



Raptor Lake-S Intel® Converged Security and Management Engine Firmware 17.0

Consumer Firmware Bring Up Guide

November 2021

Revision 0.85

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 ITigerNSE to any patent claim thereafter drafted which includes subject matter disclosed herein.

INFORMATION IN THIS DOCUMENT IS PROVIDED IN CONNECTION WITH Intel® PRODUCTS. NO LTigerNSE, 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, OFFTigerRS, 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 Raptor Lake Platform and Raptor Lake 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.

Intel® AMT should be used by a knowledgeable IT administrator and requires enabled systems, software, activation, and connection to a corporate network. Intel AMT functionality on mobile systems may be limited in some situations. Your results will depend on your specific implementation. Learn more by visiting [Intel® Active Management Technology](#).

Intel® Small Business Technology (Intel® SBT) requires an Intel® Small Business Technology enabled system and proper configuration. Availability of features will depend upon the setup and configuration by your PC manufacturer. Consult your system manufacturer.

Intel® vPro™ Technology requires setup and activation by a knowledgeable IT administrator. Availability of features and results will depend upon the setup and configuration of your hardware, software and IT environment. Learn more at: <http://www.intel.com/technology/vpro>.

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, Intel vPro™, 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.

KVM Remote Control (Keyboard, Video, Mouse) is only available with Intel® Core™ i5 vPro™ and Core™ i7 vPro™ processors with integrated graphics and Intel® Active Management technology activated. Discrete graphics are not supported.

Copyright © 2014-2021, Intel Corporation. All rights reserved.

Contents

1	Introduction	6
1.1	Related Documentation	6
1.2	Prerequisites	6
1.3	Acronyms and Definitions	7
1.3.1	General	7
1.3.2	Intel® Converged Security and Management Engine	8
1.3.3	System States and Power Management	9
1.4	Reference Documents	9
1.5	Format and Notation	10
1.6	Kit Contents	11
1.7	External Hardware Requirements for Bring Up	16
2	Image Creation: Intel® Flash Image Tool	17
2.1	Start Intel® Modular FIT	17
2.2	Step-by-Step Guide to Build SPI Flash Image with Intel® MFIT Interface	17
3	Programming SPI Flash Devices and Checking Firmware Status	116
3.1	Flash Burner/Programmer	116
3.1.1	In-Circuit SPI Flash Programming for CRB	116
3.2	Flash Programming Tool (Intel® FPT)	116
3.2.1	Intel® FPT Windows* Version	117
3.3	Checking Intel® CSME Firmware Status	117
3.4	Common Bring Up Issues and Troubleshooting Table	119
A	Appendix — Flash Configurations	120
B	Appendix — Boot Guard Configuration	121
C	Appendix — Intel® Platform Trust Technology	123
D	Appendix — Integrated Sensor Hub (ISH) Public Key Settings	124

Figures

Tables

1-1	Number Format Notation.....	10
1-2	Data Format Notation	10
1-3	Kit Contents	11
2-1	- Initial Screen Layout	18
2-2	- Build Settings.....	26
2-3	- Flash Layout	29
2-4	- Flash Settings	35
2-5	- GPIO.....	45
2-6	- Internal PCH Buses	47
2-7	- Power	54
2-8	- Networking & Connectivity	56
2-9	- Flex I/O Straps.....	58
2-10	- Platform Protection	79
2-11	- Debug.....	86
2-12	- Intel® ME Kernel	92
2-13	- Integrated Sensor Hub	97
2-14	- Integrated Clock Controller	99
2-15	- CPU Straps	107
2-16	- FW Update Image Build	110
2-17	- Platform Service Record Configuration	110
2-18	- Intel® AMT	111
2-19	- Camera	111
2-20	- Intel® Unique Platform ID.....	112
2-21	- Dnx	113
2-22	- Intel® FIT - Build Image	115
3-1	Common Bring Up Issues and Troubleshooting Table	119

