

Lake Field Platform Intel® Converged Security Engine Firmware 13.30

Firmware Bring Up Guide

June 2019

Revision 1.0

Intel Confidential



By using this document, in addition to any agreements you have with Intel, you accept the terms set forth below. You may not use or facilitate the use of this document in connection with any infringement or other legal analysis concerning Intel products described herein. You agree to grant Intel a non-exclusive, royalty-free license to any patent claim thereafter drafted which includes subject matter disclosed herein.

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.

The Lake Field Platform and Lake Field PCH products 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.

Any software source code reprinted in this document is furnished under a software license and may only be used or copied in accordance with the terms of that license.

64-bit computing on Intel architecture requires a computer system with a processor, chipset, BIOS, operating system, device drivers and applications enabled for Intel® 64 architecture. Processors will not operate (including 32-bit operation) without an Intel® 64 architecture-enabled BIOS. Performance will vary depending on your hardware and software configurations. Consult with your system vendor for more information.

Intel processor numbers are not a measure of performance. Processor numbers differentiate features within each processor family, not across different processor families. See http://www.intel.com/products/processor_number for details. I2C is a two-wire communications bus/protocol developed by Philips. SMBus is a subset of the I2C bus/protocol and was developed by Intel. Implementations of the I2C bus/protocol may require licenses from various entities, including Philips Electronics N.V. and North American Philips Corporation.

Microsoft*, Windows* and the Windows* logo are trademarks or registered trademarks of Microsoft Corporation in the United States and/or other countries.

Intel, Celeron, Pentium, Intel Xeon, Intel Core, and the Intel logo are trademarks of Intel Corporation in the United States and/or other countries. *Other names and brands may be claimed as the property of others.

Copyright © 2014-2019, Intel Corporation. All rights reserved.



Contents

1	Introduction	6
1.1	Related Documentation	6
1.2	Intel® CSE FW Features	6
1.3	Prerequisites	6
1.4	Acronyms and Definitions	7
1.4.1	General	7
1.4.2	Intel® Management Engine	8
1.4.3	System States and Power Management	8
1.5	Reference Documents	9
1.6	Format and Notation	9
1.7	Kit Contents	11
1.8	External Hardware Requirements for Bring Up	15
2	Image Creation: Intel® Flash Image Tool	16
2.1	Start Intel® FIT	16
2.2	Step-by-Step Guide to Build SPI / UFS Flash Image with Intel® FIT Interface	16
3	Programming SPI Flash Devices and Checking Firmware Status	81
3.1	Flash Burner/Programmer	81
3.1.1	In-Circuit SPI Flash Programming for CRB	81
3.2	Flash Programming Tool (Intel® FPT)	81
3.2.1	Intel® FPT Windows* Version	82
3.3	Checking Intel® ME Firmware Status	83
3.4	Common Bring Up Issues and Troubleshooting Table	85
A	Appendix — DnX Image Creation	86
A.1	DnX Image	86
A.1.1	Generate Key Pair for Signing	87
A.1.2	Using Intel® MEU Tool for Public key hash generation and OEMKey Manifest generation	87
B	Appendix — Intel® ICCS SKU Support Matrix	93
B.1	Intel® ICCS SKU Matrix - LKF	93
C	Appendix — Boot Guard Configuration	94
C.1	Boot Guard Profiles	94
C.2	Enforcement Policies	94
C.3	OEM Profile Parameters	95
D	Appendix — Intel® Platform Trust Technology	96
D.1	Intel® Platform Trust Technology	96



Figures

A-1	High Level setup details for DnX	86
A-2	Updating MEU_config.XML	87
A-3	Default OEM Key Manifest XML	88
A-4	Updating OEM Key Manifest XML with Public hash key.....	89
A-1	Intel® FIT -> Platform Protection.....	92
A-2	Intel® FIT -> Download and Execute.....	92
B-1	Intel® ICCS SKU Matrix - LKF.....	93

Tables

1-1	Number Format Notation.....	9
1-2	Data Format Notation	9
1-3	Kit Contents	11
2-1	Initial Screen Layout	17
2-2	Build Settings	24
2-3	Flash Layout.....	27
2-4	Flash Settings.....	31
2-5	Intel® ME Kernel.....	39
2-6	Platform Protection.....	42
2-7	Integrated Clock Controller.....	48
2-8	Internal PCH Buses	55
2-9	Power.....	58
2-10	Integrated Sensor Hub	59
2-11	Camera	61
2-12	Debug	62
2-13	CPU Straps.....	67
2-14	Flex I/O Straps	69
2-15	GPIO.....	74
2-16	Intel® Precise Touch and Stylus	75
2-17	Download and Execute.....	76
2-18	FW Update Image Build	78
2-20	Intel® FIT - Build Image	80
3-1	Common Bring Up Issues and Troubleshooting Table	85
A-1	DnX Setup Requirements.....	86
C-1	Profile Description.....	94
C-2	Enforcement Policy Description.....	94
C-3	Profile Parameters Description.....	95
D-1	Intel® Platform Trust Technology Configuration table	96



Revision History

Document Number	Revision Number	Description	Revision Date
	0.7	First external release	May 2018
	0.71	Added note on Boot Guard Profile Configuration Added FW Update Image Build tab information	May 2018
	0.8	Added Boot Guard and Intel® PTT Appendix sections Updated FIT screen captures	Sept 2018
	0.81	Added A-Step / B-Step drop down information Added Intel® FPF Anti-Rollback Configuration settings Added UFS Configuration settings Changed references from Intel® CSME to Intel® CSE	Dec 2018
	0.82	Updated DnX Image Creation Appendix chapter	March 2019
	0.83	Updated SPI frequency value	May 2019
	0.84	Removed Appendix B.2	June 2019
	1.0	Updated revision	June 2019

§ §



1 Introduction

This document covers the Intel® Converged Security Engine Firmware (Intel® CSE) 13.30 - Firmware bring up procedure. Intel® CSE is tied to essential platform functionality — this dependency cannot be avoided for engineering reasons.

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

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

For more details on SPI Flash layout, see the document **SPI & Block Media Programming Guide** and [Appendix A](#). Once the SPI Flash image is built, it will be programmed to the target based platform and the platform will be booted. This document also covers any tests and checks required to ensure that this boot process is successful and that Intel® CSE Corporate FW is operating as expected.

1.1 Related Documentation

1.2 Intel® CSE FW Features

This firmware release includes the following applications:

- Platform Clocks – Tune clock silicon to the parameters of a specific board, configure clocks at run time, and power management clocks. **Benefit:** Allows extensive customization and soft control of “Third generation” clock solution and makes clocks available before CPU powers up.
- Silicon Workaround Capability – Intel® CSE FW will have limited capabilities to perform targeted workarounds for silicon issues. **Benefit:** Allows Intel® CSE FW to address some issues that otherwise would require a new silicon stepping.

1.3 Prerequisites

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

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

This document makes only the following limited assumptions regarding hardware:

- The platform is Lake Field based



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

1.4 Acronyms and Definitions

1.4.1 General

Acronym or Term	Definition
BIOS	Basic Input Output System
Block Media	Refers to non-serial flash block media devices (i.e. UFS, eMMC etc.)
DIMM	Dual In-line Memory Module
DMI	Direct Media Interface
EC	Embedded Controller
FPF	Field Programmable Fuses
FW	Firmware
GbE	Gigabit Ethernet
HECI	Host Embedded Controller Interface (aka Intel® MEI)
Intel® ICCS	Intel® Integrated Clock Controller Service
Intel® CSE	Intel® Converged Security Engine (Intel® CSE)
Intel® MEI	Intel® Management Engine Interface (Intel® MEI) (renamed from HECI)
Intel® PTT	Intel® Platform Trusted Technology (Intel® PPT)
Intel® MSS	Intel® Management and Security Status Application
LAN	Local Area Network
MCP	Multi-Chip Package (Central Processing Unit / Platform Controller Hub)
NVM	Non-Volatile Memory
OS	Operating System
PAVP	Protected Audio and Video Path
PCI	Peripheral Component Interconnect
PCIe*	Peripheral Component Interconnect Express
PHY	Physical Layer (Networking)
RTC	Real Time Clock
SMBus	System Management Bus
SPI Flash	Serial Peripheral Interface Flash
TPM	Trusted Platform Module
UFS	A Type of non-serial flash block media devices
VSCC	Vendor Specific Configuration



1.4.2 Intel® Management Engine

Acronym or 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® Management Engine Firmware.
Host Service/Application	An application that is running on the host CPU
INF	An information file (.inf) used by Microsoft* operating systems that supports the Plug & Play feature. When installing a driver, this file provides the OS the necessary information about driver filenames, driver components, and supported hardware.
Intel® Converged Security Engine Interface (Intel® MEI)	Interface between the Intel® Converged Security 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
MECI	ME-VE Communication Interface
NVM	Non-Volatile Memory: A type of memory that will retain its contents even if power is removed. In the Intel® 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® Management Engine Firmware when it leaves the OEM factory. At this stage the Intel® Management Engine Firmware is not functional and must be configured.

1.4.3 System States and Power Management

Acronym or Term	Definition
G3	A system state of Mechanical Off where all power is disconnected from the system. G3 power state does not necessarily indicate that RTC power is removed.
CM0	Intel® Converged Security Engine 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 Management Engine 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.



Acronym or Term	Definition
Snooze Mode	Intel® Converged Security Engine activities are mostly suspended to save power. The Intel® Converged Security Engine monitors HW activities and can restore its activities depending on the HW event.
Standby	System state where the OS state is saved in memory and resumed from the memory when mouse/keyboard is clicked.
Sx	All S states which are different than S0.

1.5 Reference Documents

Document	Doc Number/ Location*
<i>Lake Field Intel® Converged Security Engine (Intel® CSE) and Embedded Controller Interaction Product Specification Revision 0.5</i>	TBD / CDI
Intel® Converged Security and Management Engine: <i>BIOS Writers Guide</i>	TBD / *
Intel® Converged Security Engine: <i>(Intel® CSE) 13.30 SKU Firmware Compliance Guide for Lake Field PCH Chipset Family - Lake Field Platform Compliance and Testing Guide - Revision 1.1</i>	TBD / CDI

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

1.6 Format and Notation

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

Table 1-1. Number Format Notation

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

Table 1-2. Data Format Notation

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



Table 1-2. Data Format Notation

Data Type	Notation	Size
Megabyte	MB	1,048,576 bytes or 1024 KB
Gigabit	Gb	1,073,741,824 bits
Gigabyte	GB	1024 MB



1.7 Kit Contents

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

Table 1-3. Kit Contents (Sheet 1 of 4)

File or [Directory]	Content Description
[root]	Root directory
	This document
	How to program SPI device parameters and descriptor region details. Also contains a complete SPI Flash softstrap reference.
[Image Components]	
[BIOS]	
	BIOS image only for Intel CRB.
[PMC]	
[CSE]	
	Intel® CSE firmware image (Non Production FW Rom Bypass) - supports unfused Kabylake PCH Platform I/O MCP steppings: <ul style="list-style-type: none"> • Unfused (Super SKU) Note: For PAVP Testing , you must match Production FW with Production Part and Non Production FW with Non Production Parts.
[Dekel PHY]	
[DnX]	
[Fwupdate_bin]	
[3rd Party Licenses in FW]	
[Installers]	
[3rd Party Licenses in SW]	
[WindowsDriverPackages]	
[ME_SW_MSI]	
[Tools]	
[ICC_Tools]	
	ICC Tools User Guide



Table 1-3. Kit Contents (Sheet 2 of 4)

File or [Directory]	Content Description
[CCT]	
	Exe file
	Ini file
	Exe file
[EFI]	
	CCT for EFI
[System Tools]	
	Sybase Open Watcom Public License version 1.0 document.
	System Tools User Guide
[Flash Image Tool]	
	Intel® Flash Image Tool (Intel® FIT)
	FITC Configuration XML file
	Binary containing the supported SPI parts
	Documentation listing the SPI parts supported by vscccommn.bin
[Flash Programming Tool]	
[DOS]	
	List of supported SPI Flash devices with specific Flash parameters
	Intel® FPT for DOS
[EFI 64]	
	List of supported SPI Flash devices with specific Flash parameters
	Intel® FPT for EFI
[Windows]	
	List of supported SPI Flash devices with specific Flash parameters
	Intel® FPT for Windows*
[Windows64]	
	List of supported SPI Flash devices with specific Flash parameters
	Intel® FPT for Windows* (64-bit) OS
[FWUpdate]	
[EFI 64]	
	FW Update Tool (EFI version)
[DOS]	



Table 1-3. Kit Contents (Sheet 3 of 4)

File or [Directory]	Content Description
	FW Update Tool (DOS version)
[Win]	
	FW Update Tool (Windows* version 32bit)
[Win64]	
	FW Update Tool (Windows* version 64bit)
[Manifest Extension Utility]	
[Win]	
	Intel® Manifest Extension Utility (MEU) executable file that allows input of FW binary and outputs and independent updatable partition that is compressed and signed.
[MEInfo]	
[DOS]	
	Intel® CSE Information Tool (DOS version)
[EFI 64]	
	Intel® CSE Information Tool (EFI version)
[Windows]	
	Intel® CSE Information Tool (Windows* version 32bit)
[Windows64]	
	Intel® CSE Information Tool (Windows* version 64bit)
[MEManuf]	
[DOS]	
	Intel® CSE Manufacturing Tool (DOS version)
	Binary containing the supported SPI parts
	Documentation listing the SPI parts supported by vscccommn.bin
[EFI 64]	
	Documentation listing the SPI parts supported by vscccommn.bin
	Intel® CSE Manufacturing Tool (EFI version)
	Binary containing the supported SPI parts
[Windows]	
	Intel® CSE Manufacturing Tool (Windows* version 32bit)

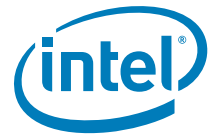





Table 1-3. Kit Contents (Sheet 4 of 4)

File or [Directory]	Content Description
<div></div>	
	Binary containing the supported SPI parts
	Documentation listing the SPI parts supported by vscccommn.bin
	[Windows64]
	Intel® CSE Manufacturing Tool (Windows* version 64bit)
	Binary containing the supported SPI parts
	Documentation listing the SPI parts supported by vscccommn.bin



1.8 External Hardware Requirements for Bring Up

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

Windows* OS System	Flash Burner	DOS Bootable USB Key
		
<p>Equipment:</p> <ul style="list-style-type: none"> Laptop or desktop that supports win32 applications <p>Purpose:</p> <ul style="list-style-type: none"> Will run firmware image assembly and build process software. 	<p>Equipment:</p> <ul style="list-style-type: none"> (Optional) For platforms that don't boot, a Flash Chip Programmer will be required For platforms that can boot to DOS or Windows*, a Intel® FPT is provided in this kit <p>Purpose:</p> <ul style="list-style-type: none"> Will burn firmware images onto the target system Flash device(s). 	<p>Equipment:</p> <ul style="list-style-type: none"> A DOS Bootable USB Key (Size > 512 MB) <p>Purpose:</p> <ul style="list-style-type: none"> Acting as a bootable device and will be used to run Intel® FPT (fpt.exe) directly on the system that is undergoing Bring Up process. Or will be used to transfer a firmware image onto a Flash burner.

§ §



2 Image Creation: Intel® Flash Image Tool

Intel® Flash Image Tool (Intel® FIT) can be used to generate either a full SPI Flash binary image with Descriptor, GbE, 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: The Flash Image Tool may be updated throughout the release cycles. As a general rule, please ensure you use the tools, images and other content from the same kit and refrain from using different version tools.

2.1 Start Intel® FIT

1. Invoke Intel® Flash Image Tool. Using Explorer*, navigate to **[root]\Tools\System Tools\Flash Image Tool**. Verify that the directory contents are correct (see [Section 1.7](#)). Double-click **FIT.exe**.
2. **NOTE:** In the tables below, where default settings are listed for Lake Field, if the value is the same one value will be listed. If there is a different default value when the program loads with either platform, both values will be listed to show the difference.

2.2 Step-by-Step Guide to Build SPI / UFS Flash Image with Intel® FIT Interface



Table 2-1. Initial Screen Layout (Sheet 1 of 7)

#	Label	Contents
1	New	This button labeled 'New' on rollover allows opening of a new session with default values
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 (see page 23)
5	Build Settings	This button labeled 'Build Settings' brings up the build settings popup Window see (Table 2-2)
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' on rollover allows build of firmware update image.



Table 2-1. Initial Screen Layout (Sheet 2 of 7)

#	Label	Contents
8	Drop Down Selector	This drop down allows selection of platform chipset Stepping is being used
9	Drop Down Selector	This drop down allows selection of SKU within platform selected
10	Dialog Box	This shows which boot media is being used by the Intel® CSE firmware binary



Table 2-1. Initial Screen Layout (Sheet 3 of 7)

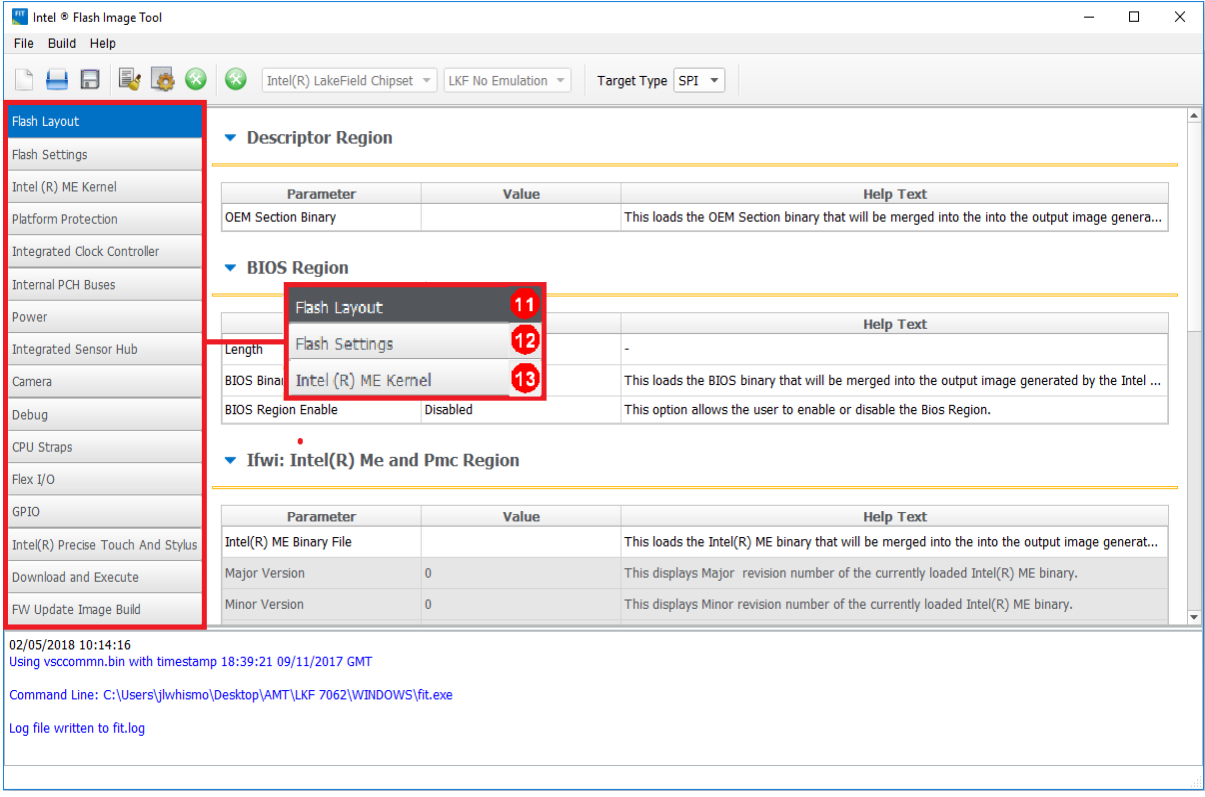
#	Label	Contents
		
11	Flash Layout Tab	Flash Layout which contains (see Table 2-3): <ul style="list-style-type: none"> • Descriptor Region • BIOS Region • IFWI: Intel® ME and PMC Region • SubPartitions • PDR Region
12	Flash Settings Tab	Flash Settings which contains (see Table 2-4): <ul style="list-style-type: none"> • Flash Components • Host CPU/ BIOS Master Access • Intel® ME Master Access • Flash Configuration • VSCC Table - VSCC Entry • BIOS Configuration • OEM and Platform IDs • FPF Configuration • Boot Media Policies
13	Intel® ME Kernel Tab	Intel® ME Kernel which contains (see Table 2-5): <ul style="list-style-type: none"> • Processor • Intel® ME Firmware Update • Image Identification • Firmware Diagnostics • Post Manufacturing Lock • Intel® ME Boot Configuration



Table 2-1. Initial Screen Layout (Sheet 4 of 7)

#	Label	Contents
14	Platform Protection Tab	Platform Protection which contains (see Table 2-6): <ul style="list-style-type: none"> Content Protection Hash Key Configuration for Bootguard / ISH Boot Guard Configuration Intel® PTT Configuration TPM Over SPI Bus Configuration BIOS Guard Configuration
15	Integrated Clock Controller Tab	Integrated Clock Controller which contains (see Table 2-7): <ul style="list-style-type: none"> Integrated Clock Controller Policies Profiles
16	Internal PCH Buses Tab	Internal PCH Buses which contains (see Table 2-8): <ul style="list-style-type: none"> PCH Timer Configuration OPI /DMI Configuration eSPI Configuration I2C Configuration



Table 2-1. Initial Screen Layout (Sheet 5 of 7)

#	Label	Contents
17	Power Tab	Power which contains (see Table 2-9): <ul style="list-style-type: none"> Platform Power PCH Thermal Reporting
18	Integrated Sensor Hub Tab	Integrated Sensor Hub which contains (see Table 2-10): <ul style="list-style-type: none"> Integrated Sensor Hub ISH Image ISH Data
19	Camera	<ul style="list-style-type: none"> IPU Security (see Table 2-11): IPU Debug
20	Debug Tab	Debug which contains (see Table 2-12): <ul style="list-style-type: none"> IDLM Delayed Authentication Mode Configuration Intel® Trace Hub Technology Intel® ME Firmware Debugging Overrides Direct Connection Interface Configuration Early USB DBC over Type-A Configuration eSPI Feature Overrides



Table 2-1. Initial Screen Layout (Sheet 6 of 7)

#	Label	Contents
21	CPU Straps Tab	CPU Straps which contain a detailed list of parameters (see Table 2-13) <ul style="list-style-type: none"> CPU Straps
22	Flex I/O Tab	Flex I/O which contains (see Table 2-14): <ul style="list-style-type: none"> PCIe Lane Reversal Configuration PCIe Port Configuration USB3 Port Configuration USB2 Port Configuration Type-C Subsystem Configuration PCIe PLL Reference Clock Source XHCI Port Configuration
23	GPIO Tab	GPIO which contains (see Table 2-15): <ul style="list-style-type: none"> ME Feature Pins Touch Controller Pins
24	Intel® Precise Touch and Stylus	Intel® Precise Touch and Stylus which contains (see Table 2-16): <ul style="list-style-type: none"> Integrated Touch Configuration Intel® Integrated Touch and Stylus Configuration



Table 2-1. Initial Screen Layout (Sheet 7 of 7)

#	Label	Contents
25	Download and Execute	<ul style="list-style-type: none">• DnX Configuration (see Table 2-17):• USB Descriptor
26	FW Update Image	<ul style="list-style-type: none">• FW Update Image Build (see Table 2-18):• ME Image• PMC Image• OEM KM Image• Dekel PHY Image• ISH Image• IUNINT Image
27	Console Window Area	Displays opening messages, log file entries, and build activity messages



Table 2-2. Build Settings (Sheet 1 of 3)

Click on Build Button in the top menu bar> Build Settings window pop up is displayed:			
#	Parameter	CRB	Values
1	Output Path		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 - default is outimage.bin in the same folder as Intel® FIT tool
2	Generate Intermediate Files	Yes	Yes/No - Yes is default
3	Enable Boot Guard warning message at build time	Yes	Yes/No - Yes is default

**Table 2-2. Build Settings (Sheet 2 of 3)**

Click on Build Button in the top menu bar> Build Settings window pop up is displayed:			
4	Enable Intel(R) Platform Trust Technology warning message at build time	Yes	Yes/No - Yes is default



Table 2-2. Build Settings (Sheet 3 of 3)

Click on Build Button in the top menu bar > Build Settings window pop up is displayed:			
#	Parameter	CRB	Values
5	Region Order	Yes	53241 - is default
6	Target Type	SPI / UFS	Shows which Target Type has been selected from the toolbar.
7	IFWI Build Version	Yes	0x0 is default
8	Redundancy Enabled	True/False	This enables redundancy support for critical components.
9	Intel® Manifest Extension Utility Path	File Path	This setting determines the file path for the Intel® Manifest Utility program.
10	Signing Tool Path	File Path	This setting determines the file path for the Signing Tool program.
11	Signing Tool	OpenSSL/ MobileSigning Util	This setting determines is the Signing Tool is using OpenSSL or MobileSigningUtil for signatures.
12			\$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 Manageability Engine kit



Table 2-3. Flash Layout (Sheet 1 of 4)

Click on Flash Layout in the left tabs menu> Descriptor Region is expanded by default:																			
<div> <div>▼ Descriptor Region</div> <div>1</div> <table> <tr> <th>Parameter</th><th>Value</th><th colspan="2"></th></tr> <tr> <td>OEM Section Binary</td><td></td><td colspan="2">This loads the OEM Sec</td></tr> </table> </div>				Parameter	Value			OEM Section Binary		This loads the OEM Sec									
Parameter	Value																		
OEM Section Binary		This loads the OEM Sec																	
#	Parameter	Target Type	Settings																
1	Flash Layout - Descriptor Region																		
	OEM Section Binary This loads the OEM Section binary that will be merged into the output image generated by the Intel® FIT tool.	SPI	OEM Binary (optional)																
		UFS	N/A																
Click on Flash Layout in the left tabs menu> BIOS Region is expanded by default:																			
<div> <div>▼ BIOS Region</div> <div>2</div> <table> <tr> <th>Parameter</th><th>Value</th><th colspan="2">Help Text</th></tr> <tr> <td>Length</td><td>0</td><td colspan="2">-</td></tr> <tr> <td>BIOS Binary File</td><td></td><td colspan="2">This loads the BIOS binary that will be merged</td></tr> <tr> <td>BIOS Region Enable</td><td>Enabled</td><td colspan="2">This option allows the user to enable or disabl</td></tr> </table> </div>				Parameter	Value	Help Text		Length	0	-		BIOS Binary File		This loads the BIOS binary that will be merged		BIOS Region Enable	Enabled	This option allows the user to enable or disabl	
Parameter	Value	Help Text																	
Length	0	-																	
BIOS Binary File		This loads the BIOS binary that will be merged																	
BIOS Region Enable	Enabled	This option allows the user to enable or disabl																	
#	Parameter	Target Type	Settings																
2	Flash Layout - BIOS Region																		
	BIOS Region - Length	SPI	0																
		UFS	0																
	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.	SPI	biosimage.bin																
		UFS	biosimage.bin																
Click on Flash Layout in the left tabs menu> Intel® ME Region is expanded by default:																			



Table 2-3. Flash Layout (Sheet 2 of 4)

▼ Ifwi: Intel(R) Me and Pmc Region 3			
Parameter	Value	Help Text	
IFWI Layout	Layout 1.6	This setting determine which IFWI layout the platfo	
Length	0	-	
Intel(R) ME Binary File		This loads the Intel(R) ME binary that will be merge	
Major Version	0	This displays Major revision number of the current	
Minor Version	0	This displays Minor revision number of the currentl	
Hotfix Version	0	This displays Hot-Fix revision number of the curren	
Build Version	0	This displays Build version number of the currently	
Chipset Initialization Version		This displays the current Chipset Initialization versi	
Chipset Initialization Binary		This loads the Chipset Initialization binary that will	
ChipsetInit Override Version		This displays the version of the Chipset Initializtion	
Intel(R) Trace Hub Binary		This loads the Intel(R) Trace Hub binary that will b	
PMC Binary File		This loads the PMC binary that will be merged into	
Version	0	-	
#	Parameter	Target Type	Settings
3	Flash Layout - IFWI: Intel® ME and Pmc Region		
	Intel® ME Binary File Navigate to your Source Directory (as specified in Table 2-2) and switch to the ME 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 meimage.bin file, check that the ME region is enabled in tool before building image.	SPI	meimage.bin
		UFS	meimage.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.		
	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.	SPI	Chipset.bin (Optional)
		UFS	Chipset.bin (Optional)
	ChipsetInit Override Version - This displays the version of the Chipset Initialization Binary override if specified.		



Table 2-3. Flash Layout (Sheet 3 of 4)

	PMC Binary File - This loads the PMC binary that will be merged into the output image generated by the Intel® FIT tool.	SPI	PMC.bin
		UFS	PMC.bin
	PMC Length	SPI	
		UFS	
	Version - This displays the version of PMC		
Click on Flash Layout in the left tabs menu> IUnit Sub-Partition is expanded by default:			
▼ IUnit Sub-Partition 4			
Parameter	Value	Help Te	
IUnit Binary File		This loads the IUnit binary that will be merged into	
Length	0xA000	-	
#	Parameter	Target Type	Settings
4	Flash Layout - IUnit Sub-Partition		
	IUNIT Sub-Partition Binary This loads the IUnit Sub Partition binary that will be merged into the output image generated by the Intel® FIT tool.	SPI	Iunit.bin (Optional)
		UFS	Iunit.bin (Optional)
	IUNIT Length	SPI	
		UFS	
Click on Flash Layout in the left tabs menu> PCH Configuration Sub-Partition is expanded by default:			
▼ PCH Configuration Sub-Partition 5			
Parameter	Value	Help T	
PCH Configuration File		This loads the PCH Configuration binary that will b	
Length	0x1000	-	
#	Parameter	Target Type	Settings
5	Flash Layout - PCH Configuration Sub-Partition		
	PCH Configuration Binary This loads the PCH Configuration binary containing ICC data that will be merged into the output image generated by the Intel® FIT tool.	SPI	PCHC.bin
		UFS	PCHC.bin
	PCH Configuration Length	SPI	
		UFS	
Click on Flash Layout in the left tabs menu> PDR Region is expanded by default:			



Table 2-3. Flash Layout (Sheet 4 of 4)

▼ PDR Region 6			
Parameter	Value	Help Text	
Length	0	-	
PDR Binary File		This loads the Platform Data region binary th	
PDR Region Enable	Disabled	This option allows the user to enable or disab	
#	Parameter	Target Type	Settings
6	Flash Layout - PDR Region		
	PDR Region - Length Region is disabled by default. Displays Region size information when Binary input file is specified.	SPI	0
		UFS	0
	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.	SPI	PDR.bin (Optional)
		UFS	N/A
	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.	SPI	Disabled
		UFS	Disabled



Table 2-4. Flash Settings (Sheet 1 of 8)

Click on Flash Settings in the left tabs menu> Flash Components is expanded by default:			
<div> <div>▼ Flash Components</div> <div>1</div> </div>			
Parameter	Value		
Number of Flash Components	1	Specifies the number of Flash components	
Flash component 1 Size	16MB	This field identifies the size of the 1st Flash	
Flash component 2 Size	8MB	This field identifies the size of the 2nd Flash	
SPI Voltage Select	3.3 Volts	This strap sets the internal control signal c	
SPI Global Protected Range	0x0	Sets the default value of the Global Protec	
SPI Idle to Deep Power Down T...	0x5	SPI Idle to Deep Power Down Timeout Def	
SPI Out of Order operation Ena...	Yes	When this setting is enabled priority opera	
SPI Resume Hold-off Delay	4us	Specifies the time after the completion of	
SPI Max write / erase Resume ...	No Ceiling	This setting specifies the maximum value 1	
SPI Suspend / Resume Enabled	Yes	When this setting is enabled writes and er	
#	Parameter	Target Type	Settings
1	Flash Settings - Flash Components		
	Number of 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.	SPI	1
		UFS	N/A
	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.	SPI	32MB
		UFS	N/A
	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'.	SPI	Greyed Out
		UFS	N/A
	SPI Voltage Select Values: 1.8 Volts, 3.3 Volts - This strap sets the internal control signal on the pad for either 1.8 or 3.3 volts. See Lake Field LP SPI Programming Guide for further details.	SPI	3.3 Volts
		UFS	N/A
	SPI Global Protected Range - This sets the default value of the Global Protected Range register in the SPI Flash Controller.	SPI	0x0
		UFS	N/A
	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.	SPI	0x5
		UFS	N/A
	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.	SPI	Yes
		UFS	N/A



Table 2-4. Flash Settings (Sheet 2 of 8)

	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.	SPI	4us
		UFS	N/A
	SPI Max write / erase Resume to Suspend intervals - This setting specifies the maximum value for the write and erase Resume to Suspend intervals.	SPI	No Ceiling
		UFS	N/A
	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.	SPI	Yes
		UFS	N/A
	Software Re-Binding Enabled Values: Yes/No When enabled this setting allows for SPI rebinding to a new PCH during manufacturing flow prior to platform EOM. Note: Rebinding to a replacement PCH can only be done a maximum of 5 time before the SPI part needs to be re-flashed.	SPI	No
		UFS	N/A

Click on Flash Layout in the left tabs menu> BIOS Region is expanded by default:

▼ Host CPU / BIOS Master Access

2

Parameter	Value	Help Text
Host CPU / BIOS Write Access Intel Recommended	0xFFFF	This setting determines write access control
Host CPU / BIOS Write Access Custom	0x0	This setting determines write access control
Host CPU / BIOS Read Access Intel Recommended	0xFFFF	This setting determines read access control
Host CPU / BIOS Read Access Custom	0x0	This setting determines read access control

#	Parameter	Target Type	Settings
2	Flash Settings - Host CPU / BIOS Master Access		
	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). 0x010A = Production with access to EC 0x011A = Production with access to EC and PDR Custom = User custom Host / BIOS Write Access values For further details on Region Access Control see Lake Field LP SPI Programming guide further details.	SPI	0xFFFF
		UFS	N/A
	Host CPU / BIOS Write Access Custom - This setting allows free form user customized Host CPU / BIOS Write Access regions permissions Note: This setting is grayed out unless Custom is selected under the Host CPU / BIOS Write Access Intel Recommended drop down menu. Warning: Setting region access permission values outside of Intel recommendation could result in compromised platform security	SPI	Hex Input
		UFS	N/A



Table 2-4. Flash Settings (Sheet 3 of 8)

	Host CPU / BIOS Read Access Values: 0xFFFF, 0x000F, 0x001F, 0x010F, 0x011F - This setting determines read access control for the BIOS region. 0xFFFF = Debug/Manufacturing 0x000F = Production 0x001F = Production with access to PDR (should ONLY be used if PDR region is implemented). 0x010F = Production with access to EC 0x011F = Production with access to EC and PDR Custom = User custom Host / BIOS Read Access values For further details on Region Access Control see Lake Field LP SPI Programming guide.	SPI	0xFFFF															
		UFS	N/A															
	Host CPU / BIOS Read Access Custom - This setting allows free form user customized Host CPU / BIOS Read Access regions permissions Note: This setting is grayed out unless Custom is selected under the Host CPU / BIOS Read Access Intel Recommended drop down menu. Warning: Setting region access permission values outside of Intel recommendation could result in compromised platform security	SPI	Hex Input															
		UFS	N/A															
Click on Flash Settings in the left tabs menu> Intel® ME Master Access is expanded by default:																		
▼ Intel(R) ME Master Access <div>3</div>																		
<table><tr><th>Parameter</th><th>Value</th><th>Help Text</th></tr><tr><td>Intel(R) ME Write Access Intel Recomendaded</td><td>0xFFFF</td><td>This setting determines read access control for the</td></tr><tr><td>Intel(R) ME Write Access Custom</td><td>0x0</td><td>This setting determines read access control for the</td></tr><tr><td>Intel(R) ME Read Access Intel Recomendaded</td><td>0xFFFF</td><td>This setting determines read access control for the</td></tr><tr><td>Intel(R) ME Read Access Custom</td><td>0x0</td><td>This setting determines read access control for the</td></tr></table>				Parameter	Value	Help Text	Intel(R) ME Write Access Intel Recomendaded	0xFFFF	This setting determines read access control for the	Intel(R) ME Write Access Custom	0x0	This setting determines read access control for the	Intel(R) ME Read Access Intel Recomendaded	0xFFFF	This setting determines read access control for the	Intel(R) ME Read Access Custom	0x0	This setting determines read access control for the
Parameter	Value	Help Text																
Intel(R) ME Write Access Intel Recomendaded	0xFFFF	This setting determines read access control for the																
Intel(R) ME Write Access Custom	0x0	This setting determines read access control for the																
Intel(R) ME Read Access Intel Recomendaded	0xFFFF	This setting determines read access control for the																
Intel(R) ME Read Access Custom	0x0	This setting determines read access control for the																
#	Parameter	Target Type	Settings															
<div>3</div>	Flash Settings - Intel® ME Master Access																	
	Intel® ME Write Access Intel Recommended Values: 0xFFFF, 0x0004 - This setting determines write access control for the Intel® CSE region. 0xFFFF = Debug/Manufacturing 0x0004 = Production 0x000C = Production Custom = User custom Intel® CSE Write Access values For further details on Region Access Control see Lake Field SPI / UFS Programming guide further details.	SPI	0xFFFF															
		UFS	N/A															
	Intel® ME Write Access Custom - This setting allows free form user customized Intel® CSE Write Access regions permissions Note: This setting is grayed out unless Custom is selected under the Intel® CSE Write Access Intel Recommended drop down menu. Warning: Setting region access permission values outside of Intel recommendation could result in compromised platform security	SPI	Hex Input															
		UFS	N/A															



Table 2-4. Flash Settings (Sheet 4 of 8)

	Intel® ME Read Access Intel Recommended Values: 0xFFFF, 0x000D - This setting determines read access control for the Intel® CSE region. 0xFFFF = Debug/Manufacturing 0x000D = Production Custom = User custom Intel® CSE Read Access values For further details on Region Access Control see Lake Field SPI / UFS Programming guide further details.	SPI	0xFFFF
		UFS	N/A
	Intel® ME Read Access Custom - This setting allows free form user customized Intel® CSE Read Access regions permissions Note: This setting is grayed out unless Custom is selected under the Intel® CSE Read Access Intel Recommended drop down menu. Warning: Setting region access permission values outside of Intel recommendation could result in compromised platform security	SPI	Hex Input
		UFS	N/A
Click on Flash Layout in the left tabs menu> Flash Configuration is expanded by default:			
<div>▼ Flash Configuration<div>4</div></div>			



Table 2-4. Flash Settings (Sheet 5 of 8)

	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. See Lake Field LP SPI Programming guide for further details.	SPI	Yes
		UFS	N/A
	Dual Output Read Enabled Values: Yes/No - This setting allows the customer to enable support for Dual Output Read capabilities for flash components. See Lake Field LP SPI Programming guide for further details.	SPI	Yes
		UFS	N/A
	Fast Read Clock Frequency Values: 14MHz, 25MHz, 50MHz - This setting allows the customer to configure the flash component clock frequency setting for Fast Read. See Lake Field LP SPI Programming guide for further details.	SPI	50MHz
		UFS	N/A
	Fast Read Supported Values: Yes/No - This setting allows the customer to enable support for Fast Read capabilities for flash components. See Lake Field LP SPI Programming guide for further details. 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.	SPI	Yes
		UFS	N/A
	Invalid Instruction 0 - This setting allows the customer to configure invalid instruction to protect against Chip Erase. See Lake Field LP SPI Programming guide for further details. Note: This setting should be set to '0' if there are not Invalid instructions.	SPI	0x00000021
		UFS	N/A
	Invalid Instruction 1 - This setting allows the customer to configure invalid instruction to protect against Chip Erase. See Lake Field LP SPI Programming guide for further details. Note: This setting should be set to '0' if there are not Invalid instructions.	SPI	0x00000042
		UFS	N/A
	Invalid Instruction 2 - This setting allows the customer to configure invalid instruction to protect against Chip Erase. See Lake Field LP SPI Programming guide for further details. Note: This setting should be set to '0' if there are not Invalid instructions.	SPI	0x00000060
		UFS	N/A
	Invalid Instruction 3 - This setting allows the customer to configure invalid instruction to protect against Chip Erase. See Lake Field LP SPI Programming guide for further details. Note: This setting should be set to '0' if there are not Invalid instructions.	SPI	0x000000AD
		UFS	N/A
	Invalid Instruction 4 - This setting allows the customer to configure invalid instruction to protect against Chip Erase. See Lake Field LP SPI Programming guide for further details. Note: This setting should be set to '0' if there are not Invalid instructions.	SPI	0x000000B7
		UFS	N/A
	Invalid Instruction 5 - This setting allows the customer to configure invalid instruction to protect against Chip Erase. See Lake Field LP SPI Programming guide for further details. Note: This setting should be set to '0' if there are not Invalid instructions.	SPI	0x000000B9
		UFS	N/A
	Invalid Instruction 6 - This setting allows the customer to configure invalid instruction to protect against Chip Erase. See Lake Field LP SPI Programming guide for further details. Note: This setting should be set to '0' if there are not Invalid instructions.	SPI	0x000000C4
		UFS	N/A
	Invalid Instruction 7 - This setting allows the customer to configure invalid instruction to protect against Chip Erase. See Lake Field LP SPI Programming guide for further details. Note: This setting should be set to '0' if there are not Invalid instructions.	SPI	0x000000C7
		UFS	N/A
	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. See Lake Field LP SPI Programming guide for further details.	SPI	Yes
		UFS	N/A
	Quad Output Read Enabled Values: Yes/No - This setting allows the customer to enable support for Quad Output Read capabilities for flash components. See Lake Field LP SPI Programming guide for further details.	SPI	Yes
		UFS	N/A
	Read ID and Read Status clock frequency Values: 14MHz, 25MHz, 50MHz - This setting allows the customer to configure the flash component clock frequency setting for Read ID and Read Status. See Lake Field LP SPI Programming guide for further details.	SPI	50MHz
		UFS	N/A



Table 2-4. Flash Settings (Sheet 6 of 8)

	Write and Erase clock frequency Values: 14MHz, 25MHz, 50MHz - This setting allows the customer to configure the flash component clock frequency setting for Write and Erase. See Lake Field / Coffee Lake LP SPI Programming guide for further details.	SPI	50MHz
		UFS	N/A

Click on Flash Settings in the left tabs menu> Legacy VSCC Table is expanded by default:

▼ Legacy VSCC Table **5**

▼ VSCC Entries **6**

W25Q128BV **7** + Add VSCC Entry

Parameter	Value	Help Text
Part Name	W25Q128BV	This setting allow the OEM input a name designation for each flash...
Vendor ID	0xEF	This configures the JEDEC vendor specific byte ID of the SPI flash ...
Device ID 0	0x40	This configures the JEDEC device specific byte ID 0 of the SPI flas...
Device ID 1	0x18	This configures the JEDEC device specific byte ID 1 of the SPI flas...

#	Parameter	Target Type	Settings
5	Flash Settings - VSCC Table VSCC Entries		
	W25Q128BV		
6	VSCC Entry		
	Name - 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 component operation.	SPI	Winbond
		UFS	N/A
	Vendor ID - This configures the JEDEC vendor specific byte ID of the SPI flash component. See Lake Field LP SPI Programming guide for further details.	SPI	0xEF
		UFS	N/A
	Device ID 0 - This configures the JEDEC device specific byte ID 0 of the SPI flash component. See Lake Field LP SPI Programming guide for further details.	SPI	0x40
		UFS	N/A
	Device ID 1 - This configures the JEDEC device specific byte ID 1 of the SPI flash component. See Lake Field LP SPI Programming guide for further details.	SPI	0x18
		UFS	N/A
7	+ Add VSCC Entry		

Click on Flash Settings in the left tabs menu> BIOS Configuration is expanded by default:



Table 2-4. Flash Settings (Sheet 7 of 8)

▼ Bios Configuration 8			
Parameter	Value	Help	
Top Swap Block Size	64KB	This configures the Top Swap Block size for th	
BIOS Boot Select	Boot from SPI	This setting determines if BIOS will be booted	
#	Parameter	Target Type	Settings
8	Flash Settings - BIOS Configuration		
	Top Swap Block Size Values: 64KB, 128KB, 256KB, 512KB, 1MB This configures the Top Swap Block size for the platform. For further details see Lake Field LP Platform Controller Hub EDS.	SPI UFS	64KB N/A
Click on Flash Settings in the left tabs menu > OEM and Platform IDs			
▼ OEM and Platform IDs 9			
Parameter	Value	Help Te	
OEM Vendor ID	0x0	This setting allows OEMs to configure their Unique	
OEM Platform ID	0x0	This setting allows OEMs to configure a Unique Pla	
#	Parameter	Target Type	Settings
9	Flash Settings - OEM and Platform IDs		
	OEM Vendor ID This is a free form 32bit field that allows the OEM to configure their unique Vendor identifier in the firmware image.	SPI UFS	
	OEM Platform ID This is a free form 32bit field that allows the OEM to configure their unique platform identifier in the firmware image.	SPI UFS	
Click on Flash Settings in the left tabs menu> BIOS Configuration is expanded by default:			
▼ FPF Configuration 10			
Parameter	Value	H	
FPF Hardware Binding Enabled	Disabled	This setting configures the FPF Hardware b	
#	Parameter	Target Type	Settings



Table 2-4. Flash Settings (Sheet 8 of 8)

10	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.	SPI	Disabled									
		UFS	Disabled									
Click on Flash Settings in the left tabs menu> BIOS Media Policies is expanded by default:												
▼ Boot Media Policies11												
<table><tr><th>Parameter</th><th>Value</th><th></th></tr><tr><td>Boot Media Sx Reset Policy</td><td>BM_Reset# Not Asserted</td><td>This setting determine that behavior</td></tr><tr><td>Boot Media Second Reset Policy</td><td>BM_Reset# Not Asserted</td><td>This setting determine that behavior</td></tr></table>				Parameter	Value		Boot Media Sx Reset Policy	BM_Reset# Not Asserted	This setting determine that behavior	Boot Media Second Reset Policy	BM_Reset# Not Asserted	This setting determine that behavior
Parameter	Value											
Boot Media Sx Reset Policy	BM_Reset# Not Asserted	This setting determine that behavior										
Boot Media Second Reset Policy	BM_Reset# Not Asserted	This setting determine that behavior										
#	Parameter	Target Type	Settings									
11	Boot Media Policies											
	Boot Media Sx Reset Policy Values: BM_Reset# Asserted / BM_Reset# Not Asserted This setting determines the behavior of Boot Media Sx Reset.	SPI	BM_Reset# Not Asserted									
		UFS	BM_Reset# Not Asserted									
	Boot Media Second Reset Policy Values: BM_Reset# Asserted / BM_Reset# Not Asserted This setting determines the behavior of Boot Media Second Reset.	SPI	BM_Reset# Not Asserted									
		UFS	BM_Reset# Not Asserted									



Table 2-5. Intel® ME Kernel (Sheet 1 of 3)

Click on Intel® ME Kernel in the left tabs menu> Processor is expanded by default:															
<div>▼ Processor 1</div> <table> <tr> <th>Parameter</th><th>Value</th><th colspan="2">Help Text</th></tr> <tr> <td>Processor Emulation</td><td>No Emulation</td><td colspan="2">-</td></tr> </table>				Parameter	Value	Help Text		Processor Emulation	No Emulation	-					
Parameter	Value	Help Text													
Processor Emulation	No Emulation	-													
#	Parameter	Target Type	Settings												
1	Intel® ME Kernel - Processor														
	Processor Emulation Values: No Emulation EMULATE Intel® vPro (TM) capable Processor EMULATE Intel® Core (TM) branded Processor EMULATE Intel® Celeron (R) branded Processor EMULATE Intel® Pentium (R) branded Processor EMULATE Intel® Xeon (R) branded Processor EMULATE Intel® Xeon (R) Manageability capable Processor This setting determines processor type to be emulated on pre-production silicon. Set this parameter to the type of processor that the target system will use during production. This field will emulate that processor class for pre-production silicon.	SPI UFS	No Emulation No Emulation												
Click on Intel® ME Kernel in the left tabs menu> Intel® ME Firmware Update is expanded by default:															
<div>▼ Intel (R) ME Firmware Update 2</div> <table> <tr> <th>Parameter</th><th>Value</th><th colspan="2">Help Text</th></tr> <tr> <td>Firmware Update OEM ID</td><td>00000000-0000-0000-0000-000...</td><td colspan="2">-</td></tr> <tr> <td>Intel(R) ME Region Flash Prot...</td><td>Yes</td><td colspan="2">-</td></tr> </table>				Parameter	Value	Help Text		Firmware Update OEM ID	00000000-0000-0000-0000-000...	-		Intel(R) ME Region Flash Prot...	Yes	-	
Parameter	Value	Help Text													
Firmware Update OEM ID	00000000-0000-0000-0000-000...	-													
Intel(R) ME Region Flash Prot...	Yes	-													
#	Parameter	Target Type	Settings												
2	Intel® ME Kernel - 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.	SPI UFS	0 string 0 string												
	Intel® ME Region Flash Protection Override Values: Yes/No This setting enables descriptor unlock of the Intel® CSE Region when the HMRFPD message is sent to firmware prior to BIOS End of POST.	SPI UFS	Yes N/A												
Click on Intel® ME Kernel in the left tabs menu> Image Identification is expanded by default:															



Table 2-5. Intel® ME Kernel (Sheet 2 of 3)

▼ Image Identification 3			
Parameter	Value	Help Text	
OEM Tag	0x00000000	-	
#	Parameter	Target Type	Settings
3	Intel® ME Kernel - Image Identification		
	OEM Tag	SPI	0x00000000
	This is a free form 32bit field that allows the OEM to configure their own unique identifier in the firmware image.	UFS	0x00000000
Click on Intel® ME Kernel in the left tabs menu> Firmware Diagnostics is expanded by default:			
▼ Firmware Diagnostics 4			
Parameter	Value	Help Text	
Automatic Built in Self Test	Disabled	-	
#	Parameter	Target Type	Settings
4	Intel® ME Kernel - Firmware Diagnostics		
	Automatic Built in Self Test	SPI	Disabled
	Values: Enabled/Disabled	UFS	Disabled
	This setting enables the firmware Automatic Built in Self Test which is executed during first platform boot after initial image flashing.		
Click on Intel® ME Kernel in the left tabs menu> Post Manufacturing Lock is expanded by default:			
▼ Post Manufacturing Lock 5			
Parameter	Value	Help Text	
Post Manufacturing NVAR Configuration Enabled	Yes	This setting determines if modifications to Cust	
#	Parameter	Target Type	Settings
5	Intel® ME Kernel - Post Manufacturing Lock		
	Post Manufacturing NVAR Configuration Enabled	SPI	Yes
	This setting determines if modifications to Customer configurable NVARs is to be allowed after close of manufacturing.	UFS	Yes
Click on Intel® ME Kernel in the left tabs menu> Intel® ME Boot Configuration is expanded by default:			



Table 2-5. Intel® ME Kernel (Sheet 3 of 3)

▼ Intel (R) ME Boot Configuration 6			
Parameter		Value	
Persistent PRTC Backup Power		Exists	FPF that indicates if the device is designed
#	Parameter	Target Type	Settings
6	Intel® ME Kernel - Intel® ME Boot Configuration		
	Persistent PRTC Backup Power Values: None / Exists	SPI	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.	UFS	Exists



Table 2-6. Platform Protection (Sheet 1 of 6)

Click on Platform Protection in the left tabs menu> Content Protection is expanded by default:			
<div> <div>▼ Content Protection</div> <div>1</div> </div>			
Parameter	Value		
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	Target Type	Settings
1	Platform Protection - Content Protection		
	PAVP Supported Values: Yes/No This setting determines if the Protected Audio Video Path (PAVP) feature will be permanently disabled in the FW image.	SPI	Yes
		UFS	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.	SPI	None
		UFS	None
	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.	SPI	None
		UFS	None
Click on Platform Protection in the left tabs menu> Hash Key Configuration for Bootguard / ISH is expanded by default:			
<div> <div>▼ Hash Key Configuration for Bootguard / ISH</div> <div>3</div> </div>			
Parameter	Value		
OEM Public Key Hash	00 00 00 00 00 00 00 00 00 00 ...	Raw hash string for the SHA-256 hash of the OEM Public Key	
OEM Key Manifest Binary		Signed manifest file containing hashes of the OEM Public Key and the OEM Private Key	
#	Parameter	Target Type	Settings
3	Platform Protection - Hash Key Configuration for Bootguard / ISH		



Table 2-6. Platform Protection (Sheet 2 of 6)

	OEM Public Key Hash This option is for entering the raw hash string or certificate file for Boot Guard and ISH. This 256-bit field represents the SHA-256 hash of the OEM public key corresponding to the private key used to sign the BIOS-SM or ISH image. Please see Appendix F for further details.	SPI	0x00000000
		UFS	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).	SPI	
		UFS	
Click on Platform Protection in the left tabs menu> Boot Guard Configuration is expanded by default:			
▼ Boot Guard Configuration <div>4</div>			
Parameter		Value	
Key Manifest ID		0	
Boot Guard Profile Configuration		Boot Guard Profile 0 - No_FVME	
CPU Debugging		Enabled	
BSP Initialization		Enabled	
S3 Optimization		Enabled	
#	Parameter	Target Type	Settings
4	Platform Protection - 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.	SPI	0x0
		UFS	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.	SPI	Boot Guard Profile 0 - No_FVME
		UFS	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.	SPI	Enabled
		UFS	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).	SPI	Enabled
		UFS	Enabled



Table 2-6. Platform Protection (Sheet 3 of 6)

	S3 Optimization Values: Enabled/Disabled	SPI	Enabled
	This setting overrides Boot Guard S3 optimization. <i>Note: Used for testing only.</i>	UFS	Enabled
Click on Platform Protection in the left tabs menu> Intel® PTT Configuration is expanded by default:			
▼ Intel(R) PTT Configuration 5			
Parameter		Value	
Intel(R) PTT Supported		Yes	This setting permanently disables
Intel(R) PTT initial power-up state		Enabled	-
Intel(R) PTT Supported [FPF]		Yes	This setting will permanently disa
#	Parameter	Target Type	Settings
5	Platform Protection - Intel® PTT Configuration		
	Intel® PTT initial power-up state Values: Enabled/Disabled This setting determines if Intel® PTT is enabled on platform power-up.	SPI	Enabled
		UFS	Enabled
	Intel® PTT Supported Values: Yes/No This setting permanently disables Intel® PTT in the firmware image.	SPI	Yes
		UFS	Yes
	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.	SPI	Yes
		UFS	Yes
Click on Platform Protection in the left tabs menu> TPM Over SPI Bus Configuration is expanded by default:			
▼ TPM Over SPI Bus Configuration 6			
Parameter		Value	
TPM Clock Frequency		17MHz	This setting determines the clock frequency setting to be used fo...
TPM Over SPI Bus Enabled		No	This setting determines if TPM over SPI bus is enabled on the pl...
#	Parameter	Target Type	Settings
6	Platform Protection - TPM Over SPI Bus Configuration		



Table 2-6. Platform Protection (Sheet 4 of 6)

	TPM Clock Frequency Values: 17MHz, 30MHz, 48MHz This setting determines the clock frequency setting to be used for the TPM over SPI bus.	SPI	17MHz
		UFS	17MHz
	TPM Over SPI Bus Enabled Values: Yes/No This setting determines if TPM over SPI bus is enabled on the platform.	SPI	No
		UFS	No
Click on Platform Protection in the left tabs menu> BIOS Guard Configuration is expanded by default:			
▼ BIOS Guard Configuration 7			
Parameter	Value	Help Text	
BIOS Guard Protection Override Enabled	No	This setting allows BIOS Guard to bypass SPI flash controller	
#	Parameter	Target Type	Settings
7	Platform Protection - BIOS Guard Configuration		
	BIOS Guard Protection Override Enabled This setting allows BIOS Guard to bypass SPI flash controller protections (i.e. Protected Range Registers and Top Swap).	SPI	No
		UFS	N/A
Click on Platform Protection in the left tabs menu> Intel FPF Anti-Rollback Configuration is expanded by default:			
▼ Intel FPF Anti-Rollback Configuration 8			
Parameter	Value	Help Text	
FPF SVN Enabled	Disabled	This option enables usage of Intel FPF for Antiroll	
RBE SVN Enabled	Disabled	This option enables usage of Intel FPF for Antiroll	
IDL M SVN Enabled	Disabled	This option enables usage of Intel FPF for Antiroll	
DNX SVN Enabled	Disabled	This option enables usage of Intel FPF for Antiroll	
OEM Key Manifest SVN Enabled	Disabled	This option enables usage of Intel FPF for Antiroll	
PMC SVN Enabled	Disabled	This option enables usage of Intel FPF for Antiroll	
uCode SVN Enabled	Disabled	This option enables usage of Intel FPF for Antiroll	
NWLD SVN Enabled	Disabled	This option enables usage of Intel FPF for Antiroll	
OS SVN Enabled	Disabled	This option enables usage of Intel FPF for Antiroll	
CPU FW SVN Enabled	Disabled	This option enables usage of Intel FPF for Antiroll	
Secure Boot Key Manifest SVN Enabled	Disabled	This option enables usage of Intel FPF for Antiroll	
Secure Boot Key Manifest SVN Enabled	Disabled	This option enables usage of Intel FPF for Antiroll	
ROT KM SVN Enabled	Disabled	This option enables usage of Intel FPF for Antiroll	
OBB SVN Enabled	Disabled	This option enables usage of Intel FPF for Antiroll	



Table 2-6. Platform Protection (Sheet 5 of 6)

#	Parameter	Target Type	Settings
8	Platform Protection - Intel FPF Anti-Rollback Configuration		
	FPF SVN Enabled Values: Enabled / Disabled / Custom This setting enables the Intel® FPF Anti-Rollback mechanism for all firmware components. Note: Individual firmware component enable / disable can be done by selecting the Custom option.	SPI	Disabled
		UFS	Disabled
	RBE SVN Enabled Values: Enabled / Disabled This setting enables the Intel® FPF Anti-Rollback mechanism for the RBE firmware component.	SPI	Disabled
		UFS	Disabled
	IDLM SVN Enabled Values: Enabled / Disabled This setting enables the Intel® FPF Anti-Rollback mechanism for the IDLM firmware component.	SPI	Disabled
		UFS	Disabled
	DNX SVN Enabled Values: Enabled / Disabled This setting enables the Intel® FPF Anti-Rollback mechanism for the DNX firmware component.	SPI	Disabled
		UFS	Disabled
	OEM Key Manifest SVN Enabled Values: Enabled / Disabled This setting enables the Intel® FPF Anti-Rollback mechanism for the OEM Key Manifest firmware component.	SPI	Disabled
		UFS	Disabled
	PMC SVN Enabled Values: Enabled / Disabled This setting enables the Intel® FPF Anti-Rollback mechanism for the PMC firmware component.	SPI	Disabled
		UFS	Disabled
	uCode SVN Enabled Values: Enabled / Disabled This setting enables the Intel® FPF Anti-Rollback mechanism for the uCode firmware component.	SPI	Disabled
		UFS	Disabled
	NWLD SVN Enabled Values: Enabled / Disabled This setting enables the Intel® FPF Anti-Rollback mechanism for the NWLD firmware component.	SPI	Disabled
		UFS	Disabled
	OS SVN Enabled Values: Enabled / Disabled This setting enables the Intel® FPF Anti-Rollback mechanism for the OS firmware component.	SPI	Disabled
		UFS	Disabled
	CPU FW SVN Enabled Values: Enabled / Disabled This setting enables the Intel® FPF Anti-Rollback mechanism for the CPU FW firmware component.	SPI	Disabled
		UFS	Disabled
	Secure Boot Key Manifest SVN Enabled Values: Enabled / Disabled This setting enables the Intel® FPF Anti-Rollback mechanism for the Secure Boot Key Manifest firmware component.	SPI	Disabled
		UFS	Disabled
	Secure Boot Key Manifest SVN Enabled Values: Enabled / Disabled This setting enables the Intel® FPF Anti-Rollback mechanism for the Secure Boot Key Manifest firmware component.	SPI	Disabled
		UFS	Disabled



Table 2-6. Platform Protection (Sheet 6 of 6)

	ROT KM SVN Enabled Values: Enabled / Disabled This setting enables the Intel® FPF Anti-Rollback mechanism for the ROT KM firmware component.	SPI	Disabled
		UFS	Disabled
	OOB SVN Enabled Values: Enabled / Disabled This setting enables the Intel® FPF Anti-Rollback mechanism for the OOB firmware component.	SPI	Disabled
		UFS	Disabled



Table 2-7. Integrated Clock Controller (Sheet 1 of 7)

Click on Integrated Clock Controller in the left tabs menu> Integrated Clock Controller Policies are expanded by default:

▼ Integrated Clock Controller Policies

1

Parameter	Value	Help Text
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	Allows user to change boot profile via BIOS menu or 3rd party appli...

#	Parameter	Target Type	Settings
1	Integrated Clock Controller - Integrated Clock Controller Policies		
	Boot Profile 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. 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". The 'Record #' refers to profile created under the "Integrated Clock Controller Profiles". Default boot profile for system is Profile 0. Double click on value column of this parameter to choose from available options.	SPI	Profile 0
		UFS	Profile 0
	Failsafe Profile 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. The 'Record #' refers to profile created under the "Integrated Clock Controller Profiles". Default Failsafe boot profile for system is Profile 0. Double click on value column of this parameter to choose from available options.	SPI	Profile 0
		UFS	Profile 0
	Profile Changeable Possible configuration: True/False. 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. Double click on value column of this parameter to choose from available options.	SPI	True
		UFS	True

Click on Integrated Clock Controller in the left tabs menu> Profiles are expanded by default:



Table 2-7. Integrated Clock Controller (Sheet 2 of 7)

▼ Profiles

Profile 0

3

+ Add Profile

▼ Profile

2

Parameter	Value	Help Text
Profile Name	Profile 0	Editable text string.
Profile Type	Standard	Specifies the profile. Intel (R) ME image has to be loaded to enable other ICC profile settings.

#	Parameter	Target Type	Settings
2	Integrated Clock Controller - Profiles - Profile 0 Note: Intel® CSE image has to be loaded to enable other ICC profile settings. For Lake Field , 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 provides Wimax/3G friendly configuration. 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. Note: User can select pre-defined profiles via "Integrated Clock Controller Profiles - Profile Type " parameter User can add up to maximum 16 profiles.To add new profile, please use "Integrated Clock Controller Profiles - + Add Profile Button"	SPI	Standard
		UFS	Standard
	Profile Name This parameter allows user to customize profile name for easy identification. By default it uses pre-defined profile name like Profile 0.	SPI	Profile 0
		UFS	Profile 0
	Profile Type Available ICC profiles for Lake Field are Standard, Adaptive. This parameter indicates which pre- defined profile selected for each profile#. Double click on value column of this parameter to choose from available options.	SPI	Standard
		UFS	Standard
3	+ 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.	SPI	
		UFS	

Click on Integrated Clock Controller in the left tabs menu> Profiles >Profile> Bclk Clock Configuration is expanded by default:



Table 2-7. Integrated Clock Controller (Sheet 3 of 7)

<div> ▼ BclkClockConfiguration <div>4</div> </div>																											
<table border="1"> <thead> <tr> <th>Parameter</th><th>Value</th><th colspan="2">Help Text</th></tr> </thead> <tbody> <tr> <td>BCLK Clock Frequency</td><td>This parameter is not configura...</td><td colspan="2">Select the nominal frequency for the selected clock. Range is limited based on the Clock ...</td></tr> <tr> <td>BCLK Spread setting</td><td>This parameter is not configura...</td><td colspan="2">Select the percentage of Spread setting for the selected clock. Range is limited based on...</td></tr> </tbody> </table>				Parameter	Value	Help Text		BCLK Clock Frequency	This parameter is not configura...	Select the nominal frequency for the selected clock. Range is limited based on the Clock ...		BCLK Spread setting	This parameter is not configura...	Select the percentage of Spread setting for the selected clock. Range is limited based on...													
Parameter	Value	Help Text																									
BCLK Clock Frequency	This parameter is not configura...	Select the nominal frequency for the selected clock. Range is limited based on the Clock ...																									
BCLK Spread setting	This parameter is not configura...	Select the percentage of Spread setting for the selected clock. Range is limited based on...																									
#	Parameter	Target Type	Settings																								
4	Integrated Clock Controller - Profiles - Profile BclkClockConfiguration																										
	BCLK Clock Frequency This parameter displays the nominal frequency for the BCLK. Range is limited based on the Clock Range Definition record and HW SKU. BCLK Clock Frequency is enforced by FW	SPI UFS																									
	BCLK Spread Setting This parameter displays the percentage of Spread setting for the BCLK. Range is limited based on the Clock Range Definition record and HW SKU. BCLK Spread Setting is enforced by FW.	SPI UFS																									
Click on Integrated Clock Controller in the left tabs menu> Profiles >Profile> Clock Range Definition Record is expanded by default:																											
<div> ▼ ClockRangeDefinitionRecord <div>5</div> </div>																											
<table border="1"> <thead> <tr> <th>Parameter</th><th>Value</th><th colspan="2">Help Text</th></tr> </thead> <tbody> <tr> <td>BCLK PLL Clock Source Maxi...</td><td>This parameter is not configura...</td><td colspan="2">Specifies the maximum frequency that can be applied to BCLK clock source. Value is limi...</td></tr> <tr> <td>BCLK PLL Clock Source Mini...</td><td>This parameter is not configura...</td><td colspan="2">Specifies the minimum frequency that can be applied to BCLK clock source.Value is limite...</td></tr> <tr> <td>BLCK SSC Changes Allowed</td><td>This parameter is not configura...</td><td colspan="2">Specifies if the spread mode and percentage is allowed to be modified at runtime.</td></tr> <tr> <td>BLCK SSC Halt Allowed</td><td>This parameter is not configura...</td><td colspan="2">if TRUE , the spread generator can be enabled and disabled at runtime.</td></tr> <tr> <td>BLCK SSC Percentage</td><td>This parameter is not configura...</td><td colspan="2">Specifies the maximum precentage of spread adjustment that can be applied to the clock....</td></tr> </tbody> </table>				Parameter	Value	Help Text		BCLK PLL Clock Source Maxi...	This parameter is not configura...	Specifies the maximum frequency that can be applied to BCLK clock source. Value is limi...		BCLK PLL Clock Source Mini...	This parameter is not configura...	Specifies the minimum frequency that can be applied to BCLK clock source.Value is limite...		BLCK SSC Changes Allowed	This parameter is not configura...	Specifies if the spread mode and percentage is allowed to be modified at runtime.		BLCK SSC Halt Allowed	This parameter is not configura...	if TRUE , the spread generator can be enabled and disabled at runtime.		BLCK SSC Percentage	This parameter is not configura...	Specifies the maximum precentage of spread adjustment that can be applied to the clock....	
Parameter	Value	Help Text																									
BCLK PLL Clock Source Maxi...	This parameter is not configura...	Specifies the maximum frequency that can be applied to BCLK clock source. Value is limi...																									
BCLK PLL Clock Source Mini...	This parameter is not configura...	Specifies the minimum frequency that can be applied to BCLK clock source.Value is limite...																									
BLCK SSC Changes Allowed	This parameter is not configura...	Specifies if the spread mode and percentage is allowed to be modified at runtime.																									
BLCK SSC Halt Allowed	This parameter is not configura...	if TRUE , the spread generator can be enabled and disabled at runtime.																									
BLCK SSC Percentage	This parameter is not configura...	Specifies the maximum precentage of spread adjustment that can be applied to the clock....																									
#	Parameter	Target Type	Settings																								
5	Integrated Clock Controller - Profiles - Profile ClockRangeDefinitionRecord																										
	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. Standard Setting Profile Type - Option is grayed out. Adaptive Setting Profile Type - Option is able to be edited.	SPI UFS																									



Table 2-7. Integrated Clock Controller (Sheet 4 of 7)

	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. Standard Setting Profile Type - Option is grayed out. Adaptive Setting Profile Type - Option is able to be edited.	SPI																									
		UFS																									
	BCLK SSC Changes Allowed This parameter allows user to specify if the spread mode and percentage is allowed to be modified at runtime or not. if set to "True" : Runtime modification is allowed. Standard Setting Profile Type - Option is grayed out. Adaptive Setting Profile Type - Option is able to be edited.	SPI																									
		UFS																									
	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. Standard Setting Profile Type - Option is grayed out. Adaptive Setting Profile Type - Option is able to be edited.	SPI																									
		UFS																									
	BCLK SSC 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%) Standard Setting Profile Type - Option is grayed out. Adaptive Setting Profile Type - Option is able to be edited.	SPI																									
		UFS																									
Click on Integrated Clock Controller in the left tabs menu> Profiles >Profile> Clock Output Configuration is expanded by default:																											
<div><div><div>▼ ClockOutputConfiguration</div><div>6</div></div><table><thead><tr><th>Parameter</th><th>Value</th><th>Help Text</th></tr></thead><tbody><tr><td>ITPXD</td><td>Enabled</td><td>Enable/Disable the CLKOUT_ITPXD differential output buffer.</td></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></tbody></table></div>				Parameter	Value	Help Text	ITPXD	Enabled	Enable/Disable the CLKOUT_ITPXD differential output buffer.	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 Text																									
ITPXD	Enabled	Enable/Disable the CLKOUT_ITPXD differential output buffer.																									
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	Target Type	Settings																								
6	Integrated Clock Controller - Profiles - Profile Clock Output Configuration																										



Table 2-7. Integrated Clock Controller (Sheet 5 of 7)

ITPXD, SRC[0:5], LPC[0:1] Values: Enabled/Disabled These parameters come under the Power Management section and they control Enabling /Disabling of specific Output Clocks at boot time. These settings should match with platform hardware design. For CRB, recommend keeping defaults for bring up with Intel® CSE FW. These parameters are specifically used to Enable/Disable the respective CLKOUT_XXX differential output buffers	SPI	Enabled
	UFS	Enabled
SRC0 Values: Enabled/Disabled Enables or Disables the CLKOUT_SRC1 differential output buffer.	SPI	Enabled
	UFS	Enabled
SRC1 Values: Enabled/Disabled Enables or Disables the CLKOUT_SRC2 differential output buffer.	SPI	Enabled
	UFS	Enabled
SRC2 Values: Enabled/Disabled Enables or Disables the CLKOUT_SRC3 differential output buffer.	SPI	Enabled
	UFS	Enabled
SRC3 Values: Enabled/Disabled Enables or Disables the CLKOUT_SRC4 differential output buffer.	SPI	Enabled
	UFS	Enabled
SRC4 Values: Enabled/Disabled Enables or Disables the CLKOUT_SRC5 differential output buffer.	SPI	Enabled
	UFS	Enabled
SRC5 Values: Enabled/Disabled Enables or Disables the CLKOUT_SRC6 differential output buffer.	SPI	Enabled
	UFS	Enabled
Click on Integrated Clock Controller in the left tabs menu> Profiles >Profile> Power Management Configuration is expanded by default:		



Table 2-7. Integrated Clock Controller (Sheet 6 of 7)

▼ Power Management Configuration 7			
Parameter		Value	
SRC0 CLKREQ# Mapping		GPP_B5	Assign the CLKREQ# signal assoc
SRC1 CLKREQ# Mapping		GPP_B6	Assign the CLKREQ# signal assoc
SRC2 CLKREQ# Mapping		GPP_B7	Assign the CLKREQ# signal assoc
SRC3 CLKREQ# Mapping		GPP_B8	Assign the CLKREQ# signal assoc
SRC4 CLKREQ# Mapping		GPP_B9	Assign the CLKREQ# signal assoc
SRC5 CLKREQ# Mapping		GPP_B10	Assign the CLKREQ# signal assoc
24Mhz Crystal Shutdown Wait Interval		8us	Enable Dynamic power managem

#	Parameter	Target Type	Settings
7	Integrated Clock Controller - Profiles - Profile Power Management Configuration Configuring CLKREQ# and assigning GPIO depends on how CLKOUT_SRCx configuration via FIT is done (Enabled or Disabled) and if CLKREQ is required or not. Please refer to Appendix B.3 (How to configure CLKREQ# parameters) for the detail of CLKREQ configuration for SRC Output clocks. Please configure CLKREQ parameters accordingly.		
	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.	SPI UFS	GPP_B5 GPP_B5
	SRC1 CLKREQ# Mapping Assign the CLKREQ# signal associated with CLKOUT_SRC1.	SPI UFS	GPP_B6 GPP_B6
	SRC2 CLKREQ# Mapping Assign the CLKREQ# signal associated with CLKOUT_SRC2.	SPI UFS	GPP_B7 GPP_B7
	SRC3 CLKREQ# Mapping Assign the CLKREQ# signal associated with CLKOUT_SRC3.	SPI UFS	GPP_B8 GPP_B8
	SRC4 CLKREQ# Mapping Assign the CLKREQ# signal associated with CLKOUT_SRC4.	SPI UFS	GPP_B9 GPP_B9
	SRC5 CLKREQ# Mapping Assign the CLKREQ# signal associated with CLKOUT_SRC5.	SPI UFS	GPP_B10 GPP_B10

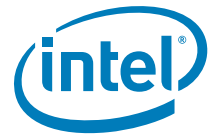


Table 2-7. Integrated Clock Controller (Sheet 7 of 7)

	24MHz Crystal Shutdown Wait Interval This parameter allows user to Enable Dynamic power management of Crystal. Upon the event that all conditions (other than this wait timer itself) are satisfied for iSCLK crystal shutdown, a timer is started. Once it expires and there are no wake events, iSCLK will shutdown crystal. Note: Recommendation is to leave setting at default value.	SPI	8us
		UFS	8us



Table 2-8. Internal PCH Buses (Sheet 1 of 3)

Click on Internal PCH Buses in the left tabs menu> PCH Timer Configuration is expanded by default:

▼ PCH Timer Configuration

1

Parameter	Value	
PCH clock output stable to PROCPWRGD high...	1ms	This setting configures the mini
PCIe Power Stable Timer (tPCH33)	Disabled	This setting configures the enab
PROCPWRGD and SYS_PWROK high to SUS_...	1ms	This setting configures the mini
APWROK Timing	2ms	This soft strap determines the t
APWROK Check Enabled	Yes	This setting determines if Intel(

#	Parameter	Target Type	Settings
1	Internal PCH Buses - 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. For further details see Lake Field LP Platform Controller Hub EDS.	SPI	100ms
		UFS	100ms
	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".	SPI	Disabled
		UFS	Disabled
	PROCPWRGD and SYS_PWROK high to SUS_STAT# de-assertion (tPCH46) Values: 1ms, 2ms, 5ms This setting configures the minimum timing from CPUPWRGD assertion to SUS_STAT#. For further details see Lake Field LP Platform Controller Hub EDS.	SPI	1ms
		UFS	1ms
	APWROK Timing Values: 2ms, 4ms, 8ms, 16ms This soft strap determines the time between the SLP_A# pin de-asserting and the APWROK timer expiration. For further details see Lake Field LP Platform Controller Hub EDS.	SPI	2ms
		UFS	2ms
	APWROK Check Enabled Values: Yes/No This setting determines if Intel® CSE should de-assert SLP_A# and wait for APWROK or not.	SPI	Yes
		UFS	Yes

Click on Internal PCH Buses in the left tabs menu> OPI Configuration is expanded by default:



Table 2-8. Internal PCH Buses (Sheet 2 of 3)

▼ OPI / DMI Configuration 2			
Parameter	Value	Help 1	
OPI / DMI Link Speed	4 GT/s	This setting configures the OPI Link Speed. For furt	
OPI / DMI Link Voltage	0.95 Volts	This setting configures the OPI Link Voltage. For fur	
OPI / DMI Link Width	4 Lanes	This setting configures the OPI Link Width. For furtl	
#	Parameter	Target Type	Settings
2	Internal PCH Buses - OPI / DMI Configuration		
	OPI Link Speed Values: GT2/GT4 This setting configures the OPI / DMI Link Speed. For further details see Lake Field PCH EDS.	SPI	2 GT/s
		UFS	2 GT/s
	OPI Link Voltage Values: 0.85 Volts, 0.95 Volts This setting configures the OPI / DMI Link Voltage. For further details see Lake Field PCH EDS.	SPI	0.85 Volts
		UFS	0.85 Volts
	OPI Link Width Values: 1 Lanes, 2 Lanes, 3 Lanes, 4 Lanes This setting configures the OPI / DMI Link Width. For further details see Lake Field PCH EDS.	SPI	4 Lanes
		UFS	4 Lanes
Click on Internal PCH Buses in the left tabs menu> eSPI Configuration is expanded by default:			
▼ eSPI Configuration 3			
Parameter	Value		
eSPI / EC Slave 1 Device Maximum I/O Mode	Single , Dual and Quad	This setting configures the maxi	
eSPI / EC Slave 1 Device Bus Frequency	60MHz	This setting configures the maxi	
#	Parameter	Target Type	Settings
3	Internal PCH Buses - eSPI Configuration		
	eSPI / EC Slave 1 Device Maximum I/O Mode <i>Note: Leave settings at Intel® FIT default values</i>		
	eSPI / EC Slave 1 Device Bus Frequency <i>Note: Leave settings at Intel® FIT default values</i>		
Click on Internal PCH Buses in the left tabs menu> I2C Configuration is expanded by default:			



Table 2-8. Internal PCH Buses (Sheet 3 of 3)

<div><div>▼ I2C Configuration</div><div>4</div></div>			
Parameter		Value	
I2C Communication Speed		High Speed	This setting determines the co
#	Parameter	Target Type	Settings
4	Internal PCH Buses - I2C Configuration		
	I2C Communication Speed	SPI	High Speed
	Values: Standard, Fast, High Speed	UFS	High Speed



Table 2-9. Power

Click on Power in the left tabs menu> Platform Power is expanded by default:			
▼ Platform Power 1			
Parameter		Value	
SLP_S0# Tunnel		Enabled	This setting Enables / Disables the tur
#	Parameter	Target Type	Settings
1	Power - Platform Power		
	SLP_S0# Tunnel <i>Note: Leave settings at Intel® FIT default values</i>		
Click on Power in the left tabs menu> PCH Thermal Reporting is expanded by default:			
▼ PCH Thermal Reporting 3			
Parameter		Value	
Thermal Power Reporting Enabled		Yes	This setting enabled a or
#	Parameter	Target Type	Settings
3	Power - PCH Thermal Reporting		
	Thermal Power Reporting Enabled	SPI	Yes
	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.	UFS	Yes



Table 2-10. Integrated Sensor Hub (Sheet 1 of 2)

Click on Integrated Sensor Hub in the left tabs menu> Integrated Sensor Hub is expanded by default:			
<div> <div>▼ Integrated Sensor Hub</div> <div>1</div> </div>			
Parameter	Value	Help Text	
Integrated Sensor Hub Supported	Yes	This setting allows customers to enable /	
Integrated Sensor Hub Initial Power State	Disabled	This setting allows customers to determin	
#	Parameter	Target Type	Settings
1	Integrated Sensor Hub - Integrated Sensor Hub		
	Integrated Sensor Hub Supported Values: Yes/No This setting allows customers to disable ISH on the platform.	SPI	Yes
		UFS	Yes
	Integrated Sensor Hub Power Up State Values: Enabled/Disabled Field is enabled for editing if "Integrated Sensor Hub Supported" field above is set to "Yes". This setting allows customers to determine the power up state for ISH.	SPI	Disabled
		UFS	Disabled
Click on Integrated Sensor Hub in the left tabs menu> ISH Image is expanded by default:			
<div> <div>▼ ISH Image</div> <div>2</div> </div>			
Parameter	Value	Help Text	
Length	0x40000	Total size (in bytes) of the ISH code partition including reserved space. It is recommended to be at leas...	
InputFile		Path to your ISH firmware binary file.	
#	Parameter	Target Type	Settings
2	Integrated Sensor Hub - ISH Image		
	Length - Total size (in bytes) of the ISH code partition including reserved space. It is recommended to be at least 256kb.		
	Input File	SPI	ISH Binary (Optional)
		UFS	ISH Binary (Optional)
Click on Integrated Sensor Hub in the left tabs menu> ISH Data is expanded by default:			

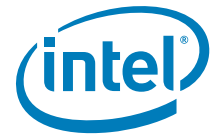


Table 2-10. Integrated Sensor Hub (Sheet 2 of 2)

<div> <div>▼ ISH Data</div> <div>3</div> </div>			
Parameter	Value	Help Text	
PDT Binary File		Path to your PDT binary file	

#	Parameter	Target Type	Settings
3	Integrated Sensor Hub - ISH Data		
	PDT Binary File	SPI	Path for PDT Binary file
		UFS	Path for PDT Binary file



Table 2-11. Camera

Click on Camera in the left tabs menu> IPU Security is expanded by default:			
▼ IPU Security 1			
Parameter		Value	
Secure Touch		Disabled	When set, CAMERA_MASK register bits p
FW Secure Mode		Enabled	If enabled, access blockers in IS and PS
Secure Touch Camera Mask		0xFF	Camera mask bits per CSI port. When SI
#	Parameter	Target Type	Settings
1	Camera - IPU Security		
	Secure Touch	SPI	Disabled
	When set, CAMERA_MASK register bits per CSI port are used to mask the data of cameras. When cleared, camera data is not masked.	UFS	Disabled
	FW Secure Mode	SPI	Enabled
	If enabled, access blockers in IS and PS are enabled, and FW is read from IMR. Must be enabled for FW authentication flow and execution of authenticated FW.	UFS	Enabled
	Secure Touch Camera Mask	SPI	0xFF
	Camera mask bits per CSI port. When SECURE_TOUCH is set each set bit masks a CSI port for secure touch. When SECURE_TOUCH is cleared this register has no impact on the CSI ports.	UFS	0xFF
Click on Camera in the left tabs menu> IPU Debug is expanded by default:			
▼ IPU Debug 2			
Parameter		Value	
IPU Debugging Enabled		No	If enabled, IPU Debugging is enabled, otherwise
#	Parameter	Target Type	Settings
2	Camera - IPU Debug		
	IPU Debugging Enabled	SPI	No
	If enabled, IPU Debugging is enabled, otherwise internal setup is checked to see if the IPU Debugging feature should be enabled or not.	UFS	No



Table 2-12. Debug (Sheet 1 of 5)

Click on Debug in the left tabs menu> Intel® ME Firmware Debugging Overrides is expanded by default:			
▼ IDLM 1			
Parameter		Value	
IDLM Binary		This allows an IDLM binary to be merged in	
#	Parameter	Target Type	Settings
1	Debug - IDLM		
	IDLM Binary	SPI	
	This allows an IDLM binary to be merged into output image built by Intel® FIT.	UFS	
Click on Debug in the left tabs menu> Delayed Authentication Mode Configuration is expanded by default:			
▼ Delayed Authentication Mode Configuration 2			
Parameter		Value	
Delayed Authentication Mode Enabled		No	
		This setting enables Delayed Authentic	
#	Parameter	Target Type	Settings
2	Debug - Delayed Authentication Mode Configuration		
	Delayed Authentication Mode Enabled	SPI	No
	Value: Yes / No	UFS	No
	This setting enables Delayed Authentication Mode on the platform.		
Click on Debug in the left tabs menu> Intel® Trace Hub Technology is expanded by default:			
▼ Intel(R) Trace Hub Technology 3			
Parameter		Value	
Intel(R) Trace Hub Binary		This loads the Intel(R) Trace	
Intel(R) Trace Hub Debug Messages Enabled		No	Intel(R) Trace Hub Debug Me
Unlock Token		This allows the OEM to input	
Intel(R) Trace Hub Soft Enable		No	When set to Yes, enables Int
Intel(R) Trace Hub Emergency Mode Enabled		No	When enabled, Intel(R) ME p
#	Parameter	Target Type	Settings
3	Debug - Intel® Trace Hub Technology		



Table 2-12. Debug (Sheet 2 of 5)

	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.	SPI	Trace Hub Binary
		UFS	Trace Hub Binary
	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.	SPI	No
		UFS	No
	Unlock Token This allows the OEM to input an Unlock Token binary file for closed chassis debug.	SPI	
		UFS	
	Intel® Trace Hub Soft Enable Values: Yes/No This setting enable / disables Intel® Trace Hub in the firmware base image.	SPI	No
		UFS	No
	Intel® Trace Hub Emergency Mode Enabled Values: Yes/No This setting enable / disables Intel® Trace Hub in the firmware base image.	SPI	No
		UFS	No

Click on Debug in the left tabs menu> Intel® ME Debugging Overrides is expanded by default:

▼ Intel(R) ME Firmware Debugging Overrides

4

Parameter	Value	
Debug Override Pre-Production Silicon	0x0	Allows the OEM t
Debug Override Production Silicon	0x0	Allows the OEM t
Intel(R) ME Reset Behavior	Intel(R) ME will Halt	This setting deter
Enable Intel(R) ME Reset Capture on CLR_RST#	No	This setting confi
Firmware ROM Bypass	No	This setting enab
AFS Idle Flash Reclaim Enabled	Yes	This controls ena

#	Parameter	Target Type	Settings
4	Debug - Intel® ME Firmware Debugging Overrides		



Table 2-12. Debug (Sheet 3 of 5)

	Debug Override Pre-Production Silicon Allows the OEM to control FW features to assist with pre-production platform debugging. This control has no effect if used on production silicon. Bit 0: Disable DRAM_INIT_DONE (default timeout 60 seconds) Bit 1: Disable Host Reset Timer Bit 2: Disable CPU_RESET_DONE timeout Bit 3: Reserved Bit 4: Disable Intel® CSE Power Gating Bit 5: Reserved Bit 6: Secure Boot debug hook. Used to shorten wait time before ENF shutdown. Bit 7: Force real FPFs on preproduction (default is to use flash) Bit 8: Secure Boot debug hook. Used to reduce S3 or FFS optimization tries. Bit 9: Reserved Bit 10: Override power package to always enter M3. Note: Certain options do not work when the descriptor is locked.	SPI	0x00000000
		UFS	0x00000000
	Debug Override Production Silicon Allows the OEM to control FW features to assist with production platform debugging. Bit 0: Extend DRAM_INIT_DONE timeout to 30 minutes (default timeout 15 seconds) Bit 1: Disable Host Reset Timer Bit 2: Disable CPU_RESET_DONE timeout Note: Certain options do not work when the descriptor is locked.	SPI	0x00000000
		UFS	0x00000000
	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.	SPI	Intel® ME Alternate image boot
		UFS	Intel® ME Alternate image boot
	Enable Intel® ME Reset Capture on CLR_RST# Note: Leave settings at Intel® FIT default values		
	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.	SPI	No
		UFS	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.	SPI	Yes
		UFS	Yes
Click on Debug in the left tabs menu> Direct Connection Interface Configuration is expanded by default:			



Table 2-12. Debug (Sheet 4 of 5)

▼ Direct Connect Interface Configuration

5

Parameter	Value	Help
Direct Connect Interface (DCI) Enabled	No	This setting enables / disables the DCI interface.
DCI BSSB over USB3 Port1 Enabled	Yes	This setting determines if the USB port be
DCI BSSB over GPIO Enabled	Yes	This setting enables BSSB (Boundary Scan

#	Parameter	Target Type	Settings
5	Debug - Direct Connection Interface Configuration		
	Direct Connect Interface (DCI) Enabled Values: Yes/No This setting enables / disables the DCI interface used for Intel® Trace Hub debugging.	SPI	No
		UFS	No
	DCI BSSB over USB3 Port 1 Enabled Values: Yes/No This setting determines if the USB port 1 has BSSB (Boundary Scan Side Band) enabled. <i>Note:</i> For S0ix and reset flows BSSB should be enabled.	SPI	Yes
		UFS	Yes
	DCI BSSB over GPIO Enabled Values: Yes/No This setting enables BSSB (Boundary Scan Side Band) over GPIO for DCI operations. <i>Note:</i> If this setting is enabled the DCI BSSB over USB3 Port1 Enabled also needs to be set to 'Yes'. <i>Note:</i> For S0ix and reset flows BSSB should be enabled.	SPI	Yes
		UFS	Yes

Click on Debug in the left tabs menu> Early USB DBC Type-A Configuration is expanded by default:

▼ Early USB DBC over Type-A Configuration

6

Parameter	Value	Help
Intel(R) ME Boot Stall Enabled	No Boot Stall	This setting enables a delay c
USB2 DbC port enable	No USB2 Ports	This setting determines which
USB Connector's Associated USB3 Port enable	No USB3 Ports	This setting determines which

#	Parameter	Target Type	Settings
---	-----------	-------------	----------



Table 2-12. Debug (Sheet 5 of 5)

6	Debug - Early USB DBC Type-A Configuration		
	Intel® ME Boot Stall Enabled Values: No Boot Stall/Boot Stall This setting enables a delay during Intel® CSE FW bring-up to allow USB DCI to be established and Early DbC arbitration to be granted.	SPI	No Boot Stall
		UFS	No Boot Stall
	USB2 DbC port enable Values: No USB2 Ports, USB2 Port1, USB2 Port2 This setting determines which USB2 ports are enabled for Early DbC debugging.	SPI	No USB2 Ports
		UFS	No USB2 Ports
	USB Connectors associated USB3 Port enable Values: No USB3 Ports, USB3 Port1, USB3 Port2 This setting determines which USB3 ports goes to the target USB2 ports connector for Early DbC debugging.	SPI	No USB3 Ports
		UFS	No USB3 Ports

Click on Debug in the left tabs menu> eSPI Feature Overrides is expanded by default:

▼ eSPI Feature Overrides

6

Parameter	Value	
eSPI / EC Low Frequency Debug Override	No	When enabled this setting will divide

#	Parameter	Target Type	Settings
	Debug - eSPI Feature Overrides		
	eSPI / EC Low Frequency Debug Override		
	Note: Leave settings at Intel® FIT default values		



Table 2-13. CPU Straps (Sheet 1 of 2)

Click on CPU Straps in the left tabs menu> CPU Straps are expanded by default:			
<div> <div>▼ CPU Straps</div> <div>1</div> </div>			
Parameter	Value	Help	
Disable Hyperthreading	No	This setting control enabling / disabling of Hyperthreading.	
BIST Initialization	No	This setting determines if BIST will be run at platform reset after BIOS requested actions.	
Flex Ratio	0x0	This setting controls the maximum processor frequency.	
Processor Boot Max Frequency	Yes	This setting determines if the processor will operate at the maximum frequency.	
JTAG Power Disable	No JTAG Power on C10 and Lo...	This setting determines if JTAG power will be requested during boot.	
Platform IMON Disable	0x0	This strap should be left at the recommended value.	
VCC Aux Present	No	This setting determines if VCC Aux exists as a separate rail.	
VCC SFR OC PG Present	No	This setting determines if VCC SFR OC PG is present.	
VCC ST PG Present	No	This setting determines if VCC ST PG is present.	
VCC STG PG Present	No	This setting determines if VCC STG PG is present.	
VDDQ TX Rail Supply	VDDQ	This setting determines if the VDDQ TX Rail supply is used.	
Big Core CPU Disable	Big Core Enabled	This setting controls the number of active Big Cores.	
Small Core CPU Disable	All Cores Active	This setting controls the number of active Small Cores.	
#	Parameter	Target Type	Settings
1	CPU Straps - CPU Straps		
	Disable Hyperthreading Values: Yes/No This setting controls enabling or disabling of Hyper threading. Note: This strap is intended for debugging purposes only. See BIOS Spec for more details on enabling / disabling Hyperthreading.	SPI	No
		UFS	No
	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.	SPI	No
		UFS	No



Table 2-13. CPU Straps (Sheet 2 of 2)

	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.	SPI	0x0
		UFS	0x0
	Processor Boot Max 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.	SPI	Yes
		UFS	Yes
	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.	SPI	No JTAG Power on C10 and Lower
		UFS	No JTAG Power on C10 and Lower
	Platform IMON Disable This strap should be left at the recommended default setting.	SPI	0x0
		UFS	0x0
	VCC Aux Present Values: Yes/No This setting determines if VCC Aux exists as a separate VR. See Processor EDS for details.	SPI	No
		UFS	No
	VCC SFR OC PG Present Values: Yes/No This setting determines if VCC SFR OC PG is present on the platform.	SPI	No
		UFS	No
	VCC ST PG Present Values: Yes/No This setting determines if VCC ST PG is present on the platform.	SPI	No
		UFS	No
	VCC STG PG Present Values: Yes/No This setting determines if VCC STG PG is present on the platform.	SPI	No
		UFS	No
	VDDQ TX Rail Supply Values: VDDQ/LP4x This setting determines if the VDDQ TX Rail is ties to VDDQ or LP4x.	SPI	VDDQ
		UFS	VDDQ
	Big Core CPU Disable Values: Big Core Enabled/Big Core Disabled This setting determines if controls the number of active Big Core CPUs on the platform. Note: There is only 1 Big Core CPU present on Lake Field.	SPI	Big Core Enabled
		UFS	Big Core Enabled
	Small Core CPU Disable Values: All Cores Active, 1 Core Disabled, 2 Cores Disabled, 3 Cores Disabled This setting determines if controls the number of active Small Core CPUs on the platform. Note: This setting does not allow all 4 of the Small Core CPUs to be disabled. One Small Core CPU is required for platform boot.	SPI	All Cores Enabled
		UFS	All Cores Enabled



Table 2-14. Flex I/O Straps (Sheet 1 of 5)

Click on Flex I/O in the left tabs menu> PCIe Lane Reversal Configuration is expanded by default:

▼ PCIe Lane Reversal Configuration1

Parameter	Value	
PCIe Controller 1 Lane Reversal...	No	This setting allows the PCIe lanes on C
PCIe Controller 2 Lane Reversal...	No	This setting allows the PCIe lanes on C

#	Parameter	Target Type	Settings
1	Flex I/O - PCIe Lane Reversal Configuration		
	PCIe Controller 1 Lane Reversal Enabled Values: Yes/ No This setting allows the PCIe lanes on Controller 1 to be reversed. <i>Note:</i> Refer to EDS for PCIe supported port configurations.	SPI UFS	No No
	PCIe Controller 2 Lane Reversal Enabled Values: Yes/ No This setting allows the PCIe lanes on Controller 2 to be reversed. <i>Note:</i> Refer to EDS for PCIe supported port configurations.	SPI UFS	No No

Click on Flex I/O in the left tabs menu> PCIe Port Configuration is expanded by default:

▼ PCIe Port Configuration2

Parameter	Value	
PCIe Controller 1 (Port 1-4)	4x1	This setting controls PCIe Port con
PCIe Controller 2 (Port 5-8)	1x4	This setting controls PCIe Port con

#	Parameter	Target Type	Settings
2	Flex I/O - PCIe Port Configuration		
	PCIe Controller 1 (Port 1-4) Values: 4x1, (1x2, 2x1), 2x2, 1x4 This setting controls PCIe Port configurations for PCIe Controller 1. For further details see Lake Field Platform Controller Hub EDS.	SPI UFS	2x2 2x2
	PCIe Controller 2 (Port 5-8) Values: 4x1, (1x2, 2x1), 2x2, 1x4 This setting controls PCIe Port configurations for PCIe Controller 2. For further details see Lake Field P Platform Controller Hub EDS.	SPI UFS	1x2, 2x1 1x2, 2x1

Click on Flex I/O in the left tabs menu> USB3 Port Configuration is expanded by default:



Table 2-14. Flex I/O Straps (Sheet 2 of 5)

▼ USB3 Port Configuration 3			
Parameter		Value	
USB3 Port 1 Connector Type Select		Type C	This setting configures th
USB3 Port 2 Connector Type Select		Type C	This setting configures th
USB3 Port 1 Initialization Speed Select		USB3.1 Gen1 LBPM	This setting determines L
USB3 Port 2 Initialization Speed Select		USB3.1 Gen1 LBPM	This setting determines L
USB3 Port 1 Speed Capability		USB 3.1 Gen2	This setting determines tl
USB3 Port 2 Speed Capability		USB 3.1 Gen2	This setting determines tl
USB Type AB Mode Select		USB Type AB SW Select	This setting determines h

#	Parameter	Target Type	Settings
3	Flex I/O - USB3 Port Configuration <i>Note:</i> USB Type-C Mux Control: On Lake Field PCH, device mode is supported on all USB3.1 Type-C ports. EC/PD/PC needs to send a OOB command to the PCH to properly map the USB 2.0 and USB 3.1 signals to the Host controller or Device mode controller when a connection is detected on the Type-C port. Without these OOB message, the USB2.0/3.1 signals may not be correctly mapped and the USB functionality may be impacted. For more detail, see USB Type-C Mux Control Over eSPI doc # 570737.		
	USB3 Port 1 Connector Type Select Values: Type-C, Type-A, Express Card M.2 S2 This setting configures the physical connector type to be used for USB 3.0 / 3.1 Port 1.	SPI UFS	Type-C Type-C
	USB3 Port 2 Connector Type Select Values: Type-C, Type-A, Express Card M.2 S2 This setting configures the physical connector type to be used for USB 3.0 / 3.1 Port 2.	SPI UFS	Type-C Type-C
	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.	SPI UFS	USB3.1 Gen1 LBPM 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.	SPI UFS	USB3.1 Gen1 LBPM 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.	SPI UFS	USB 3.1 Gen2 USB 3.1 Gen2



Table 2-14. Flex I/O Straps (Sheet 3 of 5)

	USB3 Port 2 Speed Capability Values: USB 3.1 Gen1/USB 3.1 Gen2 This setting determines the USB3 Port 2 speed capabilities.	SPI	USB 3.1 Gen2																								
		UFS	USB 3.1 Gen2																								
	USB Type AB Mode Select Values: USB Type AB SW Select/USB Type AB HW Select This setting determines how the USB Type AB connector switching is handled.	SPI	USB Type AB SW Select																								
		UFS	USB Type AB SW Select																								
Click on Flex I/O in the left tabs menu> USB2 Port Configuration is expanded by default:																											
▼ USB2 Port Configuration 4																											
<table><tr><th>Parameter</th><th>Value</th><th></th></tr><tr><td>USB2 Port 1 Connector Type Select</td><td>Type C</td><td>This setting configures the physical co</td></tr><tr><td>USB2 Port 2 Connector Type Select</td><td>Type C</td><td>This setting configures the physical co</td></tr></table>				Parameter	Value		USB2 Port 1 Connector Type Select	Type C	This setting configures the physical co	USB2 Port 2 Connector Type Select	Type C	This setting configures the physical co															
Parameter	Value																										
USB2 Port 1 Connector Type Select	Type C	This setting configures the physical co																									
USB2 Port 2 Connector Type Select	Type C	This setting configures the physical co																									
#	Parameter	Target Type	Settings																								
4	Flex I/O - USB2 Port Configuration																										
	USB2 Port 1 Connector Type Values: Type-C, Type-A, Express Card M.2 S2 This setting configures the physical connector type to be used for USB2 Port 1.	SPI	Type-C																								
		UFS	Type-C																								
	USB2 Port 2 Connector Type Values: Type-C, Type-A, Express Card M.2 S2 This setting configures the physical connector type to be used for USB2 Port 2.	SPI	Type-C																								
		UFS	Type-C																								
Click on Flex I/O in the left tabs menu> Type-C Subsystem Configuration is expanded by default:																											
▼ PHY Configuration 5																											
<table><tr><th>Parameter</th><th>Value</th><th></th></tr><tr><td>PHY Binary Configuration File</td><td></td><td>This loads the PHY binary that will be merged into t</td></tr><tr><td>PHY Length</td><td>0xC000</td><td>Set the length of PHY sub partition.</td></tr><tr><td>PHY version</td><td></td><td>PHY version expected MM.xxx.yyy.ZZZZ</td></tr><tr><td>Type-C OEM Config Data Instance 0 Binary</td><td></td><td>This loads OEM config data provided by the user.</td></tr><tr><td>Type-C OEM Config Data Instance 1 Binary</td><td></td><td>This loads OEM config data provided by the user.</td></tr><tr><td>Multi-Phy OEM Config Data Instance 0 Binary</td><td></td><td>This loads OEM config data provided by the user.</td></tr><tr><td>Multi-Phy OEM Config Data Instance 1 Binary</td><td></td><td>This loads OEM config data provided by the user.</td></tr></table>				Parameter	Value		PHY Binary Configuration File		This loads the PHY binary that will be merged into t	PHY Length	0xC000	Set the length of PHY sub partition.	PHY version		PHY version expected MM.xxx.yyy.ZZZZ	Type-C OEM Config Data Instance 0 Binary		This loads OEM config data provided by the user.	Type-C OEM Config Data Instance 1 Binary		This loads OEM config data provided by the user.	Multi-Phy OEM Config Data Instance 0 Binary		This loads OEM config data provided by the user.	Multi-Phy OEM Config Data Instance 1 Binary		This loads OEM config data provided by the user.
Parameter	Value																										
PHY Binary Configuration File		This loads the PHY binary that will be merged into t																									
PHY Length	0xC000	Set the length of PHY sub partition.																									
PHY version		PHY version expected MM.xxx.yyy.ZZZZ																									
Type-C OEM Config Data Instance 0 Binary		This loads OEM config data provided by the user.																									
Type-C OEM Config Data Instance 1 Binary		This loads OEM config data provided by the user.																									
Multi-Phy OEM Config Data Instance 0 Binary		This loads OEM config data provided by the user.																									
Multi-Phy OEM Config Data Instance 1 Binary		This loads OEM config data provided by the user.																									
#	Parameter	Target Type	Settings																								



Table 2-14. Flex I/O Straps (Sheet 4 of 5)

5	Type-C Subsystem Configuration		
	PHY Binary	SPI	Dekel PHY Binary
	This loads the Type-C Subsystem PHY binary that will be merged into the output image generated by the Intel® FIT.	UFS	Dekel PHY Binary
	PHY Length		
	PHY Version		
	OEM Type-C DRAM image instance 0 - Config Data	SPI	OEM Instance 0 Config Data
		UFS	OEM Instance 0 Config Data
	OEM Type-C DRAM image instance 0 - Config Data	SPI	OEM Instance 1 Config Data
		UFS	OEM Instance 1 Config Data
	Multi-phy (Non-Type-C) DRAM image instance 0 - Config Data	SPI	Multi-phy Instance 0 Config Data
		UFS	Multi-phy Instance 0 Config Data
	Multi-phy (Non-Type-C) DRAM image instance 1 - Config Data	SPI	Multi-phy Instance 1 Config Data
		UFS	Multi-phy Instance 1 Config Data

Click on Flex I/O in the left tabs menu> PCIe PLL Reference Clock Source is expanded by default:

▼ PCIe PLL Reference Clock Source6

Parameter	Value	
PCIe PLL Reference Clock Select	PCIe PLL Gen2	This setting determines the reference clock

#	Parameter	Target Type	Settings
6	PCIe PLL Reference Clock Select		
	PCIe PLL Reference Clock Select Values: PCIe PLL Gen2/PCIe PLL Gen4	SPI	PCIe PLL Gen2
		UFS	PCIe PLL Gen2
This setting determines the reference clock source for on board PCIe devices.			

Click on Flex I/O in the left tabs menu> XHCI Port Configuration is expanded by default:



Table 2-14. Flex I/O Straps (Sheet 5 of 5)



Table 2-15. GPIO (Sheet 1 of 2)

Click on GPIO in the left tabs menu> ME Feature Pins is expanded by default:

▼ ME Feature Pins4

Parameter	Value	
Intel(R) Precise Touch and Stylus Reset GPIO Select	None	Configure Intel(R) Precise Touch and Stylus Reset GPIO.
Intel(R) Precise Touch and Stylus Interrupt GPIO Select	None	Configure Intel(R) Precise Touch and Stylus Interrupt GPIO.

#	Parameter	Target Type	Settings
4	GPIO - ME Feature Pins		
	Intel® Precise Touch and Stylus Reset GPIO Select	SPI	None
	Configure Intel® Precise Touch and Stylus Reset GPIO.	UFS	None
	Intel® Precise Touch and Stylus Interrupt GPIO Select	SPI	None
	Configure Intel® Precise Touch and Stylus Interrupt GPIO.	UFS	None

Click on GPIO in the left tabs menu> Touch Controller Pins is expanded by default:

▼ Touch Controller Pins5

Parameter	Value	Help
GPP_D_0	GPIO	-
GPP_D_1	GPIO	-
GPP_D_2	GPIO	-
GPP_D_3	GPIO	-
GPP_D_21	GPIO	-
GPP_D_22	GPIO	-

#	Parameter	Target Type	Settings
5	GPIO - Touch Controller Pins		
	GPP_E_0	SPI	GPIO
		UFS	GPIO
	GPP_E_2	SPI	GPIO
		UFS	GPIO
	GPP_E_10	SPI	GPIO
		UFS	GPIO
	GPP_E_11	SPI	GPIO
		UFS	GPIO
	GPP_E_12	SPI	GPIO
		UFS	GPIO



Table 2-15. GPIO (Sheet 2 of 2)

	GPP_E_13	SPI	GPIO
		UFS	GPIO

Table 2-16. Intel® Precise Touch and Stylus

Click on Intel® Precise Touch and Stylus in the left tabs menu> IntegratedTouchConfiguration is expanded by default:			
▼ IntegratedTouchConfiguration 1			
Parameter		Value	
Intel(R) Precise Touch and Stylus Enabled		No	-
#	Parameter	Target Type	Settings
1	Intel® Precise Touch and Stylus - IntegratedTouchConfiguration		
	Intel® Precise Touch and Stylus Enabled	SPI	No
		UFS	No
Click on Intel® Precise Touch and Stylus in the left tabs menu> IntegratedTouchAndStylusConfiguration is expanded by default:			
▼ IntelPreciseTouchAndStylusConfiguration 2			
Parameter		Value	
Intel(R) Precise Touch and Stylus Controller 1 Maximum Frequency		30 MHz	This setting allows custom
2	Intel® Precise Touch and Stylus - IntelPerciseTouchandStylusConfiguration		
	Intel® Precise Touch and Stylus Controller 1 Maximum Frequency	SPI	30MHz
		UFS	30MHz



Table 2-17. Download and Execute (Sheet 1 of 2)

Click on Download and Execute in the left tabs menu> DnX Configuration is expanded by default:			
<div> <div>▼ DnX Configuration</div> <div>1</div> </div>			
Parameter	Value		
DnX Enabled	Yes	DnX permanent enable/disable F	
Platform ID	0	Platform ID that DnX uses to ver	
OEM ID	0	OEM ID that DnX uses to verify tl	
LED Enabled	Yes	DnX LED Permanently Enabled/D	
BuildEnabled	No	Should Intel FIT build a DnX ima	
OutputFileName	dnx.bin	-	
SigningKey		The path to the private key to us	
#	Parameter	Target Type	Settings
1	Download and Execute - Dnx Configuration		
	DnX Enabled Value: Yes/No DnX permanent enable / disable FPF	SPI	Yes
		UFS	Yes
	Platform ID Platform ID that DnX uses to verify the image is suitable for the platform. Before FPFs lock, this field is ignored and DnX will accept any image. After FPFs have been locked, only images with this Platform ID will be accepted by DnX.	SPI	0
		UFS	0
	OEM ID OEM ID that DnX uses to verify the image is suitable for the platform. Before FPFs lock, this field is ignored and DnX will accept any image. After FPFs have been locked, only images with this Platform ID will be accepted by DnX.	SPI	0
		UFS	0
	LED Enabled Value: Yes/No DnX LED Permanently Enabled/Disabled FPF	SPI	Yes
		UFS	Yes
	BuildEnabled Value: Yes/No Should Intel® FIT tool build a DnX image	SPI	No
		UFS	No
	OutputFileName	SPI	dnx.bin
		UFS	dnx.bin



Table 2-17. Download and Execute (Sheet 2 of 2)

	SigningKey	SPI	
	The path to the private key to use to sign the DnX image. This setting is only configurable when the OEM signing is enabled (See PlatformIntegrityOEMPublicKeyHash).	UFS	
Click on Download and Execute in the left tabs menu> USB Descriptor is expanded by default:			
▼ USB Descriptor 2			
Parameter		Value	Help T
USB String Descriptor 1		Used by ROM to communicate manufacturer string	
USB String Descriptor 2		Used by ROM to communicate manufacturer string	
	Download and Execute - USB Descriptor		
2			
	USB String Descriptor 1	SPI	
		UFS	
Used by ROM to communicate manufacturer string (32 characters) to recovery host. If this descriptor is not defined by OEM, identified by all 0's, ROM will use default descriptors.			
	USB String Descriptor 2	SPI	
		UFS	
Used by ROM to communicate manufacturer string (32 characters) to recovery host. If this descriptor is not defined by OEM, identified by all 0's, ROM will use default descriptors.			



Table 2-18. FW Update Image Build

Click on FW Update Image Build in the left tabs menu> ME Image is expanded by default:

ME Image

1

Parameter	Value	Help
ME Binary File		This loads the Embedded Controller binary th

#	Parameter	Target Type	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	SPI	ME Binary
	This loads the Intel® CSE binary that will be merged to create a firmware update image through the Intel® FIT tool.	UFS	ME Binary

Click on FW Update Image Build in the left tabs menu> PMC Image is expanded by default:

PMC Image

2

Parameter	Value	Help
PMC Max Length	0x20000	-
PMC Binary File		This loads the PMC binary that will be merged

#	Parameter	Target Type	Settings
2	PMC Image	SPI	PMC Binary
	This loads the PMC binary that will be merged to create a firmware update image through the Intel® FIT tool.	UFS	PMC Binary

Click on FW Update Image Build in the left tabs menu> OEM KM Image is expanded by default:

OEM KM Image

3

Parameter	Value	Help
OEM KM Enable	Enabled	This setting Enables / Disables OEM KM in the
OEM KM Max Length	0x1000	-
OEM Key Manifest Binary File		This loads the OEM Key manifest binary merg

#	Parameter	Target Type	Settings
3	OEM KM Enable Value: Enabled / Disabled	SPI	Enabled
	This setting enables OEM Key Manifest in the firmware updated binary.	UFS	Enabled
	OEM KM Image	SPI	OEM KM Binary
	This loads the OEM Key Manifest binary that will be merged to create a firmware update image through the Intel® FIT tool.	UFS	OEM KM Binary

Click on FW Update Image Build in the left tabs menu> Dekel PHY Image is expanded by default:



Table 2-18. FW Update Image Build



Table 2-20. Intel® FIT - Build Image

#	Parameter	CRB	Values
1	Green Build button		Can also select CTRL+B, or Build> Build Image from the menu bar along the top of the screen
2	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 device. These files are assumed to be named **outimage(1).bin** and **outimage(2).bin**.

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

3.1.1 In-Circuit SPI Flash Programming for CRB

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

1. Leave CRB powered on.
2. Connect Flash Programmer (such as DediProg SF600) header to connector **J3F3** which is labelled "**SPI TPM**". Make sure to line up pin 1 on the header.
3. Program the first image [outimage(1).bin] to the CRB.
4. In Dediprog software, select application memory chip 2 button and load second image if created.
5. Program the second image [outimage(2).bin] to the CRB if created.
6. Once programming is complete, disconnect the Flash Programmer header. Power off and unplug CRB. Remove cell coin battery, wait approximately 10 seconds. Replace cell coin battery, plug CRB back in and power on.

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 DOS or Windows* OS.

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



Intel® FPT DOS Version

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

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

```
fpt.exe -i
```

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

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

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

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

```
fpt.exe -f outimage.bin
```

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

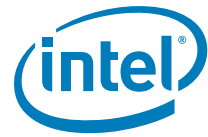
```
FPT Operation Passed
```

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

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

3.2.1 Intel® FPT Windows* Version

The Windows* OS versions supported by Intel® FPT are: Windows* PE 64, Windows* 7, Windows* 8/8.1. There are two versions of Intel® FPT for Windows*: a 32-bit version and a 64-bit version. Most Windows* OS, Windows* 7 (32-bit or 64-bit), Windows* 8/8.1 (32-bit or 64-bit) can use Windows* version of Intel® FPT. However, Windows* OS which do not support 32 bit compatible mode (Win PE 64-bit) **must use** Intel® FPT Windows* 64-bit version due to compatibility issues.



Use the following steps to program the SPI Flash devices,

1. Navigate to your **Output Directory** (as specified in [Table 2-2](#)) where your generated SPI Flash image(s) are saved. It is assumed that this image file is named **outimage.bin**. Copy this image file to 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 ---  
W25Q64BV ID:0xEF4017 Size: 8192KB (65536Kb)  
W25Q64BV ID:0xEF4017 Size: 8192KB (65536Kb)
```

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

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

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

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

```
FPT Operation Passed
```

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

4. Use `fptw.exe -greset` to perform a G3 power cycle. Next go to [Section 3.3](#) to check the Intel® ME Firmware status.

3.3 Checking Intel® ME Firmware Status

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

1. Copy the file **MEInfo.exe** in the "(root)\Tools\System Tools\MEInfo\DOS" directory to the root directory of a bootable USB key.
2. Boot the target system and use F2 or Del to enter the BIOS setup menu. Load default values for BIOS (on Intel® CRBs press F3 to load default values). Save and reboot (on Intel® CRBs press F4 and select Yes).
3. Boot the target system to DOS and change to the root directory of the bootable USB key. At the DOS prompt type:

```
MEInfo.exe -fwsts
```



The system should respond with a message similar to below.

```
Intel® MEInfo Version: 13.0.0.xxxx

Copyright(C) 2005 - 2017, Intel Corporation. All rights reserved.

FW Status Register1: 0x1E000255
FW Status Register2: 0x60002306
FW Status Register3: 0x00000300
FW Status Register4: 0x00004001
FW Status Register5: 0x00000101
FW Status Register6: 0x03C00FC9

Current State: Normal
ManufacturingMode: Enabled
FlashPartition: Valid
OperationalState: M0 with UMA
InitComplete: Complete
BUPLoadState: Success
ErrorCode: No Error
ModeOfOperation: Normal
Phase: HOSTCOMM Module
ICC: Valid OEM data, ICC programmed
SPI Flash Log: Not Present
ME File System Corrupted: No
FPF and ME Config Status: Not committed
```

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

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

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



3.4 Common Bring Up Issues and Troubleshooting Table

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

Problem / Issue	Solution / Workaround
System does not boot to DOS	By default, the system will boot to EFI Shell. To boot to DOS, <ol style="list-style-type: none"> 1. Enter BIOS menu, then go to the 'Boot' screen 2. Change 'Boot Option #1' to be your USB key (ensure USB key is formatted to be DOS bootable) 3. Press 'F4' to save settings and reboot
Hear 3 beeps when platform powers on	Possible device is disconnected or device not found, check <ul style="list-style-type: none"> • platform power and MCP fan power connectors • DIMM memory modules (if applicable for memory down modules) • USB devices (keyboard, mouse, USB key) may be plugged into inactive USB port • missing/incorrect jumpers • missing or poorly socketed MCP
No display on monitor	Ensure Corporate 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.

§ §

A Appendix — DnX Image Creation

This chapter covers how to create a DnX image for Lakefield platforms that are using a UFS flash storage device as a boot media. The DnX image being built must have a manifest, signed and include an OEM ID and Platform ID.

Figure A-1. High Level setup details for DnX

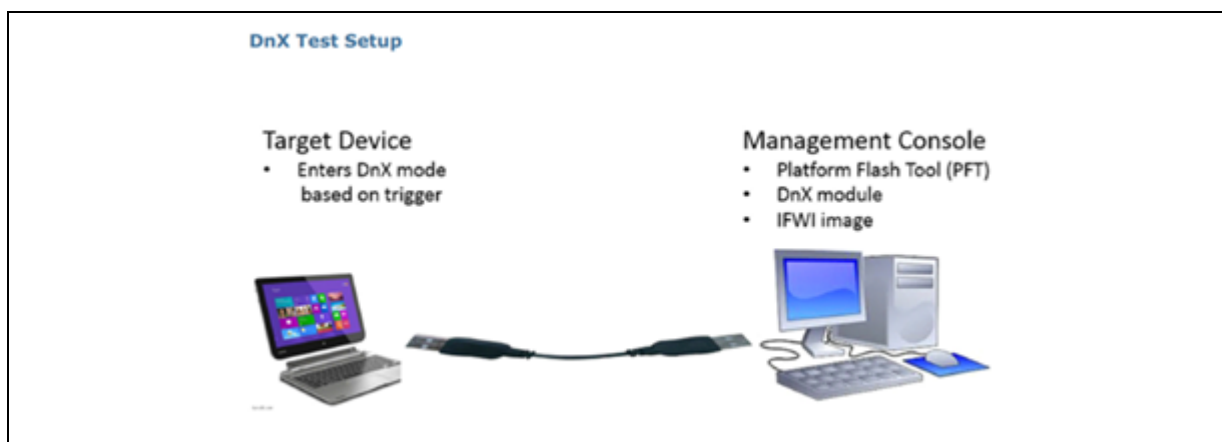


Table A-1. DnX Setup Requirements

Requirement	Description
Management Console / Recovery host	A host that can be used to execute the DnX flows.
Hardware Connection [Script in case of Virtual Platform]	USB cable connection between the Recovery Host and the platform under test.
Intel® Platform Flash Tool (PFT)	Tool that supports DnX flows running on the Recovery Host platform.
DnX Module binary	Provided in the Intel® CSME firmware kit.
DnX Image	IFWI image with DnX signed manifest to be flashed on the device under test (Created by the Intel® FIT tool provided in the Intel® CSME firmware kit).

A.1 DnX Image

Pre-requisites:

Below tools are required to create DnX images which will be flashed using DNX protocol.

- Open SSL Tool or OEM specific Tool/process
- Intel® MEU tool
- Intel® FIT Tool

Note: Ensure that the key used for signing the DnX image is the same key used for signing the OEM Key Manifest. Below steps highlights these steps.



A.1.1 Generate Key Pair for Signing

The Intel tools are designed to work together with the open source OpenSSL tool (version 1.0.2b or higher), which generates key pairs in the RSA-2048 PKCS-1.5 format. This is the only key format which is supported for the Intel IFWI image signing flow. Although other tools which generate key pairs in this format can be used for signing, Intel tools currently do not support interfacing with any other tools, and if you choose to use a different tool, Intel cannot provide any support.

The OpenSSL tool is not provided by Intel, it must be installed separately. One source for the OpenSSL binaries is Shining Light Productions, the "Light" version is sufficient. Ensure that OpenSSL.exe can be run in the directory in which it is installed, and it is able to create output files there as well, otherwise you may see errors when executing some of the commands.

You can generate a private key by running the following command from the CLI:

```
# openssl.exe genrsa -out privkey.pem 2048
```

A public key can be extracted from the private key using:

```
# openssl.exe rsa -in privkey.pem -pubout -out pubkey.pem
```

A.1.2 Using Intel® MEU Tool for Public key hash generation and OEMKey Manifest generation

A.1.2.1 Intel® MEU Configuration

To use Intel® MEU, you first need to configure the tool. To do this, run the following command:

```
# meu -gen meu_config
```

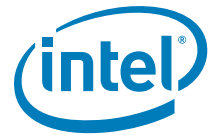
This will generate a default configuration XML file

A.1.2.2 Updating MEU_config.xml

Update MEU_config file and update signing tool path to OpenSSL Tool as well as update privatekey path.

Figure A-2. Updating MEU_config.XML





A.1.2.3 Creating the Public Key Hash

A public key hash is a binary file containing the modulus and exponent of the public key in little endian format. You can create it using the Intel® MEU Tool, Sample command:

```
C:\Tool\MEU>meu.exe -keyhash dnx_pub_hash.bin -key privkey.pem
```

Where:

dnx_pub_hash .bin = Public key hash file generated by Intel® MEU tool

privkey.pem = Private key generated using OpenSSL Tool

This will generate .bin and .txt file with public keyhash using private key.

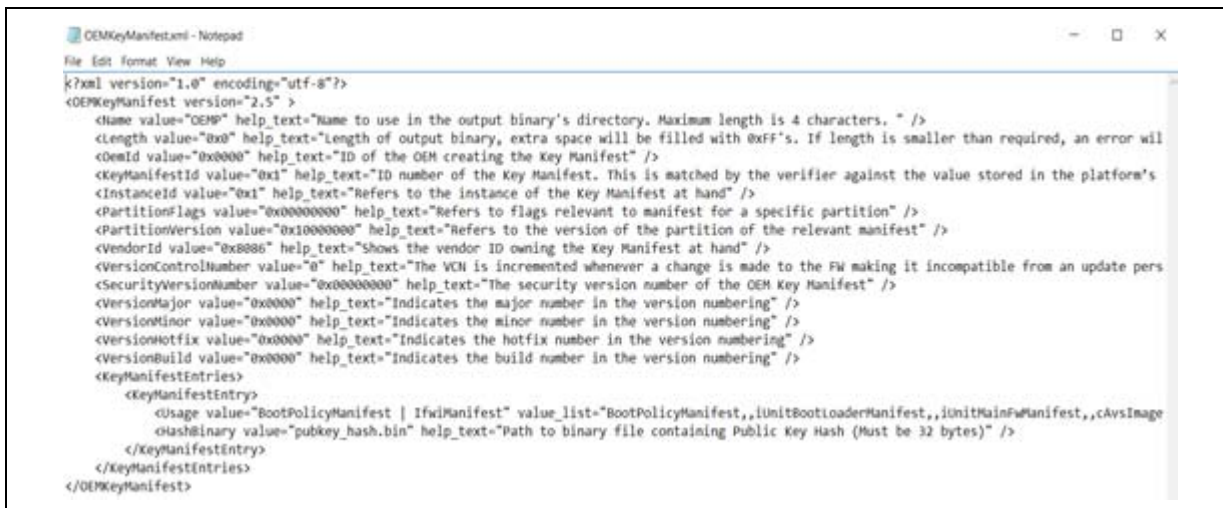
A.1.2.4 Create Manifest using MEU tool

The manifest file xml template can be generated using the following command:

```
# meu -gen OEMKeyManifest
```

This generates an xml template with a single KeyManifestEntry node, which lists the file type, and the path to its public key hash.

Figure A-3. Default OEM Key Manifest XML



A.1.2.5 Update OEM Key Manifest XML with Public hash key

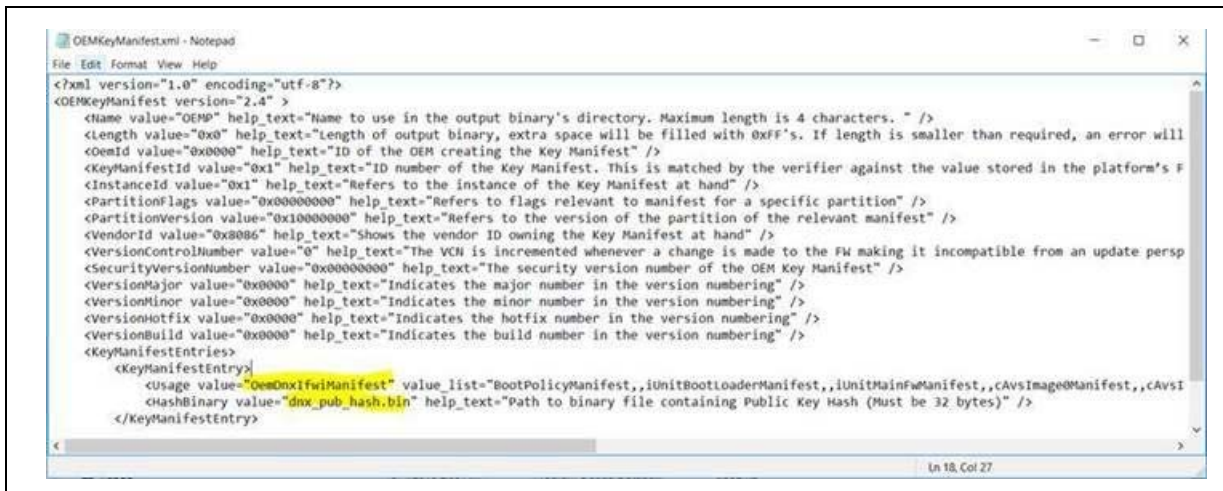
Once sample XML is generated, it should be updated with public key hash and file node.

For more detail, please review Intel® MEU Tool user guide.

See [Figure A-4](#)



Figure A-4. Updating OEM Key Manifest XML with Public hash key



A.1.2.6 Generate OEM Key Manifest Binary

Once the OEM Key Manifest xml has been edited to include all the required hashes, the MEU can be run with the xml as input, to manifest and sign it with the private key created for this purpose.

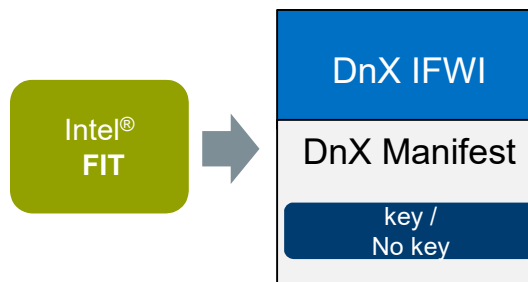
```
# meu.exe -f OEMKeyManifest.xml -o OEMKeyManifest.bin - key privatekey.pem
```

It is only necessary to override the private key for signing (as in the example) if the key is different to that defined in the default Intel MEU configuration XML.

A.1.2.7 Create DnX image

There are two ways to create a DnX Image:

A.1.2.7.1 Using Intel® FIT:



Below parameters under Intel® FIT tool need to be updated in order to create DnX image for DnX flash process.

Intel® FIT interfaces with Intel® MEU to generate Manifest and sign a DnX image during compilation time.



- Intel® FIT Tool-> **Platform Protection-> OemPublicKeyHash** – add public key has of the private key which will be used to sign DnX IFWI image
- Intel® FIT Tool-> **Platform Protection-> OEM Key Manifest Binary** – path to OEM keyManifest
- Intel® FIT Tool-> **Download and Execute-> DnxEnabled** – set to 'Yes' to enable DnX post EOM
- Intel® FIT Tool-> **Download and Execute-> BuildEnabled** – set to 'Yes' to build a DnX Image
- Intel® FIT Tool-> **Download and Execute-> SigningKey** – path to private key to sign a DnX Image
- Intel® FIT Tool-> **Download and Execute-> Outputfilename** – Path and name of the DnX image
- Intel® FIT Tool-> **Download and Execute-> Platform ID** - DnX Image attribute. Ignored before EOM. After EOM, this value will be compared to "Platform ID" FPF defined for the image used at EOM. If the values don't match, DnX Image will not be accepted by DnX module.
- Intel® FIT Tool-> **Download and Execute-> OEM ID** - DnX Image attribute. Ignored before EOM. After EOM, this value will be compared to "OEM ID" FPF defined for the image used at EOM. If the values don't match, DnX Image will not be accepted by DnX module.
- Intel® FIT Tool -> **Build->Build Settings-> Intel® Manifest Extension Utility Path** – path to Lakefield Intel® MEU tool; available within Intel® CSME Kit.
- Intel® FIT Tool -> **Build-> Build Settings-> SigningToolPath** – path to Open SSL tool (from SSL installation directory).
- Intel® FIT Tool -> **Build-> Build Settings-> SigningTool** – to choose a signing tool. When set to 'OpenSSL', will use this tool to sign the manifest. When set to 'Disabled', manifest will not be signed and there will be no key inside the manifest.

Note that with those setting, Intel® FIT will build DnX Image in addition to the regular IFWI.

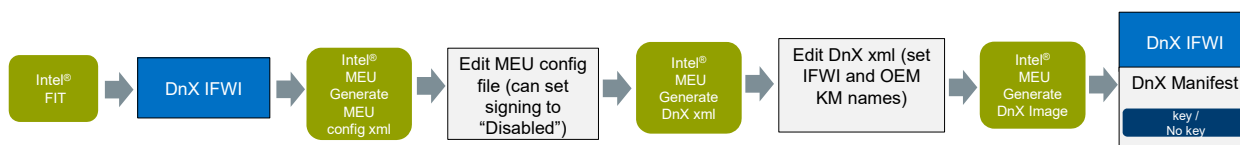
A.1.2.7.2 Using Intel® FIT to produce an IFWI and then Intel® MEU to create a DnX Image based on it.

When creating the regular IFWI, make sure to have this configuration:

- Intel® FIT Tool-> **Download and Execute-> DnxEnabled** – set to 'Yes' to enable DnX post EOM
- Intel® FIT Tool-> **Download and Execute-> BuildEnabled** – set to 'No' so that only regular IFWI is build, but not the DnX Image.

There is no need to touch rest of the parameters in **Download and Execute** tab.

Then use Intel® MEU tool to generate DnX Image. This is the flow:



Similarly to the first option, there is a way to disable signing of the manifest. It can be done by setting SigningTool to 'Disabled' in the meu_config.xml:



```

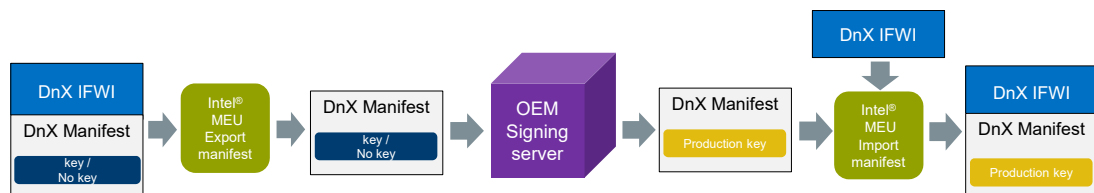
1  <?xml version="1.0" encoding="utf-8"?>
2  <MeuConfig version="2.5" >
3    <PathVars label="Path Variables">
4      <WorkingDir value="." label="$WorkingDir" help_text="Path for environment variable
5      <SourceDir value="." label="$SourceDir" help_text="Path for environment variable
6      <DestDir value="." label="$DestDir" help_text="Path for environment variable $Des
7      <UserVar1 value="." label="$UserVar1" help_text="Path for environment variable $U
8      <UserVar2 value="." label="$UserVar2" help_text="Path for environment variable $U
9      <UserVar3 value="." label="$UserVar3" help_text="Path for environment variable $U
10   </PathVars>
11   <SigningConfig label="Signing Configuration">
12     <SigningTool value="Disabled" value_list="Disabled,,OpenSSL" label="Signing Tool"
13     <SigningToolPath value="C:\Signing\openssl\openssl 1.0.2\openssl.exe" label="Signi
14     <PrivateKeyPath value="privateKey.pem" label="Private Key Path" help_text="Path to
15   </SigningConfig>
16   <CompressionConfig label="Compression Configuration">
17     <LzmaToolPath value="" label="LZMA Tool Path" help_text="Path to lzma tool executab
18   </CompressionConfig>
19 </MeuConfig>

```

Both methods should result in the same DnX Image.

A.1.2.7.3 Replace a key from Intel® FIT / MEU with production key

Following flow describes how to replace a key from Intel® FIT / MEU with actual OEM key by using Intel® MEU and OEM signing server





A.1.2.8 Examples

Figure A-1. Intel® FIT -> Platform Protection

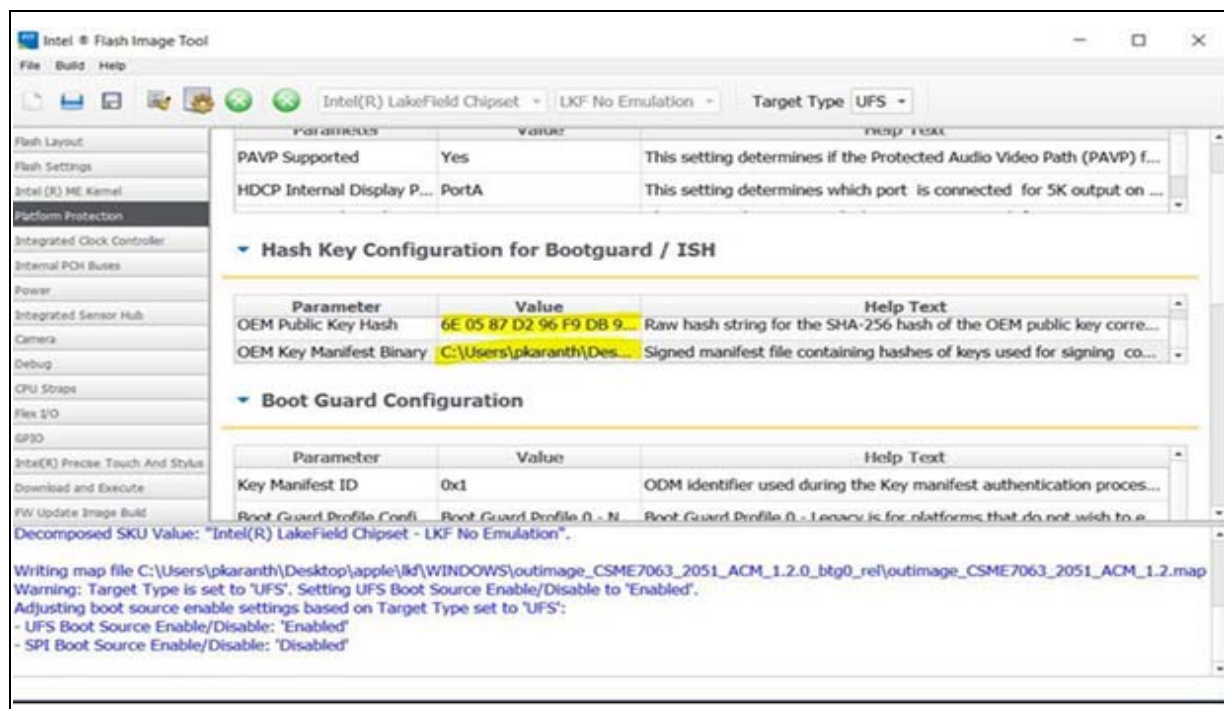
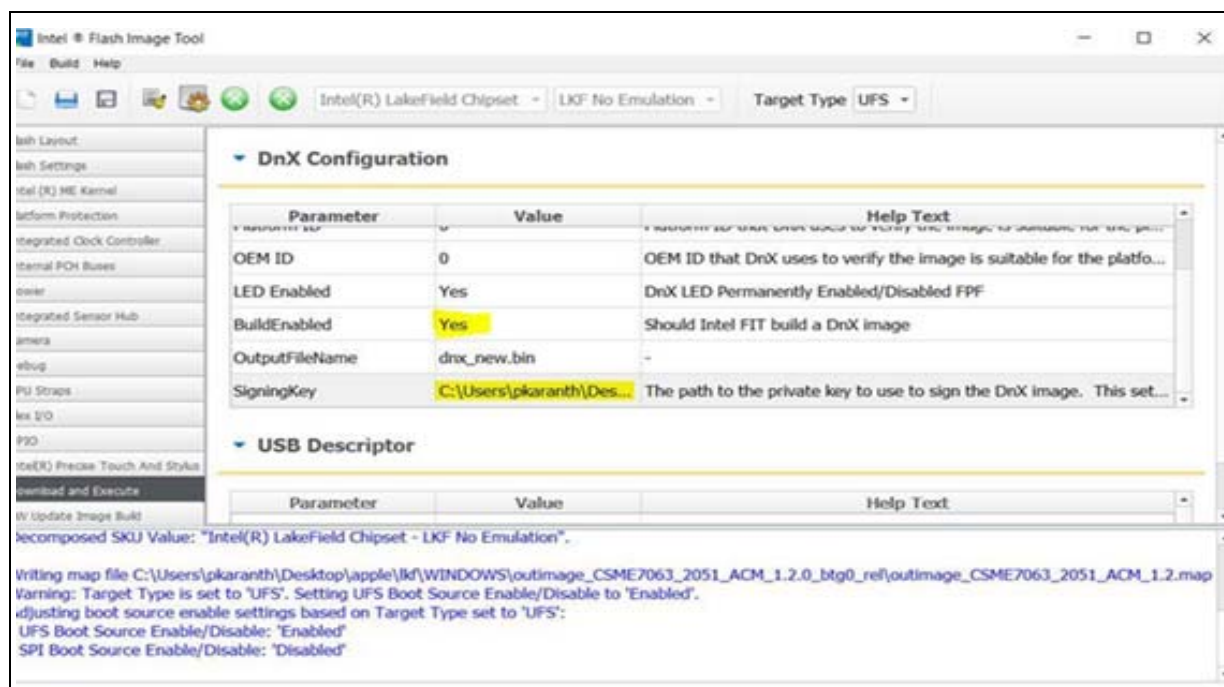


Figure A-2. Intel® FIT -> Download and Execute





B Appendix — Intel® ICCS SKU Support Matrix

The following table describes ICC features supported for specific PCH SKU, clock range (maximum and minimum), spread mode supported by Lake Field SKUs.

Note: Please refer to Lake Field Platform Controller Hub (PCH) External Design Specification (EDS) for details about Lake Field Chipset Clock architecture

In below tables,

Min = Clock Div Max (minimum allowed frequency)

Max = Clock Div Min (maximum allowed frequency)

B.1 Intel® ICCS SKU Matrix - LKF

- **Note:** ICC SKU is divided into 2 categories: Basic and Enhanced. Enhanced is supported across all SKUs.

Figure B-1. Intel® ICCS SKU Matrix - LKF

PCH SKU	Basic	Enhanced
Features Supported	Standard Clock Configuration	Standard Clock Configuration Adaptive Clock Configuration
Pre-Defined ICC profile supported	Standard	Standard Adaptive
Clock Range Supported	[Min-Max] = 100 MHz.	BCLK [Min-Max] = 98 - 100 MHz.
SSC Supported	Down SSC: 0 - 0.5%	Down SSC: 0 - 0.5%



C Appendix — Boot Guard Configuration

C.1 Boot Guard Profiles

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

Table C-1. Profile Description

Index	Profile Name	F	V	M	ENF	PBE	Description
0	Boot Guard Profile - No_FVME	0	0	0	00	0	This configuration will invoke Boot Guard during boot with neither Verification nor Measurement. For platforms with all the required Boot Guard components but do not wish to enable Boot Guard boot block verification protection.
3	Boot Guard VM	0	1	1	00	1	When Verification and Measured are desired and the asset protection is provided by TPM protection.
4	Boot Guard FVE	1	1	0	11	1	Strict Verification enforcement.
5	Boot Guard FVME	1	1	1	11	1	Strict Verification and Measured enforcement. Prevents unverified IBB from running.

C.2 Enforcement Policies

Table C-2. Enforcement Policy Description

Error Enforcement Policy (ENF)	Enforcement Mode Name	Description
00	Unrestricted Mode	Infinite time before shutdown – don't shutdown the platform, let everything run normally.
11	Restricted Mode	0 minutes before shutdown – instant shutdown policy.



C.3 OEM Profile Parameters

Table C-3. Profile Parameters Description

Parameter	Description	Settings
Force Boot Guard ACM Enabled (F)	Force Boot Guard Boot determines if the platform starts the Force Boot Guard Boot timer. If it successfully starts it indicates success. When the Force Boot Guard timer stops, it starts the Protect Bios Environment timer, if indicated by the boot policy restrictions. Anchor ACM then jumps to the Initial Boot Block (IBB) with the Force Boot Guard Boot time stopped and the Protect BIOS enable timer running.	false - Allow the CPU to jump to the legacy reset vector if the Boot Guard Module cannot be successfully loaded. (default) true - Force the Boot Guard ACM to execute.
Verified Boot Enabled (V)	Boot Guard cryptographically verifies the platform Initial Boot Block (IBB) using the boot policy key. On successful verification, Boot Guard executes Initial Boot Block (IBB) using the boot policy key. If the verification fails, Anchor signals or enters Remediation.	false - Platform does not perform verified boot (default) true - Platform performs verified boot
Measured Boot Enabled (M)	Boot Guard measures the Initial Boot Block (IBB) into the TPM. Boot Guard perform no verification that the IBB is correct or from the platform manufacturer. The Skylake implementation of Boot Guard will support measurements into TPM or Intel's Platform Trust Technology.	false - Platform does not perform measured boot (default) true - Platform performs measured boot
Protect Bios Environment Enabled (PBE)	Platform manufacturer may want Initial boot block to be protected between verification/ measurement and execution from attacks on buses and non-CPU components. Boot Guard accomplishes this by allowing the initial boot block to be verified and executed in LLC in NEM if PBE is enabled.	false - Take no actions to control the environment during execution of the BIOS components (default) true - Takes actions to control the environment during the execution of the BIOS components.
Error Enforcement Policy (ENF)	Boot Guard invokes the Enforcement Policy when a fatal error is encountered. The action taken by ENF is determined by the OEM set persistent policies. Like, <ul style="list-style-type: none"> Allowing platform to continue to boot Immediate Shutdown Shutdown with Timeout intervals When the ENF logic is invoked, PTT or TPM also disconnects.	See Section C-2 for details.



D Appendix — Intel® Platform Trust Technology

D.1 Intel® Platform Trust Technology

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

Note: Information in this section is preliminary and subject to change.

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

Configuration	Platform Protection > Intel® PTT Configuration Intel® PTT initial power up state	Platform Protection > Intel® PTT Configuration Intel® PTT Supported	Platform Protection > Intel® PTT Configuration Intel® PTT Supported [FPF]	Description
Intel® PTT Permanently Disabled in HW via FPF	Disabled	No	No	After the End of Manufacturing command, this setting will permanently set into the FPFs contained in the MCP. If disabled, the specific MCP can never be enabled for Intel® PTT.
Intel® PTT Permanently Disabled in base firmware image	Disabled	No	Yes	This setting allows Intel® PTT to be set to disabled without disabling the MCP FPFs. This is the recommended option to permanently disable Intel® PTT on a platform.
Intel® PTT Ship State Disabled in base firmware image	Disabled	Yes	Yes	Intel® PTT initially shipped in disabled mode, can be enabled by BIOS command.
Intel® PTT Enabled	Enabled	Yes	Yes	This is the recommended option to enable Intel® PTT on a platform.