000A = Production 0x001A = Production with access to PDR (should ONLY be used if PDR region is implemented). Custom = User custom Host / BIOS Write Access values	0xFFFF															

Flash Settings Tab

	<p>Host CPU / BIOS Write Access Custom - This setting allows free form user customized Host CPU / BIOS Write Access regions permissions</p> <p>Note: This setting is grayed out unless Custom is selected under the Host CPU / BIOS Write Access Intel Recommended drop down menu.</p> <p>Warning: Setting region access permission values outside of Intel recommendation could result in compromised platform security</p>	Hex Input
	<p>Host CPU / BIOS Read Access</p> <p>Values: 0xFFFF, 0x000F, 0x001F, 0x010F, 0x011F - This setting determines read access control for the BIOS region.</p> <p>0xFFFF = Debug/Manufacturing</p> <p>0x000F = Production</p> <p>0x001F = Production with access to PDR (should ONLY be used if PDR region is implemented).</p> <p>Custom = User custom Host / BIOS Read Access values</p>	0xFFFF
	<p>Host CPU / BIOS Read Access Custom - This setting allows free form user customized Host CPU / BIOS Read Access regions permissions</p> <p>Note: This setting is grayed out unless Custom is selected under the Host CPU / BIOS Read Access Intel Recommended drop down menu.</p> <p>Warning: Setting region access permission values outside of Intel recommendation could result in compromised platform security</p>	Hex Input

Intel(R) ME Master Access 3		
Parameter	Value	He
Intel(R) ME Write Access Intel Recommended	0xFFFF	This setting determines write access
Intel(R) ME Write Access Custom	0x0000	This setting determines read access
Intel(R) ME Read Access Intel Recommended	0xFFFF	This setting determines read access
Intel(R) ME Read Access Custom	0x0000	This setting determines read access

#	Parameter	Settings
3	Intel® ME Master Access	
	<p>Intel® ME Write Access Intel Recommended</p> <p>Values: 0xFFFF, 0x0004 - This setting determines write access control for the Intel® CSE region.</p> <p>0xFFFF = Debug/Manufacturing</p> <p>0x0004 = Production</p> <p>0x000C = Production</p> <p>Custom = User custom Intel® CSE Write Access values</p>	0xFFFF



Flash Settings Tab		
	<p>Intel® ME Write Access Custom - This setting allows free form user customized Intel® CSE Write Access regions permissions</p> <p>Note: This setting is grayed out unless Custom is selected under the Intel® ME Write Access Intel Recommended drop down menu.</p> <p>Warning: Setting region access permission values outside of Intel recommendation could result in compromised platform security</p>	Hex Input
	<p>Intel® ME Read Access Intel Recommended</p> <p>Values: 0xFFFF, 0x000D - This setting determines read access control for the Intel® CSE region.</p> <p>0xFFFF = Debug/Manufacturing</p> <p>0x000D = Production</p> <p>Custom = User custom Intel® CSE Read Access values</p>	0xFFFF
	<p>Intel® ME Read Access Custom - This setting allows free form user customized Intel® CSE Read Access regions permissions</p> <p>Note: This setting is grayed out unless Custom is selected under the Intel® CSE Read Access Intel Recommended drop down menu.</p> <p>Warning: Setting region access permission values outside of Intel recommendation could result in compromised platform security</p>	Hex Input

Flash Settings Tab

Flash Configuration

4

Parameter	Value	
Dual I/O Read Enable	No	This soft-strap only has effect if Dual I/O Read
Dual Output Read Enable	No	This soft-strap only has effect if Dual Output Read
Fast Read Clock Frequency	50MHz	This setting allows customers to configure the
Fast Read Supported	Yes	This setting allows customers to enable support
Invalid Instruction 0	0x21	This setting allows customers to configure invalid
Invalid Instruction 1	0x42	This setting allows customers to configure invalid
Invalid Instruction 2	0x60	This setting allows customers to configure invalid
Invalid Instruction 3	0xAD	This setting allows customers to configure invalid
Invalid Instruction 4	0xB7	This setting allows customers to configure invalid
Invalid Instruction 5	0xB9	This setting allows customers to configure invalid
Invalid Instruction 6	0xC4	This setting allows customers to configure invalid
Invalid Instruction 7	0xC7	This setting allows customers to configure invalid
Quad I/O Read Enable	Yes	This soft-strap only has effect if Quad I/O Read
Quad Output Read Enable	Yes	This soft-strap only has effect if Quad Output
Read ID and Read Status Clock ...	50MHz	This setting allows customers to configure the
Write and Erase Clock Frequency	50MHz	This setting allows customers to configure the

#	Parameter	Settings
4	Flash Configuration	
	Dual I/O Read Enabled Values: Yes/No - This setting allows the customer to enable support for Dual I/O Read capabilities for flash components.	Yes
	Dual Output Read Enabled Values: Yes/No - This setting allows the customer to enable support for Dual Output Read capabilities for flash components.	Yes
	Fast Read Clock Frequency Values: 50MHz, 33MHz, 20MHz - This setting allows the customer to configure the flash component clock frequency setting for Fast Read.	50MHz



Flash Settings Tab		
	Fast Read Supported Values: Yes/No - This setting allows the customer to enable support for Fast Read capabilities for flash components. Note: If fast read supported is set to "No" any changes made to Dual I/O, Quad I/O, Dual Output, or Quad Output will not be affected if set to yes. Fast read supported should also be set to enable frequencies greater than 20MHz.	Yes
	Invalid Instruction 0 - This setting allows the customer to configure invalid instruction to protect against Chip Erase. Note: This setting should be set to '0' if there are not Invalid instructions.	0x21
	Invalid Instruction 1 - This setting allows the customer to configure invalid instruction to protect against Chip Erase. Note: This setting should be set to '0' if there are not Invalid instructions.	0x42
	Invalid Instruction 2 - This setting allows the customer to configure invalid instruction to protect against Chip Erase. Note: This setting should be set to '0' if there are not Invalid instructions.	0x60
	Invalid Instruction 3 - This setting allows the customer to configure invalid instruction to protect against Chip Erase. Note: This setting should be set to '0' if there are not Invalid instructions.	0xAD
	Invalid Instruction 4 - This setting allows the customer to configure invalid instruction to protect against Chip Erase. Note: This setting should be set to '0' if there are not Invalid instructions.	0xB7
	Invalid Instruction 5 - This setting allows the customer to configure invalid instruction to protect against Chip Erase. Note: This setting should be set to '0' if there are not Invalid instructions.	0xB9
	Invalid Instruction 6 - This setting allows the customer to configure invalid instruction to protect against Chip Erase. Note: This setting should be set to '0' if there are not Invalid instructions.	0xC4
	Invalid Instruction 7 - This setting allows the customer to configure invalid instruction to protect against Chip Erase. Note: This setting should be set to '0' if there are not Invalid instructions.	0xC7
	Quad I/O Read Enabled Values: Yes/No - This setting allows the customer to enable support for Quad I/O Read capabilities for flash components.	Yes
	Quad Output Read Enabled Values: Yes/No - This setting allows the customer to enable support for Quad Output Read capabilities for flash components.	Yes
	Read ID and Read Status clock frequency Values: 50MHz, 33MHz, 20MHz - This setting allows the customer to configure the flash component clock frequency setting for Read ID and Read Status.	50MHz

Flash Settings Tab

	Write and Erase clock frequency Values: 50MHz, 33MHz, 20MHz - This setting allows the customer to configure the flash component clock frequency setting for Write and Erase.	50MHz															
▾ Legacy VSCC Table																	
▾ VSCC Entries 5																	
<div style="border: 1px solid #ccc; padding: 5px;"> <div style="display: flex; justify-content: space-between; align-items: center;"> ATF26DF321 +Add VSCC Entry </div> <table border="1" style="width: 100%; border-collapse: collapse;"> <thead> <tr> <th>Parameter</th><th>Value</th><th>Help Text</th></tr> </thead> <tbody> <tr> <td>Part Name</td><td>ATF26DF321</td><td>This setting allow the OEM input a name designation for each flash component being used. Note: This is a free form entry field it does not affect actual flash co...</td></tr> <tr> <td>Vendor ID</td><td>0x1F</td><td>This configures the JEDEC vendor specific byte ID of the SPI flash Component see Controller H / LP SPI Programming guide for further details.</td></tr> <tr> <td>Device ID 0</td><td>0x47</td><td>This configures the JEDEC device specific byte ID 0 of the SPI flash Component see Controller H / LP SPI Programming guide for further details.</td></tr> <tr> <td>Device ID 1</td><td>0x00</td><td>This configures the JEDEC device specific byte ID 1 of the SPI flash Component see Controller H / LP SPI Programming guide for further details.</td></tr> </tbody> </table> </div>			Parameter	Value	Help Text	Part Name	ATF26DF321	This setting allow the OEM input a name designation for each flash component being used. Note: This is a free form entry field it does not affect actual flash co...	Vendor ID	0x1F	This configures the JEDEC vendor specific byte ID of the SPI flash Component see Controller H / LP SPI Programming guide for further details.	Device ID 0	0x47	This configures the JEDEC device specific byte ID 0 of the SPI flash Component see Controller H / LP SPI Programming guide for further details.	Device ID 1	0x00	This configures the JEDEC device specific byte ID 1 of the SPI flash Component see Controller H / LP SPI Programming guide for further details.
Parameter	Value	Help Text															
Part Name	ATF26DF321	This setting allow the OEM input a name designation for each flash component being used. Note: This is a free form entry field it does not affect actual flash co...															
Vendor ID	0x1F	This configures the JEDEC vendor specific byte ID of the SPI flash Component see Controller H / LP SPI Programming guide for further details.															
Device ID 0	0x47	This configures the JEDEC device specific byte ID 0 of the SPI flash Component see Controller H / LP SPI Programming guide for further details.															
Device ID 1	0x00	This configures the JEDEC device specific byte ID 1 of the SPI flash Component see Controller H / LP SPI Programming guide for further details.															
#	Parameter	Settings															
5	VSCC Entries																
	Part Name - This setting allows the OEM input a name designation for each flash component being used. Note: This is a free form entry field it does not affect actual flash component operation.	Winbond															
	Vendor ID - This configures the JEDEC vendor specific byte ID of the SPI flash component.	0x1F															
	Device ID 0 - This configures the JEDEC device specific byte ID 0 of the SPI flash component.	0x47															
	Device ID 1 - This configures the JEDEC device specific byte ID 1 of the SPI flash component.	0x00															
6	+Add VSCC Entry																
▾ BIOS Configuration 7																	
<table border="1" style="width: 100%; border-collapse: collapse;"> <thead> <tr> <th>Parameter</th><th>Value</th><th></th></tr> </thead> <tbody> <tr> <td>BIOS Redundancy Assistance</td><td>Disabled</td><td>In case of BIOS boot failure, CSME will configure the platform to boot with backup</td></tr> <tr> <td>Top Swap Block Size</td><td>64KB</td><td>This configures the Top Swap Block size for the platform. For further details see E</td></tr> </tbody> </table>			Parameter	Value		BIOS Redundancy Assistance	Disabled	In case of BIOS boot failure, CSME will configure the platform to boot with backup	Top Swap Block Size	64KB	This configures the Top Swap Block size for the platform. For further details see E						
Parameter	Value																
BIOS Redundancy Assistance	Disabled	In case of BIOS boot failure, CSME will configure the platform to boot with backup															
Top Swap Block Size	64KB	This configures the Top Swap Block size for the platform. For further details see E															
#	Parameter	Settings															
7	BIOS Configuration																




Flash Settings Tab											
	BIOS Redundancy Assistance Values: Enabled, Disabled In cases of BIOS boot failure, Intel® CSME will configure the platform to boot with backup BIOS using Top Swap when this setting is enabled. Note: This option is only applicable when Boot Guard is enabled.	Disabled									
	Top Swap Block Size Values: 64KB, 128KB, 256KB, 512KB, 1MB - This configures the Top Swap Block size for the platform. For further details see EHL EDS.	64KB									
FPF Configuration 8											
<table><tr><th>Parameter</th><th>Value</th><th>Help</th></tr><tr><td>Hardware Binding Enabled</td><td>Disabled</td><td>This setting configures the FPF Hardware and RPI</td></tr></table>			Parameter	Value	Help	Hardware Binding Enabled	Disabled	This setting configures the FPF Hardware and RPI			
Parameter	Value	Help									
Hardware Binding Enabled	Disabled	This setting configures the FPF Hardware and RPI									
#	Parameter	Settings									
8	FPF Configuration										
	Hardware Binding Enabled Values: Enabled / Disabled This setting configures the FPF Hardware binding behavior for the platform image. If this setting is enabled FPF Hardware binding will occur when platform close manufacturing flow is executed with Intel® FPT. If this setting is disabled FPF Hardware binding will not take place when close manufacturing flow is executed. For Revenue parts this setting will be ignored and FPF Hardware binding will take place when close manufacturing flow is executed.	Disabled									
RPMC Configuration 9											
<table><tr><th>Parameter</th><th>Value</th><th></th></tr><tr><td>RPMC Supported</td><td>No</td><td>This setting determines if RPMC is enabled. Note: The SPI parts being used</td></tr><tr><td>RPMC Rebinding Enabled</td><td>No</td><td>This setting determines if Rebinding of RPMC enabled SPI parts is enabled.</td></tr></table>			Parameter	Value		RPMC Supported	No	This setting determines if RPMC is enabled. Note: The SPI parts being used	RPMC Rebinding Enabled	No	This setting determines if Rebinding of RPMC enabled SPI parts is enabled.
Parameter	Value										
RPMC Supported	No	This setting determines if RPMC is enabled. Note: The SPI parts being used									
RPMC Rebinding Enabled	No	This setting determines if Rebinding of RPMC enabled SPI parts is enabled.									
#	Parameter	Settings									
9	RPMC Configuration										
	RPMC Supported	No									

Flash Settings Tab		
	Values: Yes / No This setting determines if RPMC is enabled. Note: The SPI parts being used need to support RPMC In order to use this feature.	
	RPMC Rebinding Enabled Values: Yes / No This setting determines if Rebinding of RPMC enabled SPI parts is enabled	No

2.1.5 Intel® ME Kernel Tab

Click on Intel® ME Kernel in the left tabs' menu. All regions are expanded by default. See the table below.

Intel® ME Kernel Tab														
<div>  </div>														
<table border="1"> <thead> <tr> <th>Parameter</th><th>Value</th><th>Help</th></tr> </thead> <tbody> <tr> <td>Firmware Update OEM ID</td><td>00000000-0000-0000-0000-000...</td><td>This setting allows configuration of an OEM</td></tr> <tr> <td>Hide MEBx Firmware Update Control</td><td>No</td><td>This setting allows customers to hide the</td></tr> <tr> <td>Intel(R) ME Region Flash Protection Override</td><td>Yes</td><td>This setting enables descriptor unlock of t</td></tr> </tbody> </table>			Parameter	Value	Help	Firmware Update OEM ID	00000000-0000-0000-0000-000...	This setting allows configuration of an OEM	Hide MEBx Firmware Update Control	No	This setting allows customers to hide the	Intel(R) ME Region Flash Protection Override	Yes	This setting enables descriptor unlock of t
Parameter	Value	Help												
Firmware Update OEM ID	00000000-0000-0000-0000-000...	This setting allows configuration of an OEM												
Hide MEBx Firmware Update Control	No	This setting allows customers to hide the												
Intel(R) ME Region Flash Protection Override	Yes	This setting enables descriptor unlock of t												
#	Parameter	Settings												
1	Intel® ME Firmware Update													
	Firmware Update OEM ID This setting allows configuration of an OEM unique ID to ensure that customers can only update their platform with images from the OEM of the platform.	0 string												
	Hide MEBx Firmware Update Control This setting allows customers to hide the Firmware Update option in MEBx interface	No												
	Intel® ME Region Flash Protection Override Values: Yes/No This setting enables descriptor unlock of the Intel® CSE Region when the HMRFPO message is sent to firmware prior to BIOS End of POST.	Yes												



Intel® ME Kernel Tab											
<div>▼ Image Identification 2</div> <table border="1"><thead><tr><th>Parameter</th><th>Value</th><th>Help Text</th></tr></thead><tbody><tr><td>OEM Tag</td><td>0x00000000</td><td>-</td></tr></tbody></table>			Parameter	Value	Help Text	OEM Tag	0x00000000	-			
Parameter	Value	Help Text									
OEM Tag	0x00000000	-									
#	Parameter	Settings									
2	Image Identification										
	OEM Tag - This is a free form 32bit field that allows the OEM to configure their own unique identifier in the firmware image.	0x00000000									
<div>▼ Firmware Diagnostics 3</div> <table border="1"><thead><tr><th>Parameter</th><th>Value</th><th>Help</th></tr></thead><tbody><tr><td>Automatic Built in Self Test</td><td>Disabled</td><td>This setting enables the firmware Automatic Built</td></tr></tbody></table>			Parameter	Value	Help	Automatic Built in Self Test	Disabled	This setting enables the firmware Automatic Built			
Parameter	Value	Help									
Automatic Built in Self Test	Disabled	This setting enables the firmware Automatic Built									
#	Parameter	Settings									
3	Firmware Diagnostics										
	Automatic Built in Self Test Values: Enabled/Disabled This setting enables the firmware Automatic Built in Self-Test which is executed during first platform boot after initial image flashing.	Disabled									
<div>▼ End of Manufacturing Configuration 4</div> <table border="1"><thead><tr><th>Parameter</th><th>Value</th><th></th></tr></thead><tbody><tr><td>EOM on First Boot Enabled</td><td>No</td><td>This setting detremines if End of Manufacturing will be triggered on first boot of th</td></tr><tr><td>Flexible EOM setting options</td><td>Lock Descriptor and OEM Configs</td><td>This setting deteremines which settings will be automatically committed during End</td></tr></tbody></table>			Parameter	Value		EOM on First Boot Enabled	No	This setting detremines if End of Manufacturing will be triggered on first boot of th	Flexible EOM setting options	Lock Descriptor and OEM Configs	This setting deteremines which settings will be automatically committed during End
Parameter	Value										
EOM on First Boot Enabled	No	This setting detremines if End of Manufacturing will be triggered on first boot of th									
Flexible EOM setting options	Lock Descriptor and OEM Configs	This setting deteremines which settings will be automatically committed during End									
#	Parameter	Settings									
4	End Of Manufacturing Configuration										
	EOM of First Boot Enabled	No									

Intel® ME Kernel Tab								
	Value: Yes/No This setting determines if End of Manufacturing will be triggered on first boot of the platform after flashing. Note: When this setting is enabled Intel® CSE will enter End of Manufacturing regardless of the descriptor settings.							
	Flexible EOM setting options Value: Lock Descriptor and OEM Configs/Lock OEM Configs Only/Lock Descriptor Only/Do not lock Descriptor and OEM Configs This setting determines which settings will be automatically committed during End of Manufacturing flows. Note: The FPFs, RPMC and set manufacturing mode settings are mandatory and cannot be overridden revenue parts. Simulation can be done on non-revenue part with the Hardware binding set to disabled.	Lock Descriptor and OEM Configs						
<div> <div>Intel (R) ME Boot Configuration</div> <div>5</div> <table> <tr> <th>Parameter</th><th>Value</th><th>Help Text</th></tr> <tr> <td>Persistent PRTC Backup Power</td><td>Exists</td><td>FPF that indicates if the device is designed such that it r</td></tr> </table> </div>			Parameter	Value	Help Text	Persistent PRTC Backup Power	Exists	FPF that indicates if the device is designed such that it r
Parameter	Value	Help Text						
Persistent PRTC Backup Power	Exists	FPF that indicates if the device is designed such that it r						
#	Parameter	Settings						
5	Intel® ME Boot Configuration							
	Persistent PRTC Backup Power Values: None / Exists FPF that indicates if the device is designed such that it may lose PRTC power more than 10 times throughout the normal life-cycle of the product and hence has no persistent time or AR protection. At EOM this value is burned to the FPF, and can never be changed.	Exists						
<div> <div>Intel (R) Me Measured Boot Configuration</div> <div>6</div> <table> <tr> <th>Parameter</th><th>Value</th><th></th></tr> <tr> <td>Intel(R) ME Measured Boot State</td><td>Disabled</td><td>When measured boot is enabled firmware will u</td></tr> </table> </div>			Parameter	Value		Intel(R) ME Measured Boot State	Disabled	When measured boot is enabled firmware will u
Parameter	Value							
Intel(R) ME Measured Boot State	Disabled	When measured boot is enabled firmware will u						
#	Parameter	Settings						
6	Intel® ME Measured Boot Configuration							
	Intel® ME Measured Boot State Values: Enables/Disabled When measured boot is enabled firmware will use additional extended registers for all IUPs and Key Manifests that firmware loads and verifies from flash. Note: When measured boot is enabled any IUPs or firmware updates will require a global reset	Disabled						

Intel® ME Kernel Tab

Intel(R) ME Assisted Boot Configuration

Parameter	Value	
Intel(R) ME Assisted BIOS Boot	Intel(R) ME Assisted	This setting configures Intel(R) ME Assisted BIOS Boot capabilities.

2.1.6 Platform Protection Tab

Click on Platform Protection in the left tabs' menu. All regions are expanded by default. See the table below.

Platform Protection Tab														
<div> <div>Content Protection</div> <table> <tr> <th>Parameter</th><th>Value</th><th>Help</th></tr> <tr> <td>PAVP Supported</td><td>Yes</td><td>This setting determines if the Protected Audio Video Path (PAVP) feature will be permanently disabled in the FW image.</td></tr> <tr> <td>HDCP Internal Display Port 1 - 5K</td><td>PortA</td><td>This setting determines which port is connected for 5K output on the Internal Display 1.</td></tr> <tr> <td>HDCP Internal Display Port 2 - 5K</td><td>None</td><td>This setting determines which port is connected for 5K output on the Internal Display 2.</td></tr> </table> </div>			Parameter	Value	Help	PAVP Supported	Yes	This setting determines if the Protected Audio Video Path (PAVP) feature will be permanently disabled in the FW image.	HDCP Internal Display Port 1 - 5K	PortA	This setting determines which port is connected for 5K output on the Internal Display 1.	HDCP Internal Display Port 2 - 5K	None	This setting determines which port is connected for 5K output on the Internal Display 2.
Parameter	Value	Help												
PAVP Supported	Yes	This setting determines if the Protected Audio Video Path (PAVP) feature will be permanently disabled in the FW image.												
HDCP Internal Display Port 1 - 5K	PortA	This setting determines which port is connected for 5K output on the Internal Display 1.												
HDCP Internal Display Port 2 - 5K	None	This setting determines which port is connected for 5K output on the Internal Display 2.												
#	Parameter	Settings												
1	PAVP Supported Values: Yes/No This setting determines if the Protected Audio Video Path (PAVP) feature will be permanently disabled in the FW image.	Yes												
	HDCP Internal Display Port 1 - 5K Values: None, Port A, Port B, Port C This setting determines which port is connected for 5K output on the Internal Display 1. Note: Both Display Port 1 & 2 need to be configured for proper operation.	Port A												
	HDCP Internal Display Port 2 - 5K Values: None, Port A, Port B, Port C This setting determines which port is connected for 5K output on the Internal Display 2. Note: Both Display Port 1 & 2 need to be configured for proper operation.	None												
<div> <div>Graphics uController</div> <table> <tr> <th>Parameter</th><th>Value</th><th>Help</th></tr> <tr> <td>GuC Encryption Key</td><td>00 00 00 00 00 00 ...</td><td>This option is for entering the raw hash 256 bit string for the Graphics uController.</td></tr> </table> </div>			Parameter	Value	Help	GuC Encryption Key	00 00 00 00 00 00 ...	This option is for entering the raw hash 256 bit string for the Graphics uController.						
Parameter	Value	Help												
GuC Encryption Key	00 00 00 00 00 00 ...	This option is for entering the raw hash 256 bit string for the Graphics uController.												
#	Parameter	Settings												
2	Graphics uController													
	GuC Encryption Key Values: This option is for entering the raw hash 256 bit string or certificate file for the Graphics uController.	0x00000000												



Platform Protection Tab																				
Hash Key Configuration for Bootguard 3																				
<table border="1"><thead><tr><th>Parameter</th><th>Value</th><th></th></tr></thead><tbody><tr><td>OEM Public Key Hash</td><td>00 00 00 00 00 00 ...</td><td>Raw hash string for the SHA-384 hash of the OEM public key</td></tr><tr><td>OEM Key Manifest Binary</td><td></td><td>Signed manifest file containing hashes of keys used for signing components of image</td></tr><tr><td>Second OEM key hash</td><td>00 00 00 00 00 00 ...</td><td>-</td></tr><tr><td>Oem Key Revocation Enable</td><td>No</td><td>Enabling the OEM key revocation mechanism requires the OEM public key hash and second OEM key hash to be configured.</td></tr><tr><td>Skip OEM Keys Check</td><td>No</td><td>This is meant for debugging purposes only. Enabling this parameter impacts image creation procedure in FIT tool only</td></tr></tbody></table>			Parameter	Value		OEM Public Key Hash	00 00 00 00 00 00 ...	Raw hash string for the SHA-384 hash of the OEM public key	OEM Key Manifest Binary		Signed manifest file containing hashes of keys used for signing components of image	Second OEM key hash	00 00 00 00 00 00 ...	-	Oem Key Revocation Enable	No	Enabling the OEM key revocation mechanism requires the OEM public key hash and second OEM key hash to be configured.	Skip OEM Keys Check	No	This is meant for debugging purposes only. Enabling this parameter impacts image creation procedure in FIT tool only
Parameter	Value																			
OEM Public Key Hash	00 00 00 00 00 00 ...	Raw hash string for the SHA-384 hash of the OEM public key																		
OEM Key Manifest Binary		Signed manifest file containing hashes of keys used for signing components of image																		
Second OEM key hash	00 00 00 00 00 00 ...	-																		
Oem Key Revocation Enable	No	Enabling the OEM key revocation mechanism requires the OEM public key hash and second OEM key hash to be configured.																		
Skip OEM Keys Check	No	This is meant for debugging purposes only. Enabling this parameter impacts image creation procedure in FIT tool only																		
#	Parameter	Settings																		
3	Hash Key Configuration for Bootguard																			
	OEM Public Key Hash This option is for entering the raw hash string or certificate file for Boot Guard and ISH. This 384-bit / 256-bit field represents the SHA-384 / SHA-256 hash of the OEM public key corresponding to the private key used to sign the BIOS-SM or ISH image.	0x00000000																		
	OEM Key Manifest Binary Signed manifest file containing hashes of keys used for signing components of image. This setting is only configurable when OEM signing is enabled (See PlatformIntegrity / OemPublicKeyHash).																			
	Second OEM Key hash This option is for entering a secondary raw hash string or certificate file for Boot Guard and ISH used in instances of OEM Key Revocation. This 384-bit / 256-bit field represents the SHA-384 / SHA-256 hash of the OEM public key corresponding to the private key used to sign the BIOS-SM or ISH image. Note: This setting is greyed out and not configurable until the Second OEM Key Revocation Enable is set to Yes.	0x00000000																		
	OEM Key Revocation Enabled Values: Yes/No This setting enables firmware OEM Key Revocation capabilities. Note: This setting requires that both OEM Public Key Hash and Second OEM Key Hash are configured.	No																		
	Skip OEM Keys Check Values: No/Yes This is meant for debugging purposes only. Enabling this parameter impacts image creation procedure in FIT tool only	No																		

Platform Protection Tab

▼ Descriptor Configuration

4

Parameter	Value	
Flash Descriptor Verification Enabled	No	-
exclude master access in the signature	Yes	include/exclude master access in the signature

#	Parameter	Settings
4	Descriptor Configuration	
	Flash Descriptor Verification Enabled Values: Yes/No This setting enables / disables Flash Descriptor Verification	No
	exclude master access in the signature Values: Yes/No Include/exclude master access in the signature.	Yes

▼ Exclusion Ranges

5

Parameter	Value	
Range 1 offset	0x800	Range 1 offset covers manifest, cannot be changed
Range 1 size	0x400	Range 1 size covers manifest, cannot be changed
Range 2 offset	0x80	Range 2 offset covers master access offset
Range 2 size	0x20	Range 2 size covers master access size
Range 3 offset	0x0	Range 3 offset covers OEM defined unprotected range start
Range 3 size	0x0	Range 3 size covers OEM defined unprotected range length
Range 4 offset	0x0	Range 4 offset covers OEM defined unprotected range start
Range 4 size	0x0	Range 4 size covers OEM defined unprotected range length
Range 5 offset	0x0	Range 5 offset covers OEM defined unprotected range start
Range 5 size	0x0	Range 5 size covers OEM defined unprotected range length
Range 6 offset	0x0	Range 6 offset covers OEM defined unprotected range start
Range 6 size	0x0	Range 6 size covers OEM defined unprotected range length
Range 7 offset	0x0	Range 7 offset covers OEM defined unprotected range start
Range 7 size	0x0	Range 7 size covers OEM defined unprotected range length
Range 8 offset	0x0	Range 8 offset covers OEM defined unprotected range start
Range 8 size	0x0	Range 8 size covers OEM defined unprotected range length



Platform Protection Tab		
#	Parameter	Settings
5	Exclusion Ranges	
	Range 1 offset Range 1 offset covers manifest, cannot be changed	0x800
	Range 1 size Range 1 size covers manifest, cannot be changed.	0x400
	Range 2 offset Range 2 offset covers master access offset	0x80
	Range 2 size Range 2 offset covers master access size	0x20
	Range 3 offset Values: Hex Range 3 offset covers OEM defined unprotected range start.	0x0
	Range 3 size Values: Hex Range 3 size covers OEM defined unprotected range length	0x0
	Range 4 offset Values: Hex Range 3 offset covers OEM defined unprotected range start.	0x0
	Range 4 size Values: Hex Range 3 size covers OEM defined unprotected range length	0x0
	Range 5 offset Values: Hex Range 3 offset covers OEM defined unprotected range start.	0x0
	Range 5 size Values: Hex Range 3 size covers OEM defined unprotected range length	0x0
	Range 6 offset Values: Hex Range 3 offset covers OEM defined unprotected range start.	0x0
	Range 6 size Values: Hex Range 3 size covers OEM defined unprotected range length	0x0
	Range 7 offset Values: Hex Range 3 offset covers OEM defined unprotected range start.	0x0
	Range 7 size Values: Hex Range 3 size covers OEM defined unprotected range length	0x0
	Range 8 offset Values: Hex Range 3 offset covers OEM defined unprotected range start.	0x0
	Range 8 size Values: Hex Range 3 size covers OEM defined unprotected range length	0x0

Platform Protection Tab

▼ Boot Guard Configuration

6

Parameter	Value	Help Text
Key Manifest ID	0	ODM identifier used during the Key manifest authenticat
Boot Guard Profile Configuration	Boot Guard Profile 0 - No_FVME	Boot Guard Profile 0 - Legacy is for platforms that do no
CPU Debugging	Enabled	This setting determines if CPU debug modes will be disp
BSP Initialization	Enabled	This setting determines BSP behavior when it receives a

#	Parameter	Settings
6	Boot Guard Configuration	
	Key Manifest ID This option is for entering the hash of another public key, used by the ACM to verify the Boot Policy Manifest.	0x0
	Boot Guard Profile Configuration Values: Boot Guard Profile 0 - No_FVME Boot Guard Profile 3 - VM Boot Guard Profile 4 - FVE Boot Guard Profile 5 - FVME This option configures which Boot Guard Policy Profile will be used. Note: Boot Guard Profile 3 is intended for development and debugging it should not be used for production platform images.	Boot Guard Profile 0 - No_FVME
	CPU Debugging Values: Enabled/Disabled This setting determines if CPU debug modes will be displayed. When set to 'Enabled' CPU debugging is enabled.	Enabled
	BSP Initialization Values: Enabled/Disabled This setting determines BSP behavior when it receives an INIT signal. When set to 'Enabled' BSP will behave normally if it receives an INIT (Disabled BSP Initialization (DBI) bit=0). When set to 'Disabled' BSP will shutdown if it receives an INIT ("DBI" bit=1).	Enabled



Platform Protection Tab																				
<div>Intel(R) PTT Configuration 7</div> <table border="1"><thead><tr><th>Parameter</th><th>Value</th><th>Help Text</th></tr></thead><tbody><tr><td>Intel(R) PTT Supported</td><td>Yes</td><td>This setting permanently disables Intel(R) PTT in the firmware image.</td></tr><tr><td>Intel(R) PTT initial power-up state</td><td>Enabled</td><td>-</td></tr><tr><td>Intel(R) PTT Supported [FPF]</td><td>Yes</td><td>This setting will permanently disable Intel(R) PTT through platform FPFs. Caution: Using this option will permanently</td></tr><tr><td>SMx State</td><td>Enabled</td><td>-</td></tr><tr><td>Rsa 1K State</td><td>Disabled</td><td>-</td></tr></tbody></table>			Parameter	Value	Help Text	Intel(R) PTT Supported	Yes	This setting permanently disables Intel(R) PTT in the firmware image.	Intel(R) PTT initial power-up state	Enabled	-	Intel(R) PTT Supported [FPF]	Yes	This setting will permanently disable Intel(R) PTT through platform FPFs. Caution: Using this option will permanently	SMx State	Enabled	-	Rsa 1K State	Disabled	-
Parameter	Value	Help Text																		
Intel(R) PTT Supported	Yes	This setting permanently disables Intel(R) PTT in the firmware image.																		
Intel(R) PTT initial power-up state	Enabled	-																		
Intel(R) PTT Supported [FPF]	Yes	This setting will permanently disable Intel(R) PTT through platform FPFs. Caution: Using this option will permanently																		
SMx State	Enabled	-																		
Rsa 1K State	Disabled	-																		
#	Parameter	Settings																		
7	Intel® PTT Configuration																			
	Intel® PTT Supported Values: Yes/No This setting permanently disables Intel® PTT in the firmware image.	Yes																		
	Intel® PTT initial power-up state Values: Enabled/Disabled This setting determines if Intel® PTT is enabled on platform power-up.	Enabled																		
	Intel® PTT Supported [FPF] Values: Yes/No This setting will permanently disable Intel® PTT through platform FPFs. Caution: Using this option will permanently disable Intel® PTT on the platform hardware.	Yes																		
	SMx Support State Values: Enabled/Disabled This setting enables/disables SMx support.	Enabled																		
	RSA 1K State Values: Enabled/Disabled	Disabled																		
<div>TPM Over SPI Bus Configuration 8</div> <table border="1"><thead><tr><th>Parameter</th><th>Value</th><th></th></tr></thead><tbody><tr><td>TPM Over SPI Bus Enabled</td><td>Yes</td><td>This setting determines the clock frequency setting</td></tr><tr><td>TPM Clock Frequency</td><td>20MHz</td><td>This setting determines the clock frequency setting</td></tr></tbody></table>			Parameter	Value		TPM Over SPI Bus Enabled	Yes	This setting determines the clock frequency setting	TPM Clock Frequency	20MHz	This setting determines the clock frequency setting									
Parameter	Value																			
TPM Over SPI Bus Enabled	Yes	This setting determines the clock frequency setting																		
TPM Clock Frequency	20MHz	This setting determines the clock frequency setting																		
#	Parameter	Settings																		

Platform Protection Tab								
8	TPM Over SPI Bus Configuration							
	TPM Over SPI Bus Enabled Values: Yes/No - This setting determines if TPM over SPI bus is enabled on the platform.	Yes						
	TPM Clock Frequency Values: 20MHz, 33MHz, 50MHz This setting determines the clock frequency setting to be used for the TPM over SPI bus	20 MHz						
<div> <div> FuSa Configuration 9 </div> </div>								
<table> <tr> <th>Parameter</th><th>Value</th><th></th></tr> <tr> <td>FuSa Proof Test Components</td><td>0x3F80</td><td>This setting determines which FuSa tests will be r</td></tr> </table>			Parameter	Value		FuSa Proof Test Components	0x3F80	This setting determines which FuSa tests will be r
Parameter	Value							
FuSa Proof Test Components	0x3F80	This setting determines which FuSa tests will be r						
#	Parameter	Settings						
9	FuSa Configuration Note: Used to enabling FuSa safety standards							
	FuSa Proof Tests Components	0x3F80						



2.1.7 Integrated Clock Controller Tab

Click on Integrated Clock Controller in the left tabs' menu. All regions are expanded by default. See the table below

Integrated Clock Controller Tab														
<div>Integrated Clock Controller Policies 1</div> <table><thead><tr><th>Parameter</th><th>Value</th><th>Help</th></tr></thead><tbody><tr><td>Boot Profile</td><td>Profile 0</td><td>Profile applied during each boot.</td></tr><tr><td>Failsafe Boot Profile</td><td>Profile 0</td><td>Boot profile used when system instability is detected.</td></tr><tr><td>Profile Changeable</td><td>true</td><td>True = Allows user to change boot profile via BIOS.</td></tr></tbody></table>			Parameter	Value	Help	Boot Profile	Profile 0	Profile applied during each boot.	Failsafe Boot Profile	Profile 0	Boot profile used when system instability is detected.	Profile Changeable	true	True = Allows user to change boot profile via BIOS.
Parameter	Value	Help												
Boot Profile	Profile 0	Profile applied during each boot.												
Failsafe Boot Profile	Profile 0	Boot profile used when system instability is detected.												
Profile Changeable	true	True = Allows user to change boot profile via BIOS.												
#	Parameter	Settings												
1	Boot Profile <p>This parameter allows user to select default profile to be used by the final generated SPI Flash binary image for the target platform at boot time.</p> <p>Selection is limited to the profiles defined under "Integrated Clock Controller Profiles" up to maximum 16 profiles. Profiles can be added by clicking on "Add profile" button under "Integrated Clock Controller Profiles".</p> <p>The 'Record #' refers to profile created under the "Integrated Clock Controller Profiles".</p>	Profile 0												
	Failsafe Profile <p>This parameter specifies the profile index of the fail-safe profile. On boot failure detection or CMOS clear the Intel® CSE Firmware will revert to this profile if "Integrated Clock Controller Integrated Clock Controller Policies - Profile Changeable" is set to True. If profile Changeable parameter is set to False, User can not select Failsafe Boot Profile and profile 0 will be selected as a fail safe boot profile by default.</p>	Profile 0												
	Profile Changeable <p>Possible configuration: True/False.</p> <p>This parameter controls if BIOS or 3rd party application can select boot profile or not. When set to true, it allows user to change boot profile via BIOS or 3rd party application. When set to false, Runtime change to boot profile is not allowed and boot profile selected by "Integrated Clock Controller Integrated Clock Controller Policies - Boot Profile" parameter will be used to boot platform.</p>	True												

Integrated Clock Controller Tab											
<div> <div> <div></div> <div>BCLK Clock Build-time Configurations</div> <div>2</div> </div> </div>											
Parameter	Value										
BCLK Build-time Clock Configuration Enabled	Disabled	Enables/disables BCLK Build-time Clock co									
BCLK Clock Frequency	100.000 MHz	Displays the nominal frequency for the sel									
BCLK Spread setting	0.45 %	Displays the percentage of Spread setting									
#	Parameter	Settings									
2	BCLK Clock Build-time Configurations										
	BCLK Clock Configuration Enabled Values: Enabled / Disabled This setting enables / disables BCLK Clock configuration values for Adaptive /Overclocking profiles.	Disabled									
	BCLK Clock Frequency This parameter allows user to select the nominal frequency for the selected clock. Range is limited based on the Clock Range Definition record and HW SKU. Standard Setting Profile Type - Option is grayed out. Adaptive Setting Profile Type - Option is editable.	N/A									
	BCLK Spread Setting This parameter allows user to select the percentage of Spread setting for the selected clock. Range is limited based on the Clock Range Definition record and HW SKU. BCLK Clock Frequency Standard Setting Profile Type - Option is grayed out. Adaptive Setting Profile Type - Option editable.	N/A									
<div> <div> <div></div> <div>Profiles</div> <div>3</div> </div> <div>4</div> </div>											
<div> <div>Profile 0</div> <div>Add Profile</div> </div> <table> <tr> <th>Parameter</th><th>Value</th><th>Help Text</th></tr> <tr> <td>Profile Name</td><td>Profile 0</td><td>Editable text string stored with the profile for easy identification.</td></tr> <tr> <td>Profile Type</td><td>Standard</td><td>Specifies the profile template used when creating the profile. Intel (R) ME image has to be loaded to enable other ICC profi...</td></tr> </table>			Parameter	Value	Help Text	Profile Name	Profile 0	Editable text string stored with the profile for easy identification.	Profile Type	Standard	Specifies the profile template used when creating the profile. Intel (R) ME image has to be loaded to enable other ICC profi...
Parameter	Value	Help Text									
Profile Name	Profile 0	Editable text string stored with the profile for easy identification.									
Profile Type	Standard	Specifies the profile template used when creating the profile. Intel (R) ME image has to be loaded to enable other ICC profi...									
#	Parameter	Settings									
3	Profiles – Profile 0 Note: Intel® CSE image has to be loaded to enable other ICC profile settings.										



Integrated Clock Controller Tab																	
	Profile Name This parameter allows user to customize profile name for easy identification.	Profile 0															
	Profile Type For Elkhart Lake, Intel® FIT provides 2 pre- defined ICC profiles to choose from: •Standard: This profile provides default settings for standard configuration; no adaptive clocking is allowed. Platform clocks output internal and external are driven from USB3PCIE clock. Default clock frequency is 100 MHz with 0.48%DownSpread. BCLK clock source should be turned off in this case to save power. •Adaptive: This profile will configure the platform based on the Adaptive profile allowing adaptive clocking adjustment for BCLK clock source to reduce EMI interference. It supports default clock frequency of 98.875 MHz with 0.48% Downspread.	Standard															
4	+ Add Profile Button This button is used to add new ICC profile. User can add up to maximum 16 profiles. New profile will be added under "Integrated Clock Controller Profiles" tab.																
▾ Clock Range Definition Record 5																	
<table border="1"> <thead> <tr> <th>Parameter</th><th>Value</th><th></th></tr> </thead> <tbody> <tr> <td>BCLK PLL Clock Source Maximum Frequency</td><td>100.000 MHz</td><td>Specifies the maximum frequency that can</td></tr> <tr> <td>BCLK PLL Clock Source Minimum Frequency</td><td>100.00 MHz</td><td>Specifies the minimum frequency that can</td></tr> <tr> <td>BCLK SSC Halt Allowed</td><td>No</td><td>If set to Yes, the spread generator can be</td></tr> <tr> <td>BCLK SSC Maximum Percentage</td><td>0.50 MHz</td><td>Specifies the maximum percentage of spre</td></tr> </tbody> </table>			Parameter	Value		BCLK PLL Clock Source Maximum Frequency	100.000 MHz	Specifies the maximum frequency that can	BCLK PLL Clock Source Minimum Frequency	100.00 MHz	Specifies the minimum frequency that can	BCLK SSC Halt Allowed	No	If set to Yes, the spread generator can be	BCLK SSC Maximum Percentage	0.50 MHz	Specifies the maximum percentage of spre
Parameter	Value																
BCLK PLL Clock Source Maximum Frequency	100.000 MHz	Specifies the maximum frequency that can															
BCLK PLL Clock Source Minimum Frequency	100.00 MHz	Specifies the minimum frequency that can															
BCLK SSC Halt Allowed	No	If set to Yes, the spread generator can be															
BCLK SSC Maximum Percentage	0.50 MHz	Specifies the maximum percentage of spre															
#	Parameter	Settings															
5	Profiles - Clock Range Definition Record The following applies for all of the parameters below: Standard Setting Profile Type - Option is grayed out. Adaptive Setting Profile Type - Option is able to be edited																
	BCLK PLL Clock Source Maximum Frequency - This parameter allows user to specify the maximum frequency that can be applied to BCLK clock source when overclocking the platform. Value is limited by divider/frequency limits determined by HW SKU, and cannot be less than 100 MHz.																
	BCLK PLL Clock Source Minimum Frequency - This parameter allows user to specify the minimum frequency that can be applied to BCLK clock source when underclocking the platform. Value is limited by divider/frequency limits determined by HW SKU, and cannot be greater than 100 MHz.																

Integrated Clock Controller Tab																							
	BCLK SSC Halt Allowed - This parameter allows user to select if the spread generator can be disabled at runtime or not. If set to "True" , the spread generator can be enabled and disabled at runtime.																						
	BCLK SSC Maximum Percentage - This parameter Specifies the maximum percentage of spread adjustment that can be applied to the clock. Value is specified in 1/100th of percent (50=0.5%)																						
<div> <div>6</div> <div> <div>▼ Clock Output Configuration</div> <table> <tr> <th>Parameter</th><th>Value</th><th>Help</th></tr> <tr> <td>SRC0</td><td>Enabled</td><td>Enable/Disable the CLKOUT_SRC0 differential output buffer.</td></tr> <tr> <td>SRC1</td><td>Enabled</td><td>Enable/Disable the CLKOUT_SRC1 differential output buffer.</td></tr> <tr> <td>SRC2</td><td>Enabled</td><td>Enable/Disable the CLKOUT_SRC2 differential output buffer.</td></tr> <tr> <td>SRC3</td><td>Enabled</td><td>Enable/Disable the CLKOUT_SRC3 differential output buffer.</td></tr> <tr> <td>SRC4</td><td>Enabled</td><td>Enable/Disable the CLKOUT_SRC4 differential output buffer.</td></tr> <tr> <td>SRC5</td><td>Enabled</td><td>Enable/Disable the CLKOUT_SRC5 differential output buffer.</td></tr> </table> </div> </div>			Parameter	Value	Help	SRC0	Enabled	Enable/Disable the CLKOUT_SRC0 differential output buffer.	SRC1	Enabled	Enable/Disable the CLKOUT_SRC1 differential output buffer.	SRC2	Enabled	Enable/Disable the CLKOUT_SRC2 differential output buffer.	SRC3	Enabled	Enable/Disable the CLKOUT_SRC3 differential output buffer.	SRC4	Enabled	Enable/Disable the CLKOUT_SRC4 differential output buffer.	SRC5	Enabled	Enable/Disable the CLKOUT_SRC5 differential output buffer.
Parameter	Value	Help																					
SRC0	Enabled	Enable/Disable the CLKOUT_SRC0 differential output buffer.																					
SRC1	Enabled	Enable/Disable the CLKOUT_SRC1 differential output buffer.																					
SRC2	Enabled	Enable/Disable the CLKOUT_SRC2 differential output buffer.																					
SRC3	Enabled	Enable/Disable the CLKOUT_SRC3 differential output buffer.																					
SRC4	Enabled	Enable/Disable the CLKOUT_SRC4 differential output buffer.																					
SRC5	Enabled	Enable/Disable the CLKOUT_SRC5 differential output buffer.																					
#	Parameter	Settings																					
6	Profiles – Clock Output Configuration																						
	SRC0 Values: Enabled/Disabled Enables or Disables the CLKOUT_SRC1 differential output buffer.	Enabled																					
	SRC1 Values: Enabled/Disabled Enables or Disables the CLKOUT_SRC2 differential output buffer.																						
	SRC2 Values: Enabled/Disabled Enables or Disables the CLKOUT_SRC3 differential output buffer.																						
	SRC3 Values: Enabled/Disabled Enables or Disables the CLKOUT_SRC4 differential output buffer.																						
	SRC4 Values: Enabled/Disabled Enables or Disables the CLKOUT_SRC5 differential output buffer.																						
	SRC5 Values: Enabled/Disabled Enables or Disables the CLKOUT_SRC6 differential output buffer.																						



Integrated Clock Controller Tab

▼ Power Management Configuration

Parameter	Value	Help Text
SRC0 CLKREQ# Mapping	GPP_D5	Assign the CLKREQ# signal associated with CLKOUT_SRC0. Please note that remapping of any SRC CLKREQ#
SRC1 CLKREQ# Mapping	GPP_D6	Assign the CLKREQ# signal associated with CLKOUT_SRC1. Please note that remapping of any SRC CLKREQ#
SRC2 CLKREQ# Mapping	GPP_D7	Assign the CLKREQ# signal associated with CLKOUT_SRC2. Please note that remapping of any SRC CLKREQ#
SRC3 CLKREQ# Mapping	GPP_D8	Assign the CLKREQ# signal associated with CLKOUT_SRC3. Please note that remapping of any SRC CLKREQ#
SRC4 CLKREQ# Mapping	GPP_H10	Assign the CLKREQ# signal associated with CLKOUT_SRC4. Please note that remapping of any SRC CLKREQ#
SRC5 CLKREQ# Mapping	GPP_H11	Assign the CLKREQ# signal associated with CLKOUT_SRC5. Please note that remapping of any SRC CLKREQ#

#	Parameter	Settings
7	Profiles - Profile Power Management Configuration Configuring CLKREQ# and assigning GPIO depends on how CLKOUT_SRCx configuration via Intel® FIT is done (Enabled or Disabled) and if CLKREQ is required or not.	
	SRC0[0:5] CLKREQ# Mapping Possible configuration: Select one of the GPIOs from the list to map it as a CLKREQ# for specific SRC# Output clock. This parameter controls association of dynamic CLKREQ control with SRC (PCIe) clocks.	GPP_D5
	SRC1 CLKREQ# Mapping Assign the CLKREQ# signal associated with CLKOUT_SRC1.	GPP_D6
	SRC2 CLKREQ# Mapping Assign the CLKREQ# signal associated with CLKOUT_SRC2.	GPP_D7
	SRC3 CLKREQ# Mapping Assign the CLKREQ# signal associated with CLKOUT_SRC3.	GPP_D8
	SRC4 CLKREQ# Mapping Assign the CLKREQ# signal associated with CLKOUT_SRC4.	GPP_H10
	SRC5 CLKREQ# Mapping Assign the CLKREQ# signal associated with CLKOUT_SRC5.	GPP_H11

2.1.8 Networking & Connectivity Tab

Click on Networking& Connectivity in the left tabs' menu. All regions are expanded by default. See the table below

Networking & Connectivity Tab																													
▼ Gigabit and Time Sensitive Networking Configuration																													
<table> <tr> <th>Parameter</th><th>Value</th><th>Help Text</th></tr> <tr> <td>Gigabit and Time Sensitive Networking</td><td>TSN Enabled</td><td>This setting allows customers to enable / disable Gigabit and Time Sensitive Networking on the platform.</td></tr> <tr> <td>SGMII Intel(R) PSE 0</td><td>Disabled</td><td>-</td></tr> <tr> <td>SGMII Intel(R) PSE 1</td><td>Disabled</td><td>-</td></tr> <tr> <td>SGMII Host 0</td><td>Lane 8</td><td>-</td></tr> <tr> <td>Intel(R) PSE GbE 0 Phy Interface Mode</td><td>RGMII</td><td>This setting determines what mode the Intel(R) PSE GbE 0 Phy Interface will be running in RGMII or SGMII.</td></tr> <tr> <td>Intel(R) PSE GbE 1 Phy Interface Mode</td><td>RGMII</td><td>This setting determines what mode the Intel(R) PSE GbE 1 Phy Interface will be running in RGMII or SGMII.</td></tr> <tr> <td>Intel(R) PSE GbE 1 OOB Enabled</td><td>No</td><td>This setting enables OOB on Intel(R) PSE GbE 1.</td></tr> <tr> <td>Intel(R) PSE GbE 0 OOB Enabled</td><td>No</td><td>This setting enables OOB on Intel(R) PSE GbE 0.</td></tr> </table>			Parameter	Value	Help Text	Gigabit and Time Sensitive Networking	TSN Enabled	This setting allows customers to enable / disable Gigabit and Time Sensitive Networking on the platform.	SGMII Intel(R) PSE 0	Disabled	-	SGMII Intel(R) PSE 1	Disabled	-	SGMII Host 0	Lane 8	-	Intel(R) PSE GbE 0 Phy Interface Mode	RGMII	This setting determines what mode the Intel(R) PSE GbE 0 Phy Interface will be running in RGMII or SGMII.	Intel(R) PSE GbE 1 Phy Interface Mode	RGMII	This setting determines what mode the Intel(R) PSE GbE 1 Phy Interface will be running in RGMII or SGMII.	Intel(R) PSE GbE 1 OOB Enabled	No	This setting enables OOB on Intel(R) PSE GbE 1.	Intel(R) PSE GbE 0 OOB Enabled	No	This setting enables OOB on Intel(R) PSE GbE 0.
Parameter	Value	Help Text																											
Gigabit and Time Sensitive Networking	TSN Enabled	This setting allows customers to enable / disable Gigabit and Time Sensitive Networking on the platform.																											
SGMII Intel(R) PSE 0	Disabled	-																											
SGMII Intel(R) PSE 1	Disabled	-																											
SGMII Host 0	Lane 8	-																											
Intel(R) PSE GbE 0 Phy Interface Mode	RGMII	This setting determines what mode the Intel(R) PSE GbE 0 Phy Interface will be running in RGMII or SGMII.																											
Intel(R) PSE GbE 1 Phy Interface Mode	RGMII	This setting determines what mode the Intel(R) PSE GbE 1 Phy Interface will be running in RGMII or SGMII.																											
Intel(R) PSE GbE 1 OOB Enabled	No	This setting enables OOB on Intel(R) PSE GbE 1.																											
Intel(R) PSE GbE 0 OOB Enabled	No	This setting enables OOB on Intel(R) PSE GbE 0.																											
#	Parameter	Settings																											
1	Gigabit and Time Sensitive Networking Configuration																												
	Gigabit and Time Sensitive Networking Values: TSN Enable / TSN Disabled	TSN Enabled																											
	Sgmi Intel® PSE0 Values: Disabled/Lane 7	Disabled																											
	Sgmi Intel® PSE1 Values: Disabled/Lane 9/Lane 11	Disabled																											
	SgmiHost0 Values: Disabled/Lane 8/Lane 10	Lane 8																											
	Intel® PSE GbE Phy Interface Mode	RGMII																											
	Intel® PSE GbE 1 Phy Interface Mode	RGMII																											
	Intel® PSE GBE 1 OOB Enable Values: No/ Yes	No																											
	Intel® PSE GBE 0 OOB Enable Values: No/ Yes	No																											



2.1.9 Internal PCH Buses Tab

Click on Internal PCH Buses in the left tabs' menu. All regions are expanded by default. See the table below

Internal PCH Buses Tab														
<div> <div>▼ PCH Timer Configuration</div> <div> <table> <tr> <th>Parameter</th><th>Value</th><th></th></tr> <tr> <td>PCH clock output stable to PROCPWRGD high (tPCH45)</td><td>1ms</td><td>This setting configures the min</td></tr> <tr> <td>PCIe Power Stable Timer (tPCH33)</td><td>Disabled</td><td>This setting configures the ena</td></tr> <tr> <td>PROCPWRGD and SYS_PWROK high to SUS_STAT# de-assertion (tPCH46)</td><td>30us</td><td>This setting configures the min</td></tr> </table> </div> </div>			Parameter	Value		PCH clock output stable to PROCPWRGD high (tPCH45)	1ms	This setting configures the min	PCIe Power Stable Timer (tPCH33)	Disabled	This setting configures the ena	PROCPWRGD and SYS_PWROK high to SUS_STAT# de-assertion (tPCH46)	30us	This setting configures the min
Parameter	Value													
PCH clock output stable to PROCPWRGD high (tPCH45)	1ms	This setting configures the min												
PCIe Power Stable Timer (tPCH33)	Disabled	This setting configures the ena												
PROCPWRGD and SYS_PWROK high to SUS_STAT# de-assertion (tPCH46)	30us	This setting configures the min												
#	Parameter	Settings												
1	PCH Timer Configuration													
	PCH clock output stable to PROCPWRGD high (tPCH45) Values: 100ms, 50ms, 5ms, 1ms This setting configures the minimum timing from XCK_PLL locked to CPUPWRGD high.	1ms												
	PCIe Power Stable Timer (tPCH33) Values: Enabled/Disabled This setting configures the enables / disables the t36 timer. When enabled PCH will count 99ms from PWROK assertion before PLTRST# is de-asserted. Note: The recommended setting is "Disabled".	Disabled												
	PROCPWRGD and SYS_PWROK high to SUS_STAT# de-assertion (tPCH46) Values: 1ms, 2ms, 5ms, 30us This setting configures the minimum timing from CPUPWRGD assertion to SUS_STAT#.	30us												

Internal PCH Buses Tab

eSPI Configuration

2

Parameter	Value	
eSPI / EC Maximum I/O Mode	Single, Dual and Quad	Indicates the maximum IO Mode (Single/Dual/Quad) of the eSPI bus that is supported by the eSPI Master and specific platform configuration. The actual IO Mode of the eSPI bus will be the minimum of this field and the Slave's maximum IO Mode advertised in its General Capabilities register
eSPI / EC CRC Check Enabled	Yes	This setting enables CRC checking on eSPI Slave 0 channel.
eSPI Slave 3 Device Bus Frequency	14MHz	This setting configures the maximum operating frequency of the slave device
eSPI Slave 1 Device CRC Check Enable	No	This setting determines if CRC checking is enabled on the eSPI Slave 1 Device channel.
eSPI Slave 1 Device Maximum I/O Mode	Single, Dual and Quad	Indicates the maximum IO Mode (Single/Dual/Quad) of the eSPI bus that is supported by the eSPI Master and specific platform configuration. The actual IO Mode of the eSPI bus will be the minimum of this field and the Slave's maximum IO Mode advertised in its General Capabilities register
eSPI Slave 1 Device Bus Frequency	14MHz	This setting configures the maximum operating frequency of the slave device
eSPI Slave 1 Device Enabled	No	This setting enables the Slave device on the eSPI Slave 1 Device channel.
eSPI Slave Bus Frequency	50MHz	Indicates the maximum frequency of the eSPI bus
eSPI Slave 2 Device Bus Frequency	14MHz	This setting configures the maximum operating frequency of the slave device
eSPI Slave 2 Device Maximum I/O Mode	Single	This setting configures the maximum IO mode of the eSPI Slave 2 Device channel.
eSPI Slave 2 Device CRC Check Enable	No	This setting determines if CRC checking is enabled on the eSPI Slave 2 Device channel.
eSPI Slave 2 Device Enabled	No	This setting enables the Slave device on the eSPI Slave 2 Device channel.
eSPI Slave 3 Device Maximum I/O Mode	Single	This setting configures the maximum IO mode of the eSPI Slave 3 Device channel.
eSPI Slave 3 Device CRC Check Enable	No	This setting determines if CRC checking is enabled on the eSPI Slave 3 Device channel.
eSPI Slave 3 Device Enabled	No	This setting enables the Slave device on the eSPI Slave 3 Device channel.

#	Parameter	Settings
2	eSPI Configuration	
	eSPI/EC MaxI/O Mode Values: Single / Single and Dual / Single and Quad / Single, Dual and Quad Indicates the maximum IO Mode (Single/Dual/Quad) of the eSPI bus that is supported by the eSPI Master and specific platform configuration. The actual IO Mode of the eSPI bus will be the minimum of this field and the Slave's maximum IO Mode advertised in its General Capabilities register	Single, Dual and Quad
	eSPI / EC CRC Check Enabled Values: Yes/ No This setting enables CRC checking on eSPI Slave 0 channel.	Yes
	eSPI Slave 3 Device Bus Frequency Values: 14MHz / 20MHz / 33MHz This setting configures the maximum operating frequency of the slave device	14 MHz
	eSPI Slave1 Device CRC Check Enable Values: Yes / No This setting determines if CRC checking is enabled on the eSPI Slave 1 Device channel.	No



Internal PCH Buses Tab		
	eSPI/Slave 1 Device MaxI/O Mode Values: Single / Single and Duel / Single and Quad / Single, Dual and Quad This setting configures the maximum I/O mode of the Slave device.	Single, Dual and Quad
	eSPI Slave 1 Device Bus Frequency Values: 14MHz / 20MHz / 33MHz / 50MHz This setting configures the maximum operating frequency of the Slave device.	14MHz
	eSPI Slave 1 Device Enabled Values: No/ Yes This setting enables the Slave device on the eSPI interface.	No
	eSPI Slave 1 Device Bus Frequency Values: 14MHz / 20MHz / 33MHz / 50MHz Indicates the maximum frequency of the eSPI bus that is supported by the eSPI Master and platform configuration (trace length, number of Slaves, etc.). The actual frequency of the eSPI bus will be the minimum of this field and the Slave's maximum frequency advertised in its General Capabilities register	50MHz
	eSPI Slave 2 Device Bus Frequency Values: 14MHz / 20MHz / 33MHz This setting configures the maximum operating frequency of the Slave device.	14MHz
	eSPI/Slave 2 Device MaxI/O Mode Values: Single / Single and Duel / Single and Quad / Single, Dual and Quad This setting configures the maximum I/O mode of the Slave device.	Single
	eSPI Slave 2 Device CRC Check Enable Values: Yes / No This setting determines if CRC checking is enabled on the eSPI Slave 2 Device channel.	No
	eSPI Slave 2 Device Enabled Values: No/ Yes This setting enables the Slave device on the eSPI interface.	No
	eSPI/Slave 3 Device MaxI/O Mode Values: Single / Single and Duel / Single and Quad / Single, Dual and Quad This setting configures the maximum I/O mode of the Slave device.	Single
	eSPI Slave 3 Device CRC Check Enable Values: Yes / No This setting determines if CRC checking is enabled on the eSPI Slave 3 Device channel.	No

Internal PCH Buses Tab		
	eSPI Slave 3 Device Enabled Values: No/ Yes This setting enables the Slave device on the eSPI interface.	No

2.1.10 Power Tab

Click on Power in the left tabs’ menu. All regions are expanded by default. See the table below:



Power Tab

▼ Platform Power

Parameter	Value	
SLP_S0# Tunnel	Disabled	This setting Enables / Disable
PMC_BATLOW_N / GP_DSW0 Signal Configuration	Enable as PMC_BATLOW_N	This setting allows the to assic
PMC_SLP_S5_N / GP_DSW10 Signal Configuration	PMC_SLP_S5_N	This setting allows the to assic
PMC_SLP_S4_N / DP_DSW05 Signal Configuration	Enable as PMC_SLP_S4_N	This setting allows the user to
PMC_SLP_S3_N / GP_DSW04 Signal Configuration	Enable as PMC_SLP_S3_N	This setting allows the user to

#	Parameter	Settings
1	Platform Power	
	SLP_S0# Tunnel This setting Enables / Disables the tunneling of the SLP_S0# pin over ESPI to the EC when in ESPI mode.	Disabled
	PMC_BARLOW_N / GGP_DSW0 Signal Configuration Values: Enabled as PMC_BATLOW_N / Enable as GP_DSW0	Enable as PMC_BATLOW_N
	PMC_SLP_S5_N / GP_DSW10 Signal Configuration Values: PMC_SLP5_N / Enable as GP_DSW10	PMC_SLP5_N
	PMC_SLP_S4_N / DP_DSW05 Signal Configuration Values: PMC_SLP4_N / Enable as DP_DSW05	PMC_SLP4_N
	PMC_SLP_S3_N / GP_DSW04 Signal Configuration Values: PMC_SLP3_N / Enable as GP_DSW04	PMC_SLP3_N

▼ PchThermalReporting



Parameter	Value	
Thermal Power Reporting Enabled	Yes	This setting enabled a onc

#	Parameter	Settings
---	-----------	----------

Power Tab		
2	PCH Thermal Reporting	
	Thermal Power Reporting Enabled This setting enabled a once-per-second timer interrupt is enabled which triggers firmware to report power and temperature information as enabled by configuration registers. Note: When this setting is disabled ensure that the once-per-second timer interrupt associated with this feature is also disabled.	Yes

2.1.11 Debug Tab

Click on Debug in the left tabs' menu. All regions are expanded by default. See the table below:

Debug Tab								
<div>  IDLM 1 </div> <hr/> <table> <tr> <th>Parameter</th><th>Value</th><th>Help</th></tr> <tr> <td>IDLM Binary</td><td></td><td>This allows an IDLM binary to be merged into outp</td></tr> </table>			Parameter	Value	Help	IDLM Binary		This allows an IDLM binary to be merged into outp
Parameter	Value	Help						
IDLM Binary		This allows an IDLM binary to be merged into outp						
#	Parameter	Settings						
1	IDLM							
	IDLM Binary This allows an IDLM binary to be merged into output image built by Intel® FIT.							
<div>  Delayed Authentication Mode Configuration 2 </div> <hr/> <table> <tr> <th>Parameter</th><th>Value</th><th></th></tr> <tr> <td>Delayed Authentication Mode Enabled</td><td>No</td><td>This setting enables Delayed Authentication Mo</td></tr> </table>			Parameter	Value		Delayed Authentication Mode Enabled	No	This setting enables Delayed Authentication Mo
Parameter	Value							
Delayed Authentication Mode Enabled	No	This setting enables Delayed Authentication Mo						
#	Parameter	Settings						



Debug Tab																				
2	Delayed Authentication Mode Configuration																			
	Delayed Authentication Mode Enabled Value: Yes / No This setting enables Delayed Authentication Mode on the platform.	No																		
Intel(R) Trace Hub Technology 3																				
<table border="1"> <thead> <tr> <th>Parameter</th><th>Value</th><th></th></tr> </thead> <tbody> <tr> <td>Intel(R) Trace Hub Binary</td><td></td><td>This loads the Intel(R) Trace Hub binary that</td></tr> <tr> <td>Intel(R) Trace Hub Emergency Mode Enabled</td><td>No</td><td>When enabled, Intel(R) ME programs Intel(R)</td></tr> <tr> <td>Intel(R) Trace Hub Filtering</td><td></td><td>This setting allows a user input binary for filt</td></tr> <tr> <td>Intel(R) Trace Hub Debug Messages Enabled</td><td>Yes</td><td>Intel(R) Trace Hub Debug Messages Enabled</td></tr> <tr> <td>Unlock Token</td><td></td><td>This allows the OEM to input an Unlock Toke</td></tr> </tbody> </table>			Parameter	Value		Intel(R) Trace Hub Binary		This loads the Intel(R) Trace Hub binary that	Intel(R) Trace Hub Emergency Mode Enabled	No	When enabled, Intel(R) ME programs Intel(R)	Intel(R) Trace Hub Filtering		This setting allows a user input binary for filt	Intel(R) Trace Hub Debug Messages Enabled	Yes	Intel(R) Trace Hub Debug Messages Enabled	Unlock Token		This allows the OEM to input an Unlock Toke
Parameter	Value																			
Intel(R) Trace Hub Binary		This loads the Intel(R) Trace Hub binary that																		
Intel(R) Trace Hub Emergency Mode Enabled	No	When enabled, Intel(R) ME programs Intel(R)																		
Intel(R) Trace Hub Filtering		This setting allows a user input binary for filt																		
Intel(R) Trace Hub Debug Messages Enabled	Yes	Intel(R) Trace Hub Debug Messages Enabled																		
Unlock Token		This allows the OEM to input an Unlock Toke																		
#	Parameter	Settings																		
3	Intel® Trace Hub Technology																			
	Intel® Trace Hub Binary This loads the Intel® Trace Hub binary that will be merged into the output image generated by the Intel® FIT tool.	Trace Hub Binary																		
	Intel® Trace Hub Emergency Mode Enabled Values: Yes/No This setting enable / disables Intel® Trace Hub in the firmware base image.	No																		
	Intel® Trace Hub This setting allows a user input binary for filtering of output messages for Intel(R) Trace Hub																			
	Intel® Trace Hub Debug Message Enabled Values: Yes/No This setting enables/disables the Intel® Trace Hub debug messages. Note: When enabling this setting you also need to enable Intel® Trace Hub Soft Enable setting for proper operation.	Yes																		

Debug Tab

Unlock Token

This allows the OEM to input an Unlock Token binary file for closed chassis debug.

Unlock Token Binary

▼ Intel(R) CSE Firmware Debugging Overrides

4

Parameter	Value	
Debug Override Pre-Production Silicon	0x0	Allows the OEM to control FW features to assist with pre-production platform debugging. This control has no effect if used on production silicon.
Debug Override Production Silicon	0x0	Allows the OEM to control FW features to assist with production platform debugging.
Firmware ROM Bypass	No	This setting enables / disables firmware ROM bypass.
AFS Idle Flash Reclaim Enabled	Yes	This controls enabling / disabling of Intel(R) AFS Idle Flash Reclaim.
Intel(R) CSE Reset Behavior	Intel(R) ME Alternate image boot	This setting determines Intel(R) CSE behavior after a reset.

#	Parameter	Settings
4	<div><div>Intel® ME Firmware Debugging Overrides</div><div><div><div>Debug Override Pre-Production Silicon</div><div>Allows the OEM to control FW features to assist with pre-production platform debugging. This control has no effect if used on production silicon.</div><div>Bit 0: Disable DRAM_INIT_DONE (default timeout 60 seconds)</div><div>Bit 1: Disable Host Reset Timer</div><div>Bit 2: Disable CPU_RESET_DONE timeout</div><div>Bit 3: Reserved</div><div>Bit 4: Disable Intel® CSE Power Gating</div><div>Bit 5: Reserved</div><div>Bit 6: Secure Boot debug hook. Used to shorten wait time before ENF shutdown.</div><div>Bit 7: Force real FPFs on preproduction (default is to use flash)</div><div>Bit 8: Secure Boot debug hook. Used to reduce S3 or FFS optimization tries.</div><div>Bit 9: Reserved</div><div>Bit 10: Override power package to always enter M3.</div><div>Note: Certain options do not work when the descriptor is locked.</div></div></div></div>	0x0
	<div><div>Debug Override Production Silicon</div><div>Allows the OEM to control FW features to assist with production platform debugging.</div><div>Bit 0: Extend DRAM_INIT_DONE timeout to 30 minutes (default timeout 15 seconds)</div></div>	0x0



Debug Tab																				
	Bit 1: Disable Host Reset Timer Bit 2: Disable CPU_RESET_DONE timeout Note: Certain options do not work when the descriptor is locked.																			
	Firmware ROM Bypass Values: Yes/No This setting enables / disables firmware ROM bypass. Note: This setting only has affect when the firmware being used has ROM Bypass code present	No																		
	ASF Idle Flash Reclaim Enabled Values: Yes / No This controls enabling / disable the Intel® AFS Idle flash reclaim capabilities. Note: This setting should be used for debug purposes only	Yes																		
	Intel® ME Reset Behavior This setting determines Intel® CSE behavior when boot image errors are encountered. Warning: This setting should be used for debug purposes only. Note: This may block normal Firmware functional flows.	Intel® ME Alternate image boot																		
<div> Direct Connect Interface Configuration 5 </div> <table border="1"> <thead> <tr> <th>Parameter</th><th>Value</th><th></th></tr> </thead> <tbody> <tr> <td>Direct Connect Interface (DCI) Enabled</td><td>Yes</td><td>This setting enables / disables the DCI inte</td></tr> <tr> <td>DCI BSSB over USB3 Port1 Enabled</td><td>Yes</td><td>This setting determines if the USB port beir</td></tr> <tr> <td>DCI BSSB over USB3 Port2 Enabled</td><td>Yes</td><td>This setting determines if the USB port beir</td></tr> <tr> <td>DCI BSSB over USB3 Port3 Enabled</td><td>Yes</td><td>This setting determines if the USB port beir</td></tr> <tr> <td>DCI BSSB over USB3 Port4 Enabled</td><td>Yes</td><td>This setting determines if the USB port beir</td></tr> </tbody> </table>			Parameter	Value		Direct Connect Interface (DCI) Enabled	Yes	This setting enables / disables the DCI inte	DCI BSSB over USB3 Port1 Enabled	Yes	This setting determines if the USB port beir	DCI BSSB over USB3 Port2 Enabled	Yes	This setting determines if the USB port beir	DCI BSSB over USB3 Port3 Enabled	Yes	This setting determines if the USB port beir	DCI BSSB over USB3 Port4 Enabled	Yes	This setting determines if the USB port beir
Parameter	Value																			
Direct Connect Interface (DCI) Enabled	Yes	This setting enables / disables the DCI inte																		
DCI BSSB over USB3 Port1 Enabled	Yes	This setting determines if the USB port beir																		
DCI BSSB over USB3 Port2 Enabled	Yes	This setting determines if the USB port beir																		
DCI BSSB over USB3 Port3 Enabled	Yes	This setting determines if the USB port beir																		
DCI BSSB over USB3 Port4 Enabled	Yes	This setting determines if the USB port beir																		
#	Parameter	Settings																		
5	Direct Connect Interface Configuration Note: For S0ix and reset flows BSSB should be enabled. When any of the settings below is enabled, the corresponding USB3 Combo Port in the Flex I/O Tab will be Grayed out.																			
	Direct Connect Interface (DCI) Enabled	Yes																		

Debug Tab														
	Values: Yes/No This setting enables / disables the DCI interface used for Intel® Trace Hub debugging.													
	DCI BSSB over USB3 Port 1 Enabled This setting determines if the USB port 1 has BSSB (Boundary Scan Side Band) enabled.	Yes												
	DCI BSSB over USB3 Port 2 Enabled This setting determines if the USB port 2 has BSSB (Boundary Scan Side Band) enabled.	Yes												
	DCI BSSB over USB3 Port 3 Enabled This setting determines if the USB port 3 has BSSB (Boundary Scan Side Band) enabled.	Yes												
	DCI BSSB over USB3 Port 4 Enabled This setting determines if the USB port 4 has BSSB (Boundary Scan Side Band) enabled.	Yes												
<div> <div> <div></div> <div>eSPI Feature Overrides</div> </div> <div>6</div> </div>														
<table> <tr> <th>Parameter</th><th>Value</th><th></th></tr> <tr> <td>eSPI / EC Low Frequency Debug Override</td><td>Yes</td><td>When enabled this setting will divide eSPI clock f</td></tr> </table>			Parameter	Value		eSPI / EC Low Frequency Debug Override	Yes	When enabled this setting will divide eSPI clock f						
Parameter	Value													
eSPI / EC Low Frequency Debug Override	Yes	When enabled this setting will divide eSPI clock f												
#	Parameter	Settings												
6	eSPI Feature Overrides													
	eSPI / EC Low Frequency Debug Override When enabled this setting will divide eSPI clock frequency by 8. Note: This setting should only be used for debugging purposes. Leaving this setting enable will impact eSPI performance	Yes												
<div> <div> <div></div> <div>Early USB2 DBC over Type-A Configuration</div> </div> <div>7</div> </div>														
<table> <tr> <th>Parameter</th><th>Value</th><th></th></tr> <tr> <td>USB2 DbC port enable</td><td>USB2 Port 2</td><td>This setting determines which USB2 p</td></tr> <tr> <td>USB Connectors Associated USB3 Port enable</td><td>No USB3 Ports</td><td>This setting determines which USB3 p</td></tr> <tr> <td>Enable early USB2 DbC connection</td><td>Yes</td><td>This setting enables a delay during In</td></tr> </table>			Parameter	Value		USB2 DbC port enable	USB2 Port 2	This setting determines which USB2 p	USB Connectors Associated USB3 Port enable	No USB3 Ports	This setting determines which USB3 p	Enable early USB2 DbC connection	Yes	This setting enables a delay during In
Parameter	Value													
USB2 DbC port enable	USB2 Port 2	This setting determines which USB2 p												
USB Connectors Associated USB3 Port enable	No USB3 Ports	This setting determines which USB3 p												
Enable early USB2 DbC connection	Yes	This setting enables a delay during In												
#	Parameter	Settings												
7	Early USB2 DBC over Type-A Configuration													
	Usb2 dBc PORT ENABLE Values: No USB Ports / USB2 Port 1 , 2, 3 ,4 ,5 ,6 7 , ,8 ,9 ,10	USB2 Port2												



Debug Tab											
	USB Connectors Associated USB3 Port enable Values: No USB3 Ports / USB3 Port 1, 2, 3 ,4	No USB3 Ports									
	Enable early USB2 DbC connection Values: Yes/ No	Yes									
<div><div>8</div><div>TRC Emulation</div></div> <table border="1"><thead><tr><th>Parameter</th><th>Value</th><th></th></tr></thead><tbody><tr><td>TRC Enabled</td><td>No</td><td>When enabled the TRC HIP and TRC Countermeasures are e</td></tr><tr><td>TRC Enabled (FPF)</td><td>No</td><td>When enabled the TRC HIP and TRC Countermeasures are e</td></tr></tbody></table>			Parameter	Value		TRC Enabled	No	When enabled the TRC HIP and TRC Countermeasures are e	TRC Enabled (FPF)	No	When enabled the TRC HIP and TRC Countermeasures are e
Parameter	Value										
TRC Enabled	No	When enabled the TRC HIP and TRC Countermeasures are e									
TRC Enabled (FPF)	No	When enabled the TRC HIP and TRC Countermeasures are e									
#	Parameter	Settings									
8	TRC Emulation										
	TRC Enabled Values: Yes / No This setting enables TRC HIP and TRC Countermeasures used by Intel® CSME for the detection of hardware glitches as a part of security hardening. The purpose of this setting is to allow OEMs to enable TRC for testing prior to close of manufacturing and FPF commit.	No									
	TRC Enabled (FPF) Values: Yes / No When enabled the TRC HIP and TRC Countermeasures are enabled. When manufacture is completed, this value is burned into an FPF. Note: This setting should be set to "Yes" for production platforms.	No									

2.1.12 Compute Die Straps

Click on CPU Straps in the left tabs' menu. All regions are expanded by default. See the table below:

CPU Straps Tab

▼ Compute Die Straps

Parameter	Value	
Number of Active Cores	All Cores Active	This setting controls the number of active processor cores. N
BIST Initialization	No	This setting determines if BIST will be run at platform reset after
Flex Ratio	0x0	This setting controls the maximum processor non-turbo ratio. T
Processor Boot at P1 Frequency	Yes	Processor Boot at P1 Frequency
JTAG Power Disable	No JTAG Power on C10 and L0	This setting determines if JTAG power will be maintained on C
Platform IMON	Disabled	This strap should be left at the recommended default setting.
VCC SFR OC PG Present	Yes	This setting determines if VCC SFR OC PG is present on the pl
VCC ST PG Present	Yes	This setting determines if VCC ST PG is present on the platform
VCC STG PG Present	No	This setting determines if VCC STG PG is present on the platf

#	Parameter	Settings
1	CPU Straps	
	Number of Active Cores Values: All, 1, 2, 3, 4 This setting controls the number of active processor cores. Note: This strap is intended for debugging purposes only. See BIOS Spec for more details on enabling or disabling processor cores.	All
	BIST Initialization Values: Yes/No This setting determines if BIST will be run at platform reset after BIOS requested actions. Note: This strap is intended for debugging purposes only.	No
	Flex Ratio This setting controls the maximum processor non-turbo ratio. Note: This strap is intended for debugging purposes only. See BIOS Spec for more details on maximum processor non-turbo ratio configuration.	0x0
	Processor Boot at P1 Frequency Values: Yes/No This setting determines if the processor will operate at maximum frequency at power-on and boot. Note: This strap is intended for debugging purposes only.	Yes



CPU Straps Tab		
	JTAG Power Disable Values: Yes - JTAG Power on C10 and Lower/No - No Power on C10 and Lower This setting determines if JTAG power will be maintained on C10 or lower power states. Note: This strap is intended for debugging purposes only.	No JTAG Power on C10 and Lower
	Platform IMON This strap should be left at the recommended default setting.	Disabled
	VCC SFR OC PG Present Values: Yes/No This setting determines if VCC SFR OC PG is present on the platform.	Yes
	VCC ST PG Present Values: Yes/No Note: This setting determines if VCC ST PG is present on the platform.	No
	VCC ST PG Present Values: Yes/No Note: This setting determines if VCC ST PG is present on the platform.	No
	VCC STG PG Present Values: Yes/No Note: This setting determines if VCC STG PG is present on the platform.	No

2.1.13 Flex I/O Tab

Click on Flex I/O in the left tabs' menu. All regions are expanded by default. See the table below:

Flex I/O Tab														
<div>▼ PCIe Lane Reversal Configuration 1</div> <table> <tr> <th>Parameter</th><th>Value</th><th></th></tr> <tr> <td>PCIe Controller 0 Lane Reversal Enabled</td><td>Yes</td><td>This setting allows the PCIe lanes</td></tr> </table>			Parameter	Value		PCIe Controller 0 Lane Reversal Enabled	Yes	This setting allows the PCIe lanes						
Parameter	Value													
PCIe Controller 0 Lane Reversal Enabled	Yes	This setting allows the PCIe lanes												
#	Parameter	Settings												
1	PCIe Lane Reversal Configuration													
	PCIe Controller 0 Lane Reversal Enabled Values: Yes/ No This setting allows the PCIe lanes on Controller 0 to be reversed. Note: Refer to EDS for PCIe supported port configurations.	Yes												
<div>▼ PCIe Port Configuration 2</div> <table> <tr> <th>Parameter</th><th>Value</th><th></th></tr> <tr> <td>PCIe Controller 0 (Port 0-3)</td><td>1x2, 2x1</td><td>This setting controls PCIe Port configurations for PCIe Controller 0. For further details s</td></tr> </table>			Parameter	Value		PCIe Controller 0 (Port 0-3)	1x2, 2x1	This setting controls PCIe Port configurations for PCIe Controller 0. For further details s						
Parameter	Value													
PCIe Controller 0 (Port 0-3)	1x2, 2x1	This setting controls PCIe Port configurations for PCIe Controller 0. For further details s												
#	Parameter	Settings												
2	PCIe Port Configuration													
	PCIe Controller 0 (Port 0-3) Values: 4x1, (1x2, 2x1), 2x2, 1x4 This setting controls PCIe Port configurations for PCIe Controller 0.	1x2, 2x1												
<div>▼ PCIe Multi VC Port Configuration 3</div> <table> <tr> <th>Parameter</th><th>Value</th><th>Help Text</th></tr> <tr> <td>PCIe Multi VC Controller 1</td><td>Disabled</td><td>This setting controls PCIe Port configuration for PCIe Multi VC Controller 1. For further details see Elkhart Lake EDS. (Select ,Disa.</td></tr> <tr> <td>PCIe Multi VC Controller 2</td><td>Disabled</td><td>This setting controls PCIe Port configurations for PCIe Multi VC Controller 2. For further details see Elkhart Lake EDS.</td></tr> <tr> <td>PCIe Multi VC Controller 3</td><td>x1 PCIe on Lane 6</td><td>This setting controls PCIe Port configurations for PCIe Multi VC Controller 3. For further details see Elkhart Lake Platform EDS.</td></tr> </table>			Parameter	Value	Help Text	PCIe Multi VC Controller 1	Disabled	This setting controls PCIe Port configuration for PCIe Multi VC Controller 1. For further details see Elkhart Lake EDS. (Select ,Disa.	PCIe Multi VC Controller 2	Disabled	This setting controls PCIe Port configurations for PCIe Multi VC Controller 2. For further details see Elkhart Lake EDS.	PCIe Multi VC Controller 3	x1 PCIe on Lane 6	This setting controls PCIe Port configurations for PCIe Multi VC Controller 3. For further details see Elkhart Lake Platform EDS.
Parameter	Value	Help Text												
PCIe Multi VC Controller 1	Disabled	This setting controls PCIe Port configuration for PCIe Multi VC Controller 1. For further details see Elkhart Lake EDS. (Select ,Disa.												
PCIe Multi VC Controller 2	Disabled	This setting controls PCIe Port configurations for PCIe Multi VC Controller 2. For further details see Elkhart Lake EDS.												
PCIe Multi VC Controller 3	x1 PCIe on Lane 6	This setting controls PCIe Port configurations for PCIe Multi VC Controller 3. For further details see Elkhart Lake Platform EDS.												
#	Parameter	Settings												



Flex I/O Tab											
3	PCIe Multi VC Port Configuration										
	PCIe MltVcCont1 Values: Disabled /x1 PCIe on Lane 7 /x1 PCIe on Lane 8 /x1 PCIe on Lane 10 /x2 PCIe on Lanes 8 and 9 /x2 PCIe on Lanes 10 and 11 This setting controls PCIe Port configurations for PCIe Multi VC Controller 1. For further details see Elkhart Lake EDS.	Disabled									
	PCIe MltVcCont2 Values: Disabled /x1 PCIe on Lane 2 /x1 PCIe on Lane 4 /x2 PCIe on Lanes 2 and 3 /x2 PCIe on Lanes 4 and 5 This setting controls PCIe Port configurations for PCIe Multi VC Controller 2. For further details see Elkhart Lake EDS.	Disabled									
	PCIe MltVcCont3 Values: Disabled /x1 PCIe on Lane 6 /x2 PCIe on Lanes 6 and 7 This setting controls PCIe Port configurations for PCIe Multi VC Controller 3. For further details see Elkhart Lake Platform EDS.	x1 PCIe on Lane 6									
<div> <div>▼ SATA / PCIe Combo Port Configuration</div> <div>4</div> <table border="1"> <thead> <tr> <th>Parameter</th><th>Value</th><th>Help Text</th></tr> </thead> <tbody> <tr> <td>SATA / PCIe Combo Port 0</td><td>Disabled</td><td>This setting configures the Flex I/O port to operate as either PCIe Port 10 or SATA Port 10. For further details see Elkhart Lake EDS.</td></tr> <tr> <td>SATA / PCIe Combo Port 1</td><td>Disabled</td><td>This setting configures the Flex I/O port to operate as either PCIe Port 11 or SATA Port 11. For further details see Elkhart Lake EDS.</td></tr> </tbody> </table> </div>			Parameter	Value	Help Text	SATA / PCIe Combo Port 0	Disabled	This setting configures the Flex I/O port to operate as either PCIe Port 10 or SATA Port 10. For further details see Elkhart Lake EDS.	SATA / PCIe Combo Port 1	Disabled	This setting configures the Flex I/O port to operate as either PCIe Port 11 or SATA Port 11. For further details see Elkhart Lake EDS.
Parameter	Value	Help Text									
SATA / PCIe Combo Port 0	Disabled	This setting configures the Flex I/O port to operate as either PCIe Port 10 or SATA Port 10. For further details see Elkhart Lake EDS.									
SATA / PCIe Combo Port 1	Disabled	This setting configures the Flex I/O port to operate as either PCIe Port 11 or SATA Port 11. For further details see Elkhart Lake EDS.									
#	Parameter	Settings									
4	SATA/PCIe Combo Port Configuration										
	SATA / PCIe Combo Port 0 Values: GPIO Polarity PCIe, GPIO Polarity SATA, SATA, PCIe, Disabled This setting configures the PCIe port to operate as either PCIe Port 11 or SATA Port 0.	Disabled									
	SATA / PCIe Combo Port 1 Values: GPIO Polarity PCIe, GPIO Polarity SATA, SATA, PCIe, Disabled This setting configures the PCIe port to operate as either PCIe Port 12 or SATA Port 1.	Disabled									

Flex I/O Tab

▼ USB3 Port Configuration

5

Parameter	Value	Help Text
USB3 / PCIe Combo Port 0	Disabled	This setting configures the PCIe port to operate as either PCIe Port 3 or USB3 Port 0.
USB3 / PCIe Combo Port 1	Disabled	This setting configures the PCIe port to operate as either PCIe Port 4 or USB3 Port 1.
USB3 Port 1 Connector Type Select	Type C	This setting configures the physical connector type where the Super Speed USB3 Port 1 is located.
USB3 Port 2 Connector Type Select	Type A or Type C (Host Mode Only)	This setting configures the physical connector type where the Super Speed USB3 Port 2 is located.
USB3 Port 3 Connector Type Select	Type A or Type C (Host Mode Only)	This setting configures the physical connector type where the Super Speed USB3 Port 3 is located.
USB3 Port 4 Connector Type Select	Type A or Type C (Host Mode Only)	This setting configures the physical connector type where the Super Speed USB3 Port 4 is located.
USB3 Port 1 Initialization Speed Select	USB3.1 Gen1 LBPM	This setting determines USB3 Port 1 speed during platform power-up.
USB3 Port 2 Initialization Speed Select	USB3.1 Gen1 LBPM	This setting determines USB3 Port 2 speed during platform power-up.
USB3 Port 3 Initialization Speed Select	USB3.1 Gen1 LBPM	This setting determines USB3 Port 3 speed during platform power-up.
USB3 Port 4 Initialization Speed Select	USB3.1 Gen1 LBPM	This setting determines USB3 Port 4 speed during platform power-up.
USB3 Port 1 Speed Capability	USB 3.1 Gen2	This setting determines the USB3 Port 1 speed capabilities.
USB3 Port 2 Speed Capability	USB 3.1 Gen2	This setting determines the USB3 Port 2 speed capabilities.
USB3 Port 3 Speed Capability	USB 3.1 Gen2	This setting determines the USB3 Port 3 speed capabilities.
USB3 Port 4 Speed Capability	USB 3.1 Gen2	This setting determines the USB3 Port 4 speed capabilities.

#	Parameter	Settings
5	USB3 Port Configuration Note: To align with EHL EDS, for USB ports, the signal names are numbered starting from 0, but the descriptions are numbered starting from 1	
	USB3/ PCIe Combo Port 0 Values: USB3, PCIe, Disabled This setting configures the PCIe port to operate as either PCIe Port 0 or USB3 Port 1.	Disabled
	USB3/ PCIe Combo Port 1 Values: USB3, PCIe, Disabled This setting configures the PCIe port to operate as either PCIe Port 2 or USB3 Port 2.	Disabled
	USB3 Port 1 Connector Type Select Values: Type-C, Type-AB, Type A or Type-C (Host Mode Only) This setting configures the physical connector type to be used for USB 3.0 / 3.1 Port 1.	Type C
	USB3 Port 2 Connector Type Select Values: Type-C, Type-AB, Type A or Type-C (Host Mode Only) This setting configures the physical connector type to be used for USB 3.0 / 3.1 Port 2.	Type A or Type-C (Host Mode Only)
	USB3 Port 3 Connector Type Select Values: Type-C, Type-AB, Type A or Type-C (Host Mode Only)	Type A or Type-C (Host Mode Only)



Flex I/O Tab		
	This setting configures the physical connector type to be used for USB 3.0 / 3.1 Port 3.	
	USB3 Port 4 Connector Type Select Values: Type-C, Type-AB, Type A or Type-C (Host Mode Only) This setting configures the physical connector type to be used for USB 3.0 / 3.1 Port 4.	Type A or Type-C (Host Mode Only)
	USB3 Port 1 Initialization Speed Select Values: USB3.1 Gen1 LBPM/USB3.1 Gen2 Skip LBPM This setting determines USB3 Port 1 speed during platform power-up.	USB3.1 Gen1 LBPM
	USB3 Port 2 Initialization Speed Select Values: USB3.1 Gen1 LBPM/USB3.1 Gen2 Skip LBPM This setting determines USB3 Port 2 speed during platform power-up.	USB3.1 Gen1 LBPM
	USB3 Port 3 Initialization Speed Select Values: USB3.1 Gen1 LBPM/USB3.1 Gen2 Skip LBPM This setting determines USB3 Port 3 speed during platform power-up.	USB3.1 Gen1 LBPM
	USB3 Port 4 Initialization Speed Select Values: USB3.1 Gen1 LBPM/USB3.1 Gen2 Skip LBPM This setting determines USB3 Port 4 speed during platform power-up.	USB3.1 Gen1 LBPM
	USB3 Port 1 Speed Capability Values: USB 3.1 Gen1/USB 3.1 Gen2 This setting determines the USB3 Port 1 speed capabilities.	USB 3.1 Gen2
	USB3 Port 2 Speed Capability Values: USB 3.1 Gen1/USB 3.1 Gen2 This setting determines the USB3 Port 2 speed capabilities.	USB 3.1 Gen2
	USB3 Port 3 Speed Capability Values: USB 3.1 Gen1/USB 3.1 Gen2 This setting determines the USB3 Port 3 speed capabilities.	USB 3.1 Gen2
	USB3 Port 4 Speed Capability Values: USB 3.1 Gen1/USB 3.1 Gen2 This setting determines the USB3 Port 4 speed capabilities.	USB 3.1 Gen2

Flex I/O Tab

▼ USB2 Port Configuration

6

Parameter	Value	Help Text
USB2 Port 1 Connector Type Select	Type C	This setting configures the physical connector type where the
USB2 Port 2 Connector Type Select	Type A or Type C (Host Mode I	This setting configures the physical connector type where the
USB2 Port 3 Connector Type Select	Type A or Type C (Host Mode I	This setting configures the physical connector type where the
USB2 Port 4 Connector Type Select	Type A or Type C (Host Mode I	This setting configures the physical connector type where the
USB2 Port 5 Connector Type Select	Type A or Type C (Host Mode I	This setting configures the physical connector type where the
USB2 Port 6 Connector Type Select	Type A or Type C (Host Mode I	This setting configures the physical connector type where the
USB2 Port 7 Connector Type Select	Type A or Type C (Host Mode I	This setting configures the physical connector type where the
USB2 Port 8 Connector Type Select	Type A or Type C (Host Mode I	This setting configures the physical connector type where the
USB2 Port 9 Connector Type Select	Type A or Type C (Host Mode I	This setting configures the physical connector type where the
USB2 Port 10 Connector Type Select	Type A or Type C (Host Mode I	This setting configures the physical connector type where the

#	Parameter	Settings
6	USB2 Port Configuration	
	USB2 Port 1 Connector Type Values: Type-C, Type-AB, Type A or Type-C (Host Mode Only) This setting configures the physical connector type to be used for USB2 Port 1.	Type C
	USB2 Port 2 Connector Type Values: Type-C, Type-AB, Type A or Type-C (Host Mode Only) This setting configures the physical connector type to be used for USB2 Port 2.	Type A or Type-C (Host Mode Only)
	USB2 Port 3 Connector Type Values: Type-C, Type-AB, Type A or Type-C (Host Mode Only) This setting configures the physical connector type to be used for USB2 Port 3.	Type A or Type-C (Host Mode Only)
	USB2 Port 4 Connector Type Values: Type-C, Type-AB, Type A or Type-C (Host Mode Only) This setting configures the physical connector type to be used for USB2 Port 4.	Type A or Type-C (Host Mode Only)
	USB2 Port 5 Connector Type Values: Type-C, Type-AB, Type A or Type-C (Host Mode Only) This setting configures the physical connector type to be used for USB2 Port 5.	Type A or Type-C (Host Mode Only)



Flex I/O Tab																	
	USB2 Port 6 Connector Type Values: Type-C, Type-AB, Type A or Type-C (Host Mode Only) This setting configures the physical connector type to be used for USB2 Port 6.	Type A or Type-C (Host Mode Only)															
	USB2 Port 7 Connector Type Values: Type-C, Type-AB, Type A or Type-C (Host Mode Only) This setting configures the physical connector type to be used for USB2 Port 7.	Type A or Type-C (Host Mode Only)															
	USB2 Port 8 Connector Type Values: Type-C, Type-AB, Type A or Type-C (Host Mode Only) This setting configures the physical connector type to be used for USB2 Port 8.	Type A or Type-C (Host Mode Only)															
	USB2 Port 9 Connector Type Values: Type-C, Type-AB, Type A or Type-C (Host Mode Only) This setting configures the physical connector type to be used for USB2 Port 9.	Type A or Type-C (Host Mode Only)															
	USB2 Port 10 Connector Type Values: Type-C, Type-AB, Type A or Type-C (Host Mode Only) This setting configures the physical connector type to be used for USB2 Port 10.	Type A or Type-C (Host Mode Only)															
<div>7</div> <div>▼ UFS Storage Configuration</div> <table> <thead> <tr> <th>Parameter</th><th>Value</th><th></th></tr> </thead> <tbody> <tr> <td>UFS Controller 0</td><td>None</td><td>This setting enables UFS Controller 0 in x1 or x2 mode.</td></tr> <tr> <td>UFS Controller 1</td><td>None</td><td>This setting enables UFS Controller 1 in x1 or x2 mode.</td></tr> <tr> <td>UFSX2 Enabled</td><td>Yes</td><td>This determines if UFSX2 is Enabled.</td></tr> <tr> <td>MMP UFSX2 Enabled</td><td>Yes</td><td>This determines if MMP UFSX2 is Enabled.</td></tr> </tbody> </table>			Parameter	Value		UFS Controller 0	None	This setting enables UFS Controller 0 in x1 or x2 mode.	UFS Controller 1	None	This setting enables UFS Controller 1 in x1 or x2 mode.	UFSX2 Enabled	Yes	This determines if UFSX2 is Enabled.	MMP UFSX2 Enabled	Yes	This determines if MMP UFSX2 is Enabled.
Parameter	Value																
UFS Controller 0	None	This setting enables UFS Controller 0 in x1 or x2 mode.															
UFS Controller 1	None	This setting enables UFS Controller 1 in x1 or x2 mode.															
UFSX2 Enabled	Yes	This determines if UFSX2 is Enabled.															
MMP UFSX2 Enabled	Yes	This determines if MMP UFSX2 is Enabled.															
#	Parameter	Settings															
7	UFS Storage Configuration																
	UFS Storage Configuration Values: None /X1 /X2	None															
	UFS Boot Configuration Values: None /X1 /X2	None															

Flex I/O Tab		
	UFSX2 Enabled Values: Yes / No	Yes
	MP UFSX2 Enabled Values: Yes / No	Yes
▼ M.2 Pullup Configuration 8		
Parameter	Value	
M2 Config 0 Pullup Enabled	No	This setting enables the 20k pull-up for M.2 Soc
M2 Config 1 Pullup Enabled	No	This setting enables the 20k pull-up for M.2 Soc
M2 Config 2 Pullup Enabled	Yes	This setting enables the 20k pull-up for M.2 Soc
M2 Config 3 Pullup Enabled	No	This setting enables the 20k pull-up for M.2 Soc
#	Parameter	Settings
8	M.2 Pullup Configuration	
	M2 Config 0 Pullup Enabled Values: No /Yes This setting enables the 20k pull-up for M.2 Socket Configuration 0.	No
	M2 Config 1 Pullup Enabled Values: No /Yes This setting enables the 20k pull-up for M.2 Socket Configuration 1.	No
	M2 Config 2 Pullup Enabled Values: No /Yes This setting enables the 20k pull-up for M.2 Socket Configuration 2.	Yes
	M2 Config 3 Pullup Enabled Values: No /Yes This setting enables the 20k pull-up for M.2 Socket Configuration 3.	No



Flex I/O Tab

9

▼ Power Delivery (PD) Controller Configuration

Parameter	Value	Help Text
PMC-PD Controller	Disabled	This bit should be enabled if the processor is connected to a PD controller through the SM Link interface

#	Parameter	Settings
9	Power Delivery (PD) Controller Configuration	
	PMC-PD Controller Values: Enabled/Disabled	Disabled

2.1.14 GPIO Tab

Click on GPIO in the left tabs' menu. All regions are expanded by default. See the table below:

GPIO Tab		
<div> <div>1</div> <div>GPIO VCCIO Voltage Control</div> </div>		
Parameter	Value	
GPP_A0 Individual ...	1.8Volts	This setting controls the VCCIO voltage for the GPP.
GPP_A1 Individual ...	1.8Volts	This setting controls the VCCIO voltage for the GPP.
GPP_A2 Individual ...	1.8Volts	This setting controls the VCCIO voltage for the GPP.
GPP_A3 Individual ...	1.8Volts	This setting controls the VCCIO voltage for the GPP.
GPP_A4 Individual ...	1.8Volts	This setting controls the VCCIO voltage for the GPP.
GPP_A5 Individual ...	1.8Volts	This setting controls the VCCIO voltage for the GPP.
GPP_A6 Individual ...	1.8Volts	This setting controls the VCCIO voltage for the GPP.
GPP_A7 Individual ...	1.8Volts	This setting controls the VCCIO voltage for the GPP.
GPP_A8 Individual ...	1.8Volts	This setting controls the VCCIO voltage for the GPP.
GPP_A9 Individual ...	1.8Volts	This setting controls the VCCIO voltage for the GPP.
GPP_A10 Individual...	1.8Volts	This setting controls the VCCIO voltage for the GPP.
GPP_A11 Individual...	1.8Volts	This setting controls the VCCIO voltage for the GPP.
GPP_A12 Individual...	1.8Volts	This setting controls the VCCIO voltage for the GPP.
GPP_A13 Individual...	1.8Volts	This setting controls the VCCIO voltage for the GPP.
GPP_A14 Individual...	1.8Volts	This setting controls the VCCIO voltage for the GPP.
GPP_A15 Individual...	1.8Volts	This setting controls the VCCIO voltage for the GPP.
GPP_A16 Individual...	1.8Volts	This setting controls the VCCIO voltage for the GPP.
GPP_A17 Individual...	1.8Volts	This setting controls the VCCIO voltage for the GPP.
GPP_A18 Individual...	1.8Volts	This setting controls the VCCIO voltage for the GPP.
GPP_A19 Individual...	1.8Volts	This setting controls the VCCIO voltage for the GPP.
GPP_A20 Individual...	1.8Volts	This setting controls the VCCIO voltage for the GPP.
GPP_A21 Individual...	1.8Volts	This setting controls the VCCIO voltage for the GPP.
GPP_A22 Individual...	1.8Volts	This setting controls the VCCIO voltage for the GPP.
GPP_A23 Individual...	1.8Volts	This setting controls the VCCIO voltage for the GPP.
#	Parameter	Settings
1	GPIO VCCIO Control Pins Warning: Incorrectly configuring GPIO voltages may result in MCP damage.	
	GPP_A0 Individual Voltage Select	1.8 Volts



GPIO Tab		
	GPP_A1 Individual Voltage Select	1.8 Volts
	GPP_A2 Individual Voltage Select	1.8 Volts
	GPP_A3 Individual Voltage Select	1.8 Volts
	GPP_A4 Individual Voltage Select	1.8 Volts
	GPP_A5 Individual Voltage Select	1.8 Volts
	GPP_A6 Individual Voltage Select	1.8 Volts
	GPP_A7 Individual Voltage Select	1.8 Volts
	GPP_A8 Individual Voltage Select	1.8 Volts
	GPP_A9 Individual Voltage Select	1.8 Volts
	GPP_A10 Individual Voltage Select	1.8 Volts
	GPP_A11 Individual Voltage Select	1.8 Volts
	GPP_A12 Individual Voltage Select	1.8 Volts
	GPP_A13 Individual Voltage Select	1.8 Volts
	GPP_A14 Individual Voltage Select	1.8 Volts
	GPP_A15 Individual Voltage Select	1.8 Volts
	GPP_A16 Individual Voltage Select	1.8 Volts
	GPP_A17 Individual Voltage Select	1.8 Volts
	GPP_A18 Individual Voltage Select	1.8 Volts
	GPP_A19 Individual Voltage Select	1.8 Volts
	GPP_A20 Individual Voltage Select	1.8 Volts
	GPP_A21 Individual Voltage Select	1.8 Volts
	GPP_A22 Individual Voltage Select	1.8 Volts
	GPP_A23 Individual Voltage Select	1.8 Volts

GPIO Tab		
GPP_B0 Individual ...	1.8Volts	This setting controls the VCCIO voltage for the G
GPP_B1 Individual ...	1.8Volts	This setting controls the VCCIO voltage for the G
GPP_B2 Individual ...	3.3Volts	This setting controls the VCCIO voltage for the G
GPP_B3 Individual ...	1.8Volts	This setting controls the VCCIO voltage for the G
GPP_B4 Individual ...	3.3Volts	This setting controls the VCCIO voltage for the G
GPP_B5 Individual ...	1.8Volts	This setting controls the VCCIO voltage for the G
GPP_B6 Individual ...	1.8Volts	This setting controls the VCCIO voltage for the G
GPP_B7 Individual ...	1.8Volts	This setting controls the VCCIO voltage for the G
GPP_B8 Individual ...	1.8Volts	This setting controls the VCCIO voltage for the G
GPP_B9 Individual ...	1.8Volts	This setting controls the VCCIO voltage for the G
GPP_B10 Individual...	1.8Volts	This setting controls the VCCIO voltage for the G
GPP_B11 Individual...	3.3Volts	This setting controls the VCCIO voltage for the G
GPP_B12 Individual...	3.3Volts	This setting controls the VCCIO voltage for the G
GPP_B13 Individual...	3.3Volts	This setting controls the VCCIO voltage for the G
GPP_B14 Individual...	3.3Volts	This setting controls the VCCIO voltage for the G
GPP_B15 Individual...	1.8Volts	This setting controls the VCCIO voltage for the G
GPP_B16 Individual...	3.3Volts	This setting controls the VCCIO voltage for the G
GPP_B17 Individual...	3.3Volts	This setting controls the VCCIO voltage for the G
GPP_B18 Individual...	3.3Volts	This setting controls the VCCIO voltage for the G
GPP_B19 Individual...	3.3Volts	This setting controls the VCCIO voltage for the G
GPP_B20 Individual...	3.3Volts	This setting controls the VCCIO voltage for the G
GPP_B21 Individual...	3.3Volts	This setting controls the VCCIO voltage for the G
GPP_B22 Individual...	3.3Volts	This setting controls the VCCIO voltage for the G
GPP_B23 Individual...	3.3Volts	This setting controls the VCCIO voltage for the G
#	Parameter	Settings
	GPP_B0 Individual Voltage Select	1.8 Volts
	GPP_B1 Individual Voltage Select	1.8 Volts
	GPP_B2 Individual Voltage Select	3.3 Volts



GPIO Tab		
	GPP_B3 Individual Voltage Select	1.8 Volts
	GPP_B4 Individual Voltage Select	3.3 Volts
	GPP_B5 Individual Voltage Select	1.8 Volts
	GPP_B6 Individual Voltage Select	1.8 Volts
	GPP_B7 Individual Voltage Select	1.8 Volts
	GPP_B8 Individual Voltage Select	1.8 Volts
	GPP_B9 Individual Voltage Select	1.8 Volts
	GPP_B10 Individual Voltage Select	1.8 Volts
	GPP_B11 Individual Voltage Select	3.3 Volts
	GPP_B12 Individual Voltage Select	3.3 Volts
	GPP_B13 Individual Voltage Select	3.3 Volts
	GPP_B14 Individual Voltage Select	3.3 Volts
	GPP_B15 Individual Voltage Select	1.8 Volts
	GPP_B16 Individual Voltage Select	3.3 Volts
	GPP_B17 Individual Voltage Select	3.3 Volts
	GPP_B18 Individual Voltage Select	3.3 Volts
	GPP_B19 Individual Voltage Select	3.3 Volts
	GPP_B20 Individual Voltage Select	3.3 Volts
	GPP_B21 Individual Voltage Select	3.3 Volts
	GPP_B22 Individual Voltage Select	3.3 Volts
	GPP_B23 Individual Voltage Select	3.3 Volts

GPIO Tab		
GPP_C0 Individual V.	3.3Volts	This setting controls the VCCIO voltage for the GPP_C0 GPIO pin.
GPP_C1 Individual V.	3.3Volts	This setting controls the VCCIO voltage for the GPP_C1 GPIO pin.
GPP_C2 Individual V.	3.3Volts	This setting controls the VCCIO voltage for the GPP_C2 GPIO pin.
GPP_C3 Individual V.	1.8Volts	This setting controls the VCCIO voltage for the GPP_C3 GPIO pin.
GPP_C4 Individual V.	1.8Volts	This setting controls the VCCIO voltage for the GPP_C4 GPIO pin.
GPP_C5 Individual V.	3.3Volts	This setting controls the VCCIO voltage for the GPP_C5 GPIO pin.
GPP_C6 Individual V.	1.8Volts	This setting controls the VCCIO voltage for the GPP_C6 GPIO pin.
GPP_C7 Individual V.	1.8Volts	This setting controls the VCCIO voltage for the GPP_C7 GPIO pin.
GPP_C8 Individual V.	3.3Volts	This setting controls the VCCIO voltage for the GPP_C8 GPIO pin.
GPP_C9 Individual V.	3.3Volts	This setting controls the VCCIO voltage for the GPP_C9 GPIO pin.
GPP_C10 Individual .	3.3Volts	This setting controls the VCCIO voltage for the GPP_C10 GPIO pin.
GPP_C11 Individual .	3.3Volts	This setting controls the VCCIO voltage for the GPP_C11 GPIO pin.
GPP_C12 Individual .	3.3Volts	This setting controls the VCCIO voltage for the GPP_C12 GPIO pin.
GPP_C13 Individual .	3.3Volts	This setting controls the VCCIO voltage for the GPP_C13 GPIO pin.
GPP_C14 Individual .	3.3Volts	This setting controls the VCCIO voltage for the GPP_C14 GPIO pin.
GPP_C15 Individual .	3.3Volts	This setting controls the VCCIO voltage for the GPP_C15 GPIO pin.
GPP_C16 Individual .	1.8Volts	This setting controls the VCCIO voltage for the GPP_C16 GPIO pin.
GPP_C17 Individual .	1.8Volts	This setting controls the VCCIO voltage for the GPP_C17 GPIO pin.
GPP_C18 Individual .	3.3Volts	This setting controls the VCCIO voltage for the GPP_C18 GPIO pin.
GPP_C19 Individual .	3.3Volts	This setting controls the VCCIO voltage for the GPP_C19 GPIO pin.
GPP_C20 Individual .	3.3Volts	This setting controls the VCCIO voltage for the GPP_C20 GPIO pin.
GPP_C21 Individual .	3.3Volts	This setting controls the VCCIO voltage for the GPP_C21 GPIO pin.
GPP_C22 Individual .	1.8Volts	This setting controls the VCCIO voltage for the GPP_C22 GPIO pin.
GPP_C23 Individual .	1.8Volts	This setting controls the VCCIO voltage for the GPP_C23 GPIO pin.
#	Parameter	Settings
	GPP_C0 Individual Voltage Select	3.3 Volts
	GPP_C1 Individual Voltage Select	3.3 Volts
	GPP_C2 Individual Voltage Select	3.3 Volts
	GPP_C3 Individual Voltage Select	1.8 Volts



GPIO Tab		
	GPP_C4 Individual Voltage Select	3.3 Volts
	GPP_C5 Individual Voltage Select	1.8 Volts
	GPP_C6 Individual Voltage Select	1.8 Volts
	GPP_C7 Individual Voltage Select	1.8 Volts
	GPP_C8 Individual Voltage Select	3.3 Volts
	GPP_C9 Individual Voltage Select	3.3 Volts
	GPP_C10 Individual Voltage Select	3.3 Volts
	GPP_C11 Individual Voltage Select	3.3 Volts
	GPP_C12 Individual Voltage Select	3.3 Volts
	GPP_C13 Individual Voltage Select	3.3 Volts
	GPP_C14 Individual Voltage Select	3.3 Volts
	GPP_C15 Individual Voltage Select	3.3 Volts
	GPP_C16 Individual Voltage Select	1.8 Volts
	GPP_C17 Individual Voltage Select	1.8 Volts
	GPP_C18 Individual Voltage Select	3.3 Volts
	GPP_C19 Individual Voltage Select	3.3 Volts
	GPP_C20 Individual Voltage Select	3.3 Volts
	GPP_C21 Individual Voltage Select	3.3 Volts
	GPP_C22 Individual Voltage Select	1.8 Volts
	GPP_C23 Individual Voltage Select	1.8 Volts

GPIO Tab		
GPP_D0 Individual Voltage Select	3.3Volts	This setting controls the VCCIO voltage for the GPP_D0 GPIO pin.
GPP_D1 Individual Voltage Select	3.3Volts	This setting controls the VCCIO voltage for the GPP_D1 GPIO pin.
GPP_D2 Individual Voltage Select	3.3Volts	This setting controls the VCCIO voltage for the GPP_D2 GPIO pin.
GPP_D3 Individual Voltage Select	3.3Volts	This setting controls the VCCIO voltage for the GPP_D3 GPIO pin.
GPP_D4 Individual Voltage Select	3.3Volts	This setting controls the VCCIO voltage for the GPP_D4 GPIO pin.
GPP_D6 Individual Voltage Select	3.3Volts	This setting controls the VCCIO voltage for the GPP_D6 GPIO pin.
GPP_D6 Individual Voltage Select	3.3Volts	This setting controls the VCCIO voltage for the GPP_D6 GPIO pin.
GPP_D7 Individual Voltage Select	3.3Volts	This setting controls the VCCIO voltage for the GPP_D7 GPIO pin.
GPP_D8 Individual Voltage Select	3.3Volts	This setting controls the VCCIO voltage for the GPP_D8 GPIO pin.
GPP_D9 Individual Voltage Select	1.8Volts	This setting controls the VCCIO voltage for the GPP_D9 GPIO pin.
GPP_D10 Individual Voltage Select	1.8Volts	This setting controls the VCCIO voltage for the GPP_D10 GPIO pin.
GPP_D11 Individual Voltage Select	1.8Volts	This setting controls the VCCIO voltage for the GPP_D11 GPIO pin.
GPP_D12 Individual Voltage Select	1.8Volts	This setting controls the VCCIO voltage for the GPP_D12 GPIO pin.
GPP_D13 Individual Voltage Select	3.3Volts	This setting controls the VCCIO voltage for the GPP_D13 GPIO pin.
GPP_D14 Individual Voltage Select	3.3Volts	This setting controls the VCCIO voltage for the GPP_D14 GPIO pin.
GPP_D15 Individual Voltage Select	1.8Volts	This setting controls the VCCIO voltage for the GPP_D15 GPIO pin.
GPP_D16 Individual Voltage Select	3.3Volts	This setting controls the VCCIO voltage for the GPP_D16 GPIO pin.
GPP_D17 Individual Voltage Select	1.8Volts	This setting controls the VCCIO voltage for the GPP_D17 GPIO pin.
GPP_D18 Individual Voltage Select	3.3Volts	This setting controls the VCCIO voltage for the GPP_D18 GPIO pin.
GPP_D19 Individual Voltage Select	1.8Volts	This setting controls the VCCIO voltage for the GPP_D19 GPIO pin.
#	Parameter	Settings
	GPP_D0 Individual Voltage Select	3.3 Volts
	GPP_D1 Individual Voltage Select	3.3 Volts
	GPP_D2 Individual Voltage Select	3.3 Volts
	GPP_D3 Individual Voltage Select	3.3 Volts
	GPP_D4 Individual Voltage Select	3.3 Volts
	GPP_D5 Individual Voltage Select	3.3 Volts
	GPP_D6 Individual Voltage Select	3.3 Volts
	GPP_D7 Individual Voltage Select	3.3 Volts
	GPP_D8 Individual Voltage Select	3.3 Volts
	GPP_D9 Individual Voltage Select	1.8 Volts



GPIO Tab		
	GPP_D10 Individual Voltage Select	1.8 Volts
	GPP_D11 Individual Voltage Select	1.8 Volts
	GPP_D12 Individual Voltage Select	1.8 Volts
	GPP_D13 Individual Voltage Select	3.3 Volts
	GPP_D14 Individual Voltage Select	3.3 Volts
	GPP_D15 Individual Voltage Select	1.8 Volts
	GPP_D16 Individual Voltage Select	3.3 Volts
	GPP_D17 Individual Voltage Select	1.8 Volts
	GPP_D18 Individual Voltage Select	3.3 Volts
	GPP_D19 Individual Voltage Select	1.8 Volts

GPIO Tab		
GPP_E0 Individual Voltage Select	3.3Volts	This setting controls the VCCIO voltage for the GPP_E0 GPIO pin.
GPP_E1 Individual Voltage Select	1.8Volts	This setting controls the VCCIO voltage for the GPP_E1 GPIO pin.
GPP_E2 Individual Voltage Select	3.3Volts	This setting controls the VCCIO voltage for the GPP_E2 GPIO pin.
GPP_E3 Individual Voltage Select	3.3Volts	This setting controls the VCCIO voltage for the GPP_E3 GPIO pin.
GPP_E4 Individual Voltage Select	3.3Volts	This setting controls the VCCIO voltage for the GPP_E4 GPIO pin.
GPP_E6 Individual Voltage Select	1.8Volts	This setting controls the VCCIO voltage for the GPP_E6 GPIO pin.
GPP_E7 Individual Voltage Select	3.3Volts	This setting controls the VCCIO voltage for the GPP_E7 GPIO pin.
GPP_E8 Individual Voltage Select	3.3Volts	This setting controls the VCCIO voltage for the GPP_E8 GPIO pin.
GPP_E9 Individual Voltage Select	3.3Volts	This setting controls the VCCIO voltage for the GPP_E9 GPIO pin.
GPP_E10 Individual Voltage Select	3.3Volts	This setting controls the VCCIO voltage for the GPP_E10 GPIO pin.
GPP_E11 Individual Voltage Select	3.3Volts	This setting controls the VCCIO voltage for the GPP_E11 GPIO pin.
GPP_E12 Individual Voltage Select	3.3Volts	This setting controls the VCCIO voltage for the GPP_E12 GPIO pin.
GPP_E13 Individual Voltage Select	3.3Volts	This setting controls the VCCIO voltage for the GPP_E13 GPIO pin.
GPP_E14 Individual Voltage Select	3.3Volts	This setting controls the VCCIO voltage for the GPP_E14 GPIO pin.
GPP_E15 Individual Voltage Select	3.3Volts	This setting controls the VCCIO voltage for the GPP_E15 GPIO pin.
GPP_E16 Individual Voltage Select	3.3Volts	This setting controls the VCCIO voltage for the GPP_E16 GPIO pin.
GPP_E17 Individual Voltage Select	1.8Volts	This setting controls the VCCIO voltage for the GPP_E17 GPIO pin.
GPP_E18 Individual Voltage Select	1.8Volts	This setting controls the VCCIO voltage for the GPP_E18 GPIO pin.
GPP_E19 Individual Voltage Select	1.8Volts	This setting controls the VCCIO voltage for the GPP_E19 GPIO pin.
GPP_E20 Individual Voltage Select	3.3Volts	This setting controls the VCCIO voltage for the GPP_E20 GPIO pin.
GPP_E21 Individual Voltage Select	3.3Volts	This setting controls the VCCIO voltage for the GPP_E21 GPIO pin.
GPP_E22 Individual Voltage Select	3.3Volts	This setting controls the VCCIO voltage for the GPP_E22 GPIO pin.
GPP_E23 Individual Voltage Select	3.3Volts	This setting controls the VCCIO voltage for the GPP_E23 GPIO pin.
#	Parameter	Settings
	GPP_E0 Individual Voltage Select	3.3 Volts
	GPP_E1 Individual Voltage Select	1.8 Volts
	GPP_E2 Individual Voltage Select	3.3 Volts
	GPP_E3 Individual Voltage Select	3.3 Volts
	GPP_E4 Individual Voltage Select	3.3 Volts
	GPP_E5 Individual Voltage Select	1.8 Volts
	GPP_E6 Individual Voltage Select	1.8 Volts



GPIO Tab		
	GPP_E7 Individual Voltage Select	3.3 Volts
	GPP_E8 Individual Voltage Select	3.3 Volts
	GPP_E9 Individual Voltage Select	3.3 Volts
	GPP_E10 Individual Voltage Select	3.3 Volts
	GPP_E11 Individual Voltage Select	3.3 Volts
	GPP_E12 Individual Voltage Select	3.3 Volts
	GPP_E13 Individual Voltage Select	3.3 Volts
	GPP_E14 Individual Voltage Select	3.3 Volts
	GPP_E15 Individual Voltage Select	3.3 Volts
	GPP_E16 Individual Voltage Select	3.3 Volts
	GPP_E17 Individual Voltage Select	1.8 Volts
	GPP_E18 Individual Voltage Select	1.8 Volts
	GPP_E19 Individual Voltage Select	1.8 Volts
	GPP_E20 Individual Voltage Select	3.3 Volts
	GPP_E21 Individual Voltage Select	3.3 Volts
	GPP_E22 Individual Voltage Select	3.3 Volts
	GPP_E23 Individual Voltage Select	3.3 Volts

GPIO Tab		
GPP_F0 Individual Voltage Select	1.8Volts	This setting controls the VCCIO voltage for the GPP_F0 GPIO pin.
GPP_F1 Individual Voltage Select	1.8Volts	This setting controls the VCCIO voltage for the GPP_F1 GPIO pin.
GPP_F2 Individual Voltage Select	1.8Volts	This setting controls the VCCIO voltage for the GPP_F2 GPIO pin.
GPP_F3 Individual Voltage Select	1.8Volts	This setting controls the VCCIO voltage for the GPP_F3 GPIO pin.
GPP_F4 Individual Voltage Select	3.3Volts	This setting controls the VCCIO voltage for the GPP_F4 GPIO pin.
GPP_F5 Individual Voltage Select	1.8Volts	This setting controls the VCCIO voltage for the GPP_F5 GPIO pin.
GPP_F6 Individual Voltage Select	1.8Volts	This setting controls the VCCIO voltage for the GPP_F6 GPIO pin.
GPP_F7 Individual Voltage Select	1.8Volts	This setting controls the VCCIO voltage for the GPP_F7 GPIO pin.
GPP_F8 Individual Voltage Select	1.8Volts	This setting controls the VCCIO voltage for the GPP_F8 GPIO pin.
GPP_F9 Individual Voltage Select	3.3Volts	This setting controls the VCCIO voltage for the GPP_F9 GPIO pin.
GPP_F10 Individual Voltage Select	1.8Volts	This setting controls the VCCIO voltage for the GPP_F10 GPIO pin.
GPP_F11 Individual Voltage Select	1.8Volts	This setting controls the VCCIO voltage for the GPP_F11 GPIO pin.
GPP_F12 Individual Voltage Select	1.8Volts	This setting controls the VCCIO voltage for the GPP_F12 GPIO pin.
GPP_F13 Individual Voltage Select	1.8Volts	This setting controls the VCCIO voltage for the GPP_F13 GPIO pin.
GPP_F14 Individual Voltage Select	1.8Volts	This setting controls the VCCIO voltage for the GPP_F14 GPIO pin.
GPP_F16 Individual Voltage Select	1.8Volts	This setting controls the VCCIO voltage for the GPP_F16 GPIO pin.
GPP_F16 Individual Voltage Select	1.8Volts	This setting controls the VCCIO voltage for the GPP_F16 GPIO pin.
GPP_F17 Individual Voltage Select	1.8Volts	This setting controls the VCCIO voltage for the GPP_F17 GPIO pin.
GPP_F18 Individual Voltage Select	1.8Volts	This setting controls the VCCIO voltage for the GPP_F18 GPIO pin.
GPP_F19 Individual Voltage Select	1.8Volts	This setting controls the VCCIO voltage for the GPP_F19 GPIO pin.
GPP_F20 Individual Voltage Select	3.3Volts	This setting controls the VCCIO voltage for the GPP_F20 GPIO pin.
GPP_F21 Individual Voltage Select	3.3Volts	This setting controls the VCCIO voltage for the GPP_F21 GPIO pin.
GPP_F22 Individual Voltage Select	3.3Volts	This setting controls the VCCIO voltage for the GPP_F22 GPIO pin.
GPP_F23 Individual Voltage Select	3.3Volts	This setting controls the VCCIO voltage for the GPP_F23 GPIO pin.
#	Parameter	Settings
	GPP_F0 Individual Voltage Select	1.8 Volts
	GPP_F1 Individual Voltage Select	1.8 Volts
	GPP_F2 Individual Voltage Select	1.8 Volts
	GPP_F3 Individual Voltage Select	1.8 Volts
	GPP_F4 Individual Voltage Select	3.3 Volts
	GPP_F5 Individual Voltage Select	1.8 Volts
	GPP_F6 Individual Voltage Select	1.8 Volts
	GPP_F7 Individual Voltage Select	1.8 Volts



GPIO Tab		
	GPP_F8 Individual Voltage Select	1.8 Volts
	GPP_F9 Individual Voltage Select	3.3 Volts
	GPP_F10 Individual Voltage Select	1.8 Volts
	GPP_F11 Individual Voltage Select	1.8 Volts
	GPP_F12 Individual Voltage Select	1.8 Volts
	GPP_F13 Individual Voltage Select	1.8 Volts
	GPP_F14 Individual Voltage Select	1.8 Volts
	GPP_F15 Individual Voltage Select	1.8 Volts
	GPP_F16 Individual Voltage Select	1.8 Volts
	GPP_F17 Individual Voltage Select	1.8 Volts
	GPP_F18 Individual Voltage Select	1.8 Volts
	GPP_F19 Individual Voltage Select	1.8 Volts
	GPP_F20 Individual Voltage Select	3.3 Volts
	GPP_F21 Individual Voltage Select	3.3 Volts
	GPP_F22 Individual Voltage Select	3.3 Volts
	GPP_F23 Individual Voltage Select	3.3 Volts

GPIO Tab		
GPP_G0 Individual Voltage Select	3.3Volts	This setting controls the VCCIO voltage for the GPP_G0 GPIO pin.
GPP_G1 Individual Voltage Select	3.3Volts	This setting controls the VCCIO voltage for the GPP_G1 GPIO pin.
GPP_G2 Individual Voltage Select	3.3Volts	This setting controls the VCCIO voltage for the GPP_G2 GPIO pin.
GPP_G3 Individual Voltage Select	3.3Volts	This setting controls the VCCIO voltage for the GPP_G3 GPIO pin.
GPP_G4 Individual Voltage Select	3.3Volts	This setting controls the VCCIO voltage for the GPP_G4 GPIO pin.
GPP_G5 Individual Voltage Select	3.3Volts	This setting controls the VCCIO voltage for the GPP_G5 GPIO pin.
GPP_G6 Individual Voltage Select	3.3Volts	This setting controls the VCCIO voltage for the GPP_G6 GPIO pin.
GPP_G7 Individual Voltage Select	1.8Volts	This setting controls the VCCIO voltage for the GPP_G7 GPIO pin.
GPP_G8 Individual Voltage Select	1.8Volts	This setting controls the VCCIO voltage for the GPP_G8 GPIO pin.
GPP_G9 Individual Voltage Select	1.8Volts	This setting controls the VCCIO voltage for the GPP_G9 GPIO pin.
GPP_G10 Individual Voltage Select	1.8Volts	This setting controls the VCCIO voltage for the GPP_G10 GPIO pin.
GPP_G11 Individual Voltage Select	1.8Volts	This setting controls the VCCIO voltage for the GPP_G11 GPIO pin.
GPP_G12 Individual Voltage Select	3.3Volts	This setting controls the VCCIO voltage for the GPP_G12 GPIO pin.
GPP_G13 Individual Voltage Select	1.8Volts	This setting controls the VCCIO voltage for the GPP_G13 GPIO pin.
GPP_G14 Individual Voltage Select	1.8Volts	This setting controls the VCCIO voltage for the GPP_G14 GPIO pin.
GPP_G15 Individual Voltage Select	1.8Volts	This setting controls the VCCIO voltage for the GPP_G15 GPIO pin.
GPP_G16 Individual Voltage Select	1.8Volts	This setting controls the VCCIO voltage for the GPP_G16 GPIO pin.
GPP_G17 Individual Voltage Select	1.8Volts	This setting controls the VCCIO voltage for the GPP_G17 GPIO pin.
GPP_G18 Individual Voltage Select	1.8Volts	This setting controls the VCCIO voltage for the GPP_G18 GPIO pin.
GPP_G19 Individual Voltage Select	3.3Volts	This setting controls the VCCIO voltage for the GPP_G19 GPIO pin.
GPP_G20 Individual Voltage Select	1.8Volts	This setting controls the VCCIO voltage for the GPP_G20 GPIO pin.
GPP_G21 Individual Voltage Select	1.8Volts	This setting controls the VCCIO voltage for the GPP_G21 GPIO pin.
GPP_G22 Individual Voltage Select	1.8Volts	This setting controls the VCCIO voltage for the GPP_G22 GPIO pin.
GPP_G23 Individual Voltage Select	3.3Volts	This setting controls the VCCIO voltage for the GPP_G23 GPIO pin.

#	Parameter	Settings
	GPP_G0 Individual Voltage Select	3.3 Volts
	GPP_G1 Individual Voltage Select	3.3 Volts
	GPP_G2 Individual Voltage Select	3.3 Volts
	GPP_G3 Individual Voltage Select	3.3 Volts
	GPP_G4 Individual Voltage Select	3.3 Volts
	GPP_G5 Individual Voltage Select	3.3 Volts
	GPP_G6 Individual Voltage Select	3.3 Volts
	GPP_G7 Individual Voltage Select	1.8 Volts
	GPP_G8 Individual Voltage Select	1.8 Volts



GPIO Tab		
	GPP_G9 Individual Voltage Select	1.8 Volts
	GPP_G10 Individual Voltage Select	1.8 Volts
	GPP_G11 Individual Voltage Select	1.8 Volts
	GPP_G12 Individual Voltage Select	3.3 Volts
	GPP_G13 Individual Voltage Select	1.8 Volts
	GPP_G14 Individual Voltage Select	1.8 Volts
	GPP_G15 Individual Voltage Select	1.8 Volts
	GPP_G16 Individual Voltage Select	1.8 Volts
	GPP_G17 Individual Voltage Select	1.8 Volts
	GPP_G18 Individual Voltage Select	1.8 Volts
	GPP_G19 Individual Voltage Select	3.3 Volts
	GPP_G20 Individual Voltage Select	1.8 Volts
	GPP_G21 Individual Voltage Select	1.8 Volts
	GPP_G22 Individual Voltage Select	1.8 Volts
	GPP_G23 Individual Voltage Select	3.3 Volts

GPIO Tab		
GPP_H0 Individual Voltage Select	1.8Volts	This setting controls the VCCIO voltage for the GPP_H0 GPIO pin.
GPP_H1 Individual Voltage Select	1.8Volts	This setting controls the VCCIO voltage for the GPP_H1 GPIO pin.
GPP_H2 Individual Voltage Select	1.8Volts	This setting controls the VCCIO voltage for the GPP_H2 GPIO pin.
GPP_H3 Individual Voltage Select	1.8Volts	This setting controls the VCCIO voltage for the GPP_H3 GPIO pin.
GPP_H4 Individual Voltage Select	1.8Volts	This setting controls the VCCIO voltage for the GPP_H4 GPIO pin.
GPP_H6 Individual Voltage Select	1.8Volts	This setting controls the VCCIO voltage for the GPP_H6 GPIO pin.
GPP_H6 Individual Voltage Select	1.8Volts	This setting controls the VCCIO voltage for the GPP_H6 GPIO pin.
GPP_H7 Individual Voltage Select	1.8Volts	This setting controls the VCCIO voltage for the GPP_H7 GPIO pin.
GPP_H8 Individual Voltage Select	3.3Volts	This setting controls the VCCIO voltage for the GPP_H8 GPIO pin.
GPP_H9 Individual Voltage Select	3.3Volts	This setting controls the VCCIO voltage for the GPP_H9 GPIO pin.
GPP_H10 Individual Voltage Select	3.3Volts	This setting controls the VCCIO voltage for the GPP_H10 GPIO pin.
GPP_H11 Individual Voltage Select	3.3Volts	This setting controls the VCCIO voltage for the GPP_H11 GPIO pin.
GPP_H12 Individual Voltage Select	3.3Volts	This setting controls the VCCIO voltage for the GPP_H12 GPIO pin.
GPP_H13 Individual Voltage Select	3.3Volts	This setting controls the VCCIO voltage for the GPP_H13 GPIO pin.
GPP_H14 Individual Voltage Select	3.3Volts	This setting controls the VCCIO voltage for the GPP_H14 GPIO pin.
GPP_H15 Individual Voltage Select	3.3Volts	This setting controls the VCCIO voltage for the GPP_H15 GPIO pin.
GPP_H16 Individual Voltage Select	3.3Volts	This setting controls the VCCIO voltage for the GPP_H16 GPIO pin.
GPP_H17 Individual Voltage Select	3.3Volts	This setting controls the VCCIO voltage for the GPP_H17 GPIO pin.
GPP_H18 Individual Voltage Select	3.3Volts	This setting controls the VCCIO voltage for the GPP_H18 GPIO pin.
GPP_H19 Individual Voltage Select	3.3Volts	This setting controls the VCCIO voltage for the GPP_H19 GPIO pin.
GPP_H20 Individual Voltage Select	3.3Volts	This setting controls the VCCIO voltage for the GPP_H20 GPIO pin.
GPP_H21 Individual Voltage Select	3.3Volts	This setting controls the VCCIO voltage for the GPP_H21 GPIO pin.
GPP_H22 Individual Voltage Select	3.3Volts	This setting controls the VCCIO voltage for the GPP_H22 GPIO pin.
GPP_H23 Individual Voltage Select	3.3Volts	This setting controls the VCCIO voltage for the GPP_H23 GPIO pin.
#	Parameter	Settings
	GPP_H0 Individual Voltage Select	1.8 Volts
	GPP_H1 Individual Voltage Select	1.8 Volts
	GPP_H2 Individual Voltage Select	1.8 Volts
	GPP_H3 Individual Voltage Select	1.8 Volts
	GPP_H4 Individual Voltage Select	1.8 Volts
	GPP_H5 Individual Voltage Select	1.8 Volts
	GPP_H6 Individual Voltage Select	1.8 Volts
	GPP_H7 Individual Voltage Select	1.8 Volts
	GPP_H8 Individual Voltage Select	3.3 Volts



GPIO Tab		
	GPP_H9 Individual Voltage Select	3.3 Volts
	GPP_H10 Individual Voltage Select	3.3 Volts
	GPP_H11 Individual Voltage Select	3.3 Volts
	GPP_H12 Individual Voltage Select	3.3 Volts
	GPP_H13 Individual Voltage Select	3.3 Volts
	GPP_H14 Individual Voltage Select	3.3 Volts
	GPP_H15 Individual Voltage Select	3.3 Volts
	GPP_H16 Individual Voltage Select	3.3 Volts
	GPP_H17 Individual Voltage Select	3.3 Volts
	GPP_H18 Individual Voltage Select	3.3 Volts
	GPP_H19 Individual Voltage Select	3.3 Volts
	GPP_H20 Individual Voltage Select	3.3 Volts
	GPP_H21 Individual Voltage Select	3.3 Volts
	GPP_H22 Individual Voltage Select	3.3 Volts
	GPP_H23 Individual Voltage Select	3.3 Volts

GPIO Tab		
GPP_T0 Individual Voltage Select	3.3Volts	This setting controls the VCCIO voltage for the GPP_T0 GPIO pin.
GPP_T1 Individual Voltage Select	3.3Volts	This setting controls the VCCIO voltage for the GPP_T1 GPIO pin.
GPP_T2 Individual Voltage Select	3.3Volts	This setting controls the VCCIO voltage for the GPP_T2 GPIO pin.
GPP_T3 Individual Voltage Select	3.3Volts	This setting controls the VCCIO voltage for the GPP_T3 GPIO pin.
GPP_T4 Individual Voltage Select	1.8Volts	This setting controls the VCCIO voltage for the GPP_T4 GPIO pin.
GPP_T6 Individual Voltage Select	1.8Volts	This setting controls the VCCIO voltage for the GPP_T6 GPIO pin.
GPP_T0 Individual Voltage Select	1.8Volts	This setting controls the VCCIO voltage for the GPP_T7 GPIO pin.
GPP_T8 Individual Voltage Select	3.3Volts	This setting controls the VCCIO voltage for the GPP_T8 GPIO pin.
GPP_T9 Individual Voltage Select	3.3Volts	This setting controls the VCCIO voltage for the GPP_T9 GPIO pin.
GPP_T10 Individual Voltage Select	3.3Volts	This setting controls the VCCIO voltage for the GPP_T10 GPIO pin.
GPP_T11 Individual Voltage Select	3.3Volts	This setting controls the VCCIO voltage for the GPP_T11 GPIO pin.
GPP_T12 Individual Voltage Select	3.3Volts	This setting controls the VCCIO voltage for the GPP_T12 GPIO pin.
GPP_T13 Individual Voltage Select	3.3Volts	This setting controls the VCCIO voltage for the GPP_T13 GPIO pin.
GPP_T14 Individual Voltage Select	3.3Volts	This setting controls the VCCIO voltage for the GPP_T14 GPIO pin.
GPP_T15 Individual Voltage Select	3.3Volts	This setting controls the VCCIO voltage for the GPP_T15 GPIO pin.
#	Parameter	Settings
	GPP_T0 Individual Voltage Select	3.3 Volts
	GPP_T1 Individual Voltage Select	3.3 Volts
	GPP_T2 Individual Voltage Select	3.3 Volts
	GPP_T3 Individual Voltage Select	3.3 Volts
	GPP_T4 Individual Voltage Select	1.8 Volts
	GPP_T5 Individual Voltage Select	1.8 Volts
	GPP_T6 Individual Voltage Select	1.8 Volts
	GPP_T7 Individual Voltage Select	1.8 Volts
	GPP_T8 Individual Voltage Select	3.3 Volts
	GPP_T9 Individual Voltage Select	3.3 Volts
	GPP_T10 Individual Voltage Select	3.3 Volts
	GPP_T11 Individual Voltage Select	3.3 Volts
	GPP_T12 Individual Voltage Select	3.3 Volts



GPIO Tab		
	GPP_T13 Individual Voltage Select	3.3 Volts
	GPP_T14 Individual Voltage Select	3.3 Volts
	GPP_T15 Individual Voltage Select	3.3 Volts
GPP_U0 Individual Voltage Select	1.8Volts	This setting controls the VCCIO voltage for the GPP_U0 GPIO pin.
GPP_U1 Individual Voltage Select	1.8Volts	This setting controls the VCCIO voltage for the GPP_U1 GPIO pin.
GPP_U2 Individual Voltage Select	3.3Volts	This setting controls the VCCIO voltage for the GPP_U2 GPIO pin.
GPP_U3 Individual Voltage Select	3.3Volts	This setting controls the VCCIO voltage for the GPP_U3 GPIO pin.
GPP_U4 Individual Voltage Select	1.8Volts	This setting controls the VCCIO voltage for the GPP_U4 GPIO pin.
GPP_U5 Individual Voltage Select	1.8Volts	This setting controls the VCCIO voltage for the GPP_U5 GPIO pin.
GPP_U6 Individual Voltage Select	1.8Volts	This setting controls the VCCIO voltage for the GPP_U6 GPIO pin.
GPP_U7 Individual Voltage Select	3.3Volts	This setting controls the VCCIO voltage for the GPP_U7 GPIO pin.
GPP_U8 Individual Voltage Select	1.8Volts	This setting controls the VCCIO voltage for the GPP_U8 GPIO pin.
GPP_U9 Individual Voltage Select	1.8Volts	This setting controls the VCCIO voltage for the GPP_U9 GPIO pin.
GPP_U10 Individual Voltage Select	1.8Volts	This setting controls the VCCIO voltage for the GPP_U10 GPIO pin.
GPP_U11 Individual Voltage Select	3.3Volts	This setting controls the VCCIO voltage for the GPP_U11 GPIO pin.
GPP_U12 Individual Voltage Select	1.8Volts	This setting controls the VCCIO voltage for the GPP_U12 GPIO pin.
GPP_U13 Individual Voltage Select	1.8Volts	This setting controls the VCCIO voltage for the GPP_U13 GPIO pin.
GPP_U14 Individual Voltage Select	1.8Volts	This setting controls the VCCIO voltage for the GPP_U14 GPIO pin.
GPP_U15 Individual Voltage Select	1.8Volts	This setting controls the VCCIO voltage for the GPP_U15 GPIO pin.
GPP_U16 Individual Voltage Select	1.8Volts	This setting controls the VCCIO voltage for the GPP_U16 GPIO pin.
GPP_U17 Individual Voltage Select	1.8Volts	This setting controls the VCCIO voltage for the GPP_U17 GPIO pin.
GPP_U18 Individual Voltage Select	1.8Volts	This setting controls the VCCIO voltage for the GPP_U18 GPIO pin.
GPP_U19 Individual Voltage Select	3.3Volts	This setting controls the VCCIO voltage for the GPP_U19 GPIO pin.
Intel(R) HD Audio Voltage Select	1.8Volts	This setting controls configures the VCCIO voltage for all of the Intel(R) HD Audi
UFS Voltage Select	1.8Volts	This setting controls configures the VCCIO voltage for the UFS GPIO pins.
#	Parameter	Settings
	GPP_U0 Individual Voltage Select	1.8 Volts
	GPP_U1 Individual Voltage Select	1.8 Volts
	GPP_U2 Individual Voltage Select	3.3 Volts
	GPP_U3 Individual Voltage Select	3.3 Volts
	GPP_U4 Individual Voltage Select	1.8 Volts
	GPP_U5 Individual Voltage Select	1.8 Volts

GPIO Tab		
	GPP_U6 Individual Voltage Select	1.8 Volts
	GPP_U7 Individual Voltage Select	3.3 Volts
	GPP_U8 Individual Voltage Select	1.8 Volts
	GPP_U9 Individual Voltage Select	1.8 Volts
	GPP_U10 Individual Voltage Select	1.8 Volts
	GPP_U11 Individual Voltage Select	3.3 Volts
	GPP_U12 Individual Voltage Select	1.8 Volts
	GPP_U13 Individual Voltage Select	1.8 Volts
	GPP_U14 Individual Voltage Select	1.8 Volts
	GPP_U15 Individual Voltage Select	1.8 Volts
	GPP_U16 Individual Voltage Select	1.8 Volts
	GPP_U17 Individual Voltage Select	1.8 Volts
	GPP_U18 Individual Voltage Select	1.8 Volts
	GPP_U19 Individual Voltage Select	3.3 Volts
	Intel® HD Audio Voltage Select	1.8 Volts
	UFS Voltage Select	1.8 Volts



2.1.15 Download and Execute Tab

Click on Download and Execute in the left tabs' menu. All regions are expanded by default.

Note: For details about DnX image creation requirements and dependencies, refer to the Platform Flash Tool DnX user guide available in the Intel® CSE kit

Download and Execute Tab

▼ DnX Image 1

Parameter	Value	
Platform ID	0x0	DnX Image attribute. Ignored before FPFs
BuildEnabled	No	Should Intel FIT build a DnX image
OutputFileName	\$DestDir\dnx.bin	-
DnX image private sign key path.		The path to the private key to use to sign the

#	Parameter	Settings
1	DnX Image	
	Platform ID Value: Hex This configures the Platform ID that DnX uses to verify the image is correct for the platform. Before FPFs are fused, this field is ignored and DnX will accept any image. After FPS lock, only images with this Platform ID will be accepted by DnX. Caution: Ensure that the Platform ID value is correctly populated prior to close of manufacturing on the platform.	0x0
	BuildEnabled Value: Binary Yes / No This setting determines if the Intel® FIT tool should build a DnX image	No
	OutputFileName Value: Binary File This setting allow the OEM to designate the DnX binary name for the output file.	Dnx.bin
	DnX image private sign key path This designates the path to the private key to use to sign the DnX image. This setting is only configurable when OEM signing is enabled (See Platform Integrity / OemPublicKeyHash).	

Download and Execute Tab		
<div> DnX Fuses <div>2</div> </div>		
Parameter	Value	
DnX Enabled	Yes	DnX permanent enable/disable FPF
OEM Platform ID	0x0	This setting allows OEMs to configure a Unique Platform
#	Parameter	Settings
2	DnX Fuses	
	DnX Enabled Value: Yes / No This setting enables / disables DnX. <i>Caution: Setting this option to No will permanently DnX on the platform hardware.</i>	Yes
	Platform ID Value: Hex This configures the Platform ID that DnX uses to verify the image is correct for the platform. Before FPFs are fused, this field is ignored and DnX will accept any image. After FPS lock, only images with this Platform ID will be accepted by DnX. <i>Caution: Ensure that the Platform ID value is correctly populated prior to close of manufacturing on the platform.</i>	0x0



2.1.16 Firmware Update Image Build Tab

Click on FW Update Image Build in the left tabs' menu. All regions are expanded by default.
See the table below:

Firmware Update Image Build Tab											
<div>ME Image 1</div> <table border="1"><thead><tr><th>Parameter</th><th>Value</th><th>Help Text</th></tr></thead><tbody><tr><td>ME Binary File</td><td></td><td>This loads the Embedded Controller binary that will be</td></tr></tbody></table>			Parameter	Value	Help Text	ME Binary File		This loads the Embedded Controller binary that will be			
Parameter	Value	Help Text									
ME Binary File		This loads the Embedded Controller binary that will be									
#	Parameter	Settings									
	This tab option allows the Intel® FIT tool to build only firmware update binaries it is used in combination with the 'Build Image for FWUpdate' button.										
1	ME Image										
	ME Binary Image Values: Binary File This loads the Embedded Controller binary that will be merged into the FWUpdate image generated by the Intel® FIT tool.	CSE Binary									
<div>PMC Image 2</div> <table border="1"><thead><tr><th>Parameter</th><th>Value</th><th></th></tr></thead><tbody><tr><td>PMC Max Length</td><td>0x30000</td><td>-</td></tr><tr><td>PMC Binary File</td><td></td><td>This loads the PMC binary that will be merged into the FW</td></tr></tbody></table>			Parameter	Value		PMC Max Length	0x30000	-	PMC Binary File		This loads the PMC binary that will be merged into the FW
Parameter	Value										
PMC Max Length	0x30000	-									
PMC Binary File		This loads the PMC binary that will be merged into the FW									
#	Parameter	Settings									
2	PMC Image										
	PMC Mac Length										

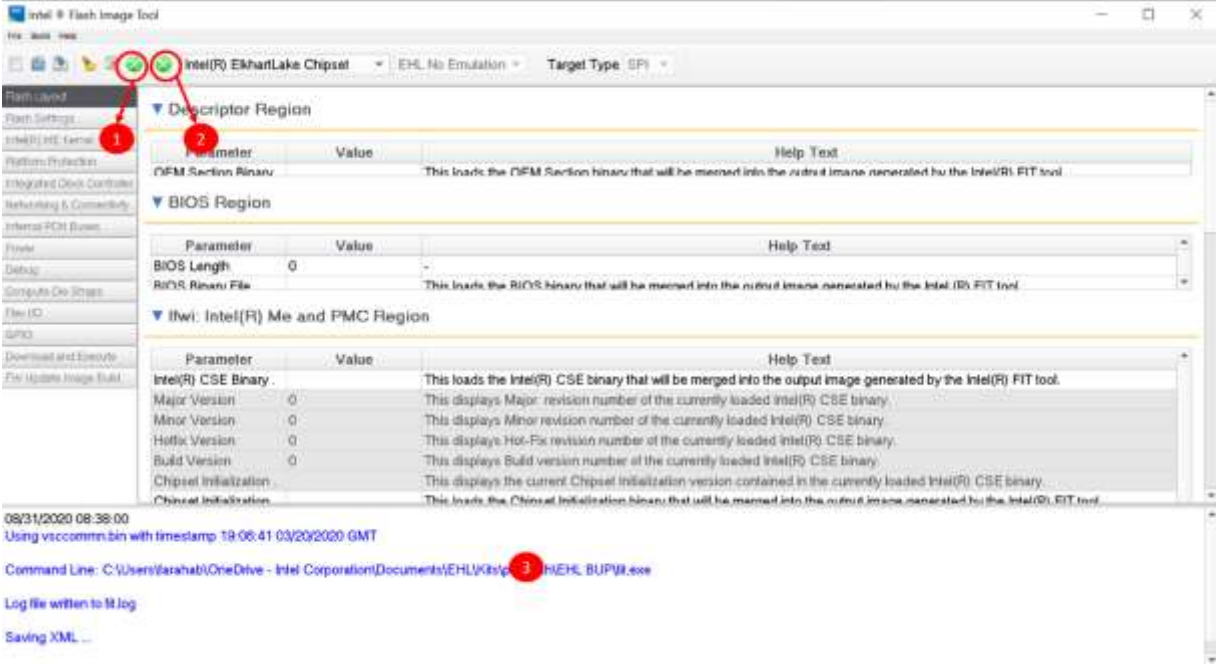
Firmware Update Image Build Tab														
	PMC Binary File This loads the PMC binary that will be merged to create a firmware update image through the Intel® FIT tool.	PMC Binary												
<div> <div> OEM KM Image </div> <div>3</div> </div> <table border="1"> <thead> <tr> <th>Parameter</th> <th>Value</th> <th></th> </tr> </thead> <tbody> <tr> <td>OEM KM</td> <td>Enabled</td> <td>This setting Enables / Disables OEM KM in the FWUpdate in</td> </tr> <tr> <td>OEM KM Max Length</td> <td>0x1000</td> <td>-</td> </tr> <tr> <td>OEM Key Manifest ...</td> <td></td> <td>This loads the OEM Key manifest binary merged into the ou</td> </tr> </tbody> </table>			Parameter	Value		OEM KM	Enabled	This setting Enables / Disables OEM KM in the FWUpdate in	OEM KM Max Length	0x1000	-	OEM Key Manifest ...		This loads the OEM Key manifest binary merged into the ou
Parameter	Value													
OEM KM	Enabled	This setting Enables / Disables OEM KM in the FWUpdate in												
OEM KM Max Length	0x1000	-												
OEM Key Manifest ...		This loads the OEM Key manifest binary merged into the ou												
#	Parameter	Settings												
3	OEM KM Image													
	OEM KM Enable Value: Enabled / Disabled This setting enables OEM Key Manifest in the firmware updated binary.													
	OEM KM Max Length													
	OEM KM Image This loads the OEM Key Manifest binary that will be merged to create a firmware update image through the Intel® FIT tool.	OEM KM Binary												
<div> <div> PCHC Image </div> <div>4</div> </div> <table border="1"> <thead> <tr> <th>Parameter</th> <th>Value</th> <th></th> </tr> </thead> <tbody> <tr> <td>PCH Configuration Max Length</td> <td>0x1000</td> <td>-</td> </tr> <tr> <td>PCH Configuration File</td> <td></td> <td>This loads the PCH Configuration bin</td> </tr> </tbody> </table>			Parameter	Value		PCH Configuration Max Length	0x1000	-	PCH Configuration File		This loads the PCH Configuration bin			
Parameter	Value													
PCH Configuration Max Length	0x1000	-												
PCH Configuration File		This loads the PCH Configuration bin												
#	Parameter	Settings												
4	PCHC Image													
	PCHC Max Length													



Firmware Update Image Build Tab														
	PCH Configuration File This loads the PCHC binary that will be merged to create a firmware update image through the Intel® FIT tool.	PCHC Binary												
▼ Intel(R) SI FW Sub-Partition 5														
<table border="1"><thead><tr><th>Parameter</th><th>Value</th><th>Help Text</th></tr></thead><tbody><tr><td>Intel(R) SI FW File</td><td></td><td>This loads the Intel(R) SI FW binary that will be merged .</td></tr><tr><td>Length</td><td>0x40000</td><td>-</td></tr><tr><td>Intel(R) SI Configurati.</td><td></td><td>Path of Intel(R) SI configuration binary</td></tr></tbody></table>			Parameter	Value	Help Text	Intel(R) SI FW File		This loads the Intel(R) SI FW binary that will be merged .	Length	0x40000	-	Intel(R) SI Configurati.		Path of Intel(R) SI configuration binary
Parameter	Value	Help Text												
Intel(R) SI FW File		This loads the Intel(R) SI FW binary that will be merged .												
Length	0x40000	-												
Intel(R) SI Configurati.		Path of Intel(R) SI configuration binary												
#	Parameter	Settings												
5	INTEL® SI FW Sub-Partition													
	INTEL® SI FW File This loads the INTEL® SI binary that will be merged to create a firmware update image through the Intel® FIT tool.	INTEL® SI binary												
	Length													
	Intel® SI Configuration file													
▼ GBST Image 6														
<table border="1"><thead><tr><th>Parameter</th><th>Value</th><th></th></tr></thead><tbody><tr><td>GBST</td><td>Enabled</td><td>This setting Enables / Disables GBST Config in the FWUpdate</td></tr><tr><td>GBST Max Length</td><td>0x8000</td><td>-</td></tr><tr><td>GBST File</td><td></td><td>This loads the GBST Condifuration binary merged into the ou</td></tr></tbody></table>			Parameter	Value		GBST	Enabled	This setting Enables / Disables GBST Config in the FWUpdate	GBST Max Length	0x8000	-	GBST File		This loads the GBST Condifuration binary merged into the ou
Parameter	Value													
GBST	Enabled	This setting Enables / Disables GBST Config in the FWUpdate												
GBST Max Length	0x8000	-												
GBST File		This loads the GBST Condifuration binary merged into the ou												
#	Parameter	Settings												
6	GBST Image													

Firmware Update Image Build Tab		
	GBST Enabled/Disabled	Enabled
	GBST Max Length	
	GBST File	GBST binary

2.2 Build Image in Intel® FIT

#	Description
	
1	Green Build button Can also select CTRL+B, or Build> Build Image from the menu bar along the top of the screen
2	Green Build button for Building FWUpdate Image Only
3	Console shows status of build and path where saved



3 Programming SPI Flash Devices and Checking Firmware Status

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

3.1 Flash Burner/Programmer

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

1. Navigate to your Output Directory (as specified in Table 2-2) where your generated SPI Flash image(s) are saved. It is assumed that this image file is named outimage.bin.

If two total SPI Flash devices were specified during the build process, then additional image files will be saved, one for each SPI Flash devices. These files are assumed to be named outimage(1).bin and outimage(2).bin.

2. Utilize a Flash burner/programmer to program the image(s). For multiple SPI Flash devices, the images are numbered sequentially to correspond to the first and second SPI Flash devices accordingly

3.2 Flash Programming Tool (Intel® FPT)

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

Note: Intel® FPT will automatically disable the Intel® CSE or EFI prior to flashing the image to the platform.

3.2.1 Intel® FPT Windows* Version

Use the following steps to program the SPI Flash devices,

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

```
fptw.exe -i
```

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

```
--- Flash Devices Found ---
```



Programming SPI Flash Devices and Checking Firmware Status

```
W25Q64BV ID:0xEF4017 Size: 8192KB (65536Kb)
W25Q64BV ID:0xEF4017 Size: 8192KB (65536Kb)
```

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

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

```
fptw.exe -f outimage.bin
```

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

```
FPT Operation Passed
```

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

2. Use fptw.exe -greset to perform a G3 power cycle

3.3 Common Bring Up Issues and Troubleshooting Table

Table 3-1: 1. Common Bring Up Issues and Troubleshooting Table

Problem / Issue	Solution / Workaround
Hear 3 beeps when platform powers on	Possible device is disconnected, or device not found, check <ul style="list-style-type: none">• platform power and processor fan power connectors• Socked DDR4 SODIMMs• USB devices (keyboard, mouse, USB key) may be plugged into inactive USB port• missing/incorrect jumpers• missing or poorly socketed processor
No display on monitor	Ensure FW SKU supports integrated graphics. Try external graphics card.
USB device not detected or does not work	USB device may be plugged into inactive USB port
System does not boot (Post Code 00)	Incorrect Flash image – possible reasons: <ul style="list-style-type: none">• wrong FW selected during Flash image build process• wrong Flash size selected Re-build image with correct settings and re-flash using Flash burner.