Revision History

Document Number	Revision Number	Description - External Release	Revision Date
	0.7	Initial Release	March 2021
	0.8	Revised to v0.8	August 2021
	0.81	Updated values for RPMC settings	August 2021
	0.82	Updated Master Access Permissions sections	August 2021
	0.83	Added OEM Certificate Stream Creation Appendix F	September 2021
	0.84	Added Platform Service Record Configuration settings	November 2021
	0.85	Updated default values for CPU Debugging and Intel® ME Region Flash Protection Override settings	November 2021

§ §

1 Introduction

This document covers the Intel® Converged Security and Management Engine Firmware (Intel® CSME) 17.0 - Consumer / Corporate Firmware bring up procedure. Intel® CSME 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® CSME FW region — Contains firmware for the Intel® Converged Security and Management Engine.
- **[optional]** GbE region — Contains firmware for Intel LAN solution.

For more details on SPI Flash layout, see the document **Raptor Lake-S SPI Programming Guide** SPI 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® ME Consumer FW is operating as expected.

1.1 Related Documentation

VIP: Kit# WIP - Intel® Ethernet Network Connections (xx.x OEM Gen) - LAN Software

CDI # WIP Intel® Ethernet Connection i2xx

Intel® CSME 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® CSME FW will have limited capabilities to perform targeted workarounds for silicon issues. **Benefit:** Allows Intel® CSME FW to address some issues that otherwise would require a new silicon stepping.

1.2 Prerequisites

Before this document is read and utilized, it is essential that the reader first review the Consumer FW Release Notes (included with this Intel® ME Consumer 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 Raptor Lake S based
- The platform is equipped with one or more SPI Flash devices with a total capacity sufficient for storing all relevant firmware images.

1.3 Acronyms and Definitions

1.3.1 General

Acronym or Term	Definition
BIOS	Basic Input Output System
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® CSME	Intel® Converged Security and Management Engine (Intel® CSME)
Intel® MFIT	Intel® Modular Flash Image Tool
Intel® MEI	Intel® Converged Security and Management Engine Interface (Intel® MEI) (renamed from HECI)
Intel® PTT	Intel® Platform Trusted Technology (Intel® PPT)
Intel® MSS	Intel® Management and Security Status Application
KVM	Keyboard, Video, Mouse
LAN	Local Area Network
MCP	Multi-Chip Package (Central Processing Unit / Platform Controller Hub)
NVM	Non-Volatile Memory
OOB	Out-of-Band
OS	Operating System
PAVP	Protected Audio and Video Path
PCI	Peripheral Component Interconnect
PCIe*	Peripheral Component Interconnect Express
PHY	Physical Layer (Networking)
RTC	Real Time Clock
SBT	Intel® Small Business Technology
SMBus	System Management Bus

Acronym or Term	Definition
SPI Flash	Serial Peripheral Interface Flash
TPM	Trusted Platform Module
VSCC	Vendor Specific Configuration

1.3.2 Intel® Converged Security and Management Engine

Acronym or Term	Definition
3PDS	3rd Party Data Storage
Agent	Software that runs on a client PC with OS running
End User	The person who uses the computer (either Desktop or Mobile). In corporate, the user usually does not have administrator privileges.
Host or Host CPU	The processor that is running the operating system. This is different than the management processor running the Intel® Converged Security and Management Engine Firmware.
Host ServTiger/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 and Management Engine Interface (Intel® MEI)	Interface between the Converged Security and Management Engine and the Host system
Intel® MEI driver	Intel® ME host driver that runs on the host and interfaces between ISV Agents and the Intel® ME HW.
IT User	Information Technology User. Typically very technical and uses a management console to ensure functionality of multiple PCs on a network.
LMS	Local Management ServTiger: A SW application which runs on the host machine and provide a secured communication between the ISV agent and the Intel® Converged Security and Management Engine Firmware.
Intel® CSME	Intel® Converged Security and Management 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® AMT current implementation, this is achieved using a FLASH memory device.
OOB Interface	Out Of Band interface: This is WSMAN interface over secure or non-secure TCP protocol.
OS not Functional	The Host OS is considered non-functional in Sx power state and any one of the following cases when system is in S0 power state: <ul style="list-style-type: none"> • OS is hung • After PCI reset • OS watch dog expires • OS is not present
System States	Operating System power states such as S0. See detailed definitions in System States and Power Management section.

1.3.3 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 and Management Engine firmware power state where all hardware power planes are activated. The host power state is S0.
CM3	Intel® Converged Security and Management Engine power state where the host is in Sx. The processor DRAM Controller is turned off and DRAM power stays in off/self refresh mode. There is no UMA usage in CM3 state. Less than 1MB of SRAM used for code and data. Code is executed off of flash takes ~1mS.
CM0-PG	Core Well Powered; Intel® ME Well Powered; (Intel® ME core not consuming power) DRAM available.
CM3-PG	An Intel® ME Firmware power state where no power is applied to the Converged Security and Management Engine subsystem. (Intel® ME firmware is shut down).
OS Hibernate	System state where the OS state is saved on the hard drive.
S0	A system state where power is applied to all HW devices and the system is running normally.
S1, S2, S3	A system state where the host CPU is halted but power remains available to the memory system (memory is in self-refresh mode).
S4	A system state where the host CPU and memory are not active.
S5	A system state where all power to the host system is off, however the power cord (and/or battery in mobile designs) is still connected.
Shut Down	Equivalent to the S5 state.
Snooze Mode	Intel® Converged Security and Management Engine activities are mostly suspended to save power. The Intel® Converged Security and Management Engine monitors HW activities and can restore its activities depending on the HW event.
Standby	System state where the OS state is saved in memory and resumed from the memory when mouse/keyboard is clicked.
Sx	All S states which are different than S0.

1.4 Reference Documents

Document	Doc Number/ Location*
<i>Raptor Lake Intel® Converged Security and Management Engine (Intel® CSME) and Embedded Controller Interaction Product Specification Revision 0.5</i>	TBD / CDI
<i>Intel® Converged Security and Management Engine BIOS Writers Guide</i>	TBD / *
<i>Intel® Converged Security and Management Engine (Intel® CSME) 17 SKU Firmware Consumer Compliance Guide for Raptor Lake PCH-S Chipset Family - Raptor Lake Platform Compliancy and Testing Guide - Revision x.x</i>	TBD / CDI

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

1.5 Format and Notation

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

Table 1-1. Number Format Notation

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

Table 1-2. Data Format Notation

Data Type	Notation	Size
Bit	b	Smallest unit, 0 or 1
Byte	B	8 bits
Word	W	16 bits or 2 bytes
Double-word	DW	32 bits or 4 bytes
Quad-word	QW	8 bytes or 4 words
Kilobyte	KB	1024 bytes
Megabit	Mb	1,048,576 bits or 128 KB
Megabyte	MB	1,048,576 bytes or 1024 KB
Gigabit	Gb	1,073,741,824 bits
Gigabyte	GB	1024 MB

1.6 Kit Contents

The Intel® ME Consumer 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 5)

File or [Directory]	Content Description
[root]	Root directory
RPP-S Consumer Bring Up Guide.pdf	This document
Raptorlake-S Client SPI Programming Guide.pdf	How to program SPI device parameters and descriptor region details. Also contains a complete SPI Flash softstrap reference.
Images Components	
3rd party Licenses in Security FW	3rd Party License code in Intel® CSME firmware
Apache Harmony Apache Version 2.0, January 2004 w header.txt	
Apache-Xerces-Java-XML-Parser.txt	
ConvertUTF unicode license.txt	
Copyright Intel Corporation.txt	
CxImage license complete.txt	
HTTP Client C MIT license.txt	
llvm.org University of Illinois_NCSA.txt	
Microsoft TPM 2.0 BSD Two Clause License.txt	
Minix 3.pdf	
MIT Kerberos for Windows.pdf	
newlib_licenses.txt	
Synopsys UFS Host Controller OS.pdf	
wpa supplicant license.txt	
zlib license.txt	
CSME	
PreProduction	
CSME_FW_Consumer_17.0.0.xxxx.bin	Intel® CSME firmware image (Non Production FW) - supports unfused Raptor Lake PCH Platform I/O steppings: <ul style="list-style-type: none"> • Unfused (Super SKU) <p>Note: For PAVP Testing, you must match Production FW with Production Part and Non Production FW with Non Production Parts.</p>
NPHY	
PreProduction	
RPLS_NPHY_13.00x.xxx.xxxx.bin	Pre-Production NPHY binary
PCHC	
PreProduction	
pchc_17.0.0.xxxx.bin	Pre-Production PCHC binary

Table 1-3. Kit Contents (Sheet 2 of 5)

File or [Directory]	Content Description
PMC	
PreProduction	
RPPS_PMC_FW_160.xx.xx.xxxx.bin	Pre-Production PMC binary
Prestitched	
PreProduction	
ADL_S_Cons_FWUpdate.bin	Pre-Production pre-stitched firmware update binary
SPHY	
PreProduction	
RPPS_sphy_13.0.x.xxxx.bin	Pre-Production SPHY binary
Installers	
Intel(R)_CSME_SW_Installation_Guide.pdf	Intel® CSME software installation guide
Intel(R)_MSS_User_Guide.pdf	Intel® Management and Security Status Application User Guide
3rd party Licenses in Security FW	3rd Party License code in Intel® CSME firmware
Apache Harmony Apache Version 2.0, January 2004 w header.txt	
Apache-Xerces-Java-XML-Parser.txt	
ConvertUTF unicode license.txt	
Copyright Intel Corporation.txt	
CxImage license complete.txt	
HTTP Client C MIT license.txt	
llvm.org University of Illinois_NCSA.txt	
Microsoft TPM 2.0 BSD Two Clause License.txt	
Minix 3.pdf	
MIT Kerberos for Windows.pdf	
newlib_licenses.txt	
Synopsys UFS Host Controller OS.pdf	
wpa supplicant license.txt	
zlib license.txt	
ME_SW_DCH	
IntelMEFWVer.dll	Intel® CSME software DCH installer files
mup.xml	
SetupME.exe	
MEI-Only Installer MSI	
IntelMEFWVer.dll	Intel® CSME software MEI Only MSI installer files
mup.xml	
SetupME.exe	

Table 1-3. Kit Contents (Sheet 3 of 5)

File or [Directory]	Content Description
WindowsDriverPackages	Individual Windows drivers and services for Intel® CSME
ICLS	
JHI	
MEI	
WiMan	
wiman_wlan_extension	
Tools	
3rd party Licenses in Security Tools	3rd Party License code in Security Tools
Android Autogenerated Files Apache 2.0.pdf	
C Make License.pdf	
Copyright Intel Corporation.txt	
EFI tool kit intel BSD 2 clause license.txt	
Expat XMLparser MIT license.txt	
Jquery MIT license.txt	
JsonCpp MIT license.txt	
MSDN Example code.pdf	
pugixml license.txt	
System_Tools	
SLA_TOOLS.PDF	Intel software license agreement for MEInfo and FWUpdate tools
System Tools User Guide.pdf	System Tools User Guide documentation
Tools Errors User Guide.pdf	System Tools Error messages documentation
FPT	
Efi64	
Fpt.efi	EFI 64bit version of Intel® Flash Programming Tool (FPT) executable file.
Linux64	
FPT	Linux version of Intel® Flash Programming Tool (FPT) executable file.
Windows32	
FPTW.exe	Windows 32bit version of Intel® Flash Programming Tool (FPT) executable file.
Windows64	
FPTW64.exe	Windows 64bit version of Intel® Flash Programming Tool (FPT) executable file.
FWUpdate	
Efi64	
errorlist.c	EFI 64bit error list C library
errorlist.h	EFI 64bit error list C header file
FwUpdateEfiLib.lib	EFI 64bit Firmware Update Library file
fwupdatelib.h	EFI 64bit Firmware Update Library C header file
FWUpdLcl.efi	EFI 64bit Firmware Update executable file.
Linux64	

Table 1-3. Kit Contents (Sheet 4 of 5)




File or [Directory]	Content Description
FWUpdLcl	Linux 64bit Firmware Updated executable file.
Windows32	
errorlist.c	Windows 32bit error list C library
errorlist.h	Windows 32bit error list C header file
fwupdatelib.h	Windows 32bit Firmware Update Library C header file
FwUpdateEfiLib.lib	Windows 32bit Firmware Update Library file
FWUpdateSample.c	Windows 32bit Firmware Update C Sample code
FWUpdLcl.exe	Windows 32bit Firmware Updated executable file.
Windows64	
errorlist.c	Windows 64bit error list C library
errorlist.h	Windows 64bit error list C header file
fwupdatelib.h	Windows 64bit Firmware Update Library C header file
FwUpdateEfiLib.lib	Windows 64bit Firmware Update Library file
FWUpdateSample.c	Windows 64bit Firmware Update C Sample code
FWUpdLcl64.exe	Windows 64bit Firmware Updated executable file.
FWUpdate_RS	
Efi64	
errorlist.c	Reduced source EFI 64bit error list C library
errorlist.h	Reduced source EFI 64bit error list C header file
FwUpdateEfiLib.lib	Reduced source EFI 64bit Firmware Update Library file
fwupdatelib.h	Reduced source EFI 64bit Firmware Update Library C header file
FWUpdLcl.efi	Reduced source EFI 64bit Firmware Update executable file.
FWUpdLclApp.c	Reduced source EFI 64bit Firmware Update sample application C file
ICC Tools	
ICC SDK	
Intel(R)_CSME_FW_ICC_Tools_User_Guide.pdf	
Windows32	
icc_sdk_api.h	Windows 32bit ICC SDK API C header file
IccSdk.dll	Windows 32bit ICC SDK DLL file
IccSdk.lib	Windows 32bit ICC SDK Library file
Windows64	
icc_sdk_api.h	Windows 64bit ICC SDK API C header file
IccSdk.dll	Windows 64bit ICC SDK DLL file
IccSdk.lib	Windows 64bit ICC SDK Library file
MEInfo	
Efi64	

Table 1-3. Kit Contents (Sheet 5 of 5)

File or [Directory]		Content Description
	MEInfo.efi	EFI 64bit ME Information tool (MEInfo) executable
	Linux64	
	MEInfo	Linux 64bit ME Information tool (MEInfo) executable
	Windows32	
	MEInfoWin.exe	Windows 32bit ME Information tool (MEInfo) executable
	Windows64	
	MEInfoWin64.exe	Windows 64bit ME Information tool (MEInfo) executable
	MEManuf	
	Efi64	
	MEManuf.efi	EFI 64bit ME Manufacturing tool (MEManuf) executable
	Linux64	
	MEManuf	Linux 64bit ME Manufacturing tool (MEManuf) executable
	Windows32	
	MEManufWin.exe	Windows 32bit ME Manufacturing tool (MEManuf) executable
	Windows64	
	MEManufWin64.exe	Windows 64bit ME Manufacturing tool (MEManuf) executable
	MEU	
	ADL_Signing_and_Manifesting_User_Guide.pdf	
	Linux64	
	meu	Linux 64bit Signing and Manifest (MEU) executable
	Windows32	
	meu.exe	Windows 32bit Signing and Manifest (MEU) executable
	MFIT	
	Linux64	
	mfit	Linux version of the Modular FIT tool (MFIT)
	Windows32	
	mfit.exe	Windows version of the Modular FIT tool (MFIT)

1.7 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® Modular Flash Image Tool (Intel® MFIT) can be used to generate either a full SPI Flash binary image with Descriptor, GbE, BIOS, and Intel® CSME Regions. Additionally, it can be used to create a simple image containing only the Intel® CSME 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® Modular FIT

1. Invoke Intel® Flash Image Tool. Using Explorer*, navigate to **[root]\Tools\System Tools\MFIT**. Verify that the directory contents are correct (see [Section 1.6](#)). Double-click **MFIT.exe**.
2. **NOTE:** In the tables below, where default settings are listed for RPP-S, 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 Flash Image with Intel® MFIT Interface

Table 2-1. - Initial Screen Layout (Sheet 1 of 8)

#	Icon	Description
1		This button labeled 'New image from layout' upon selection allows opening of a new session with default values.
2		This button labeled 'Decompose image' upon selection allows decomposition of binary file images previous built by Intel® MFIT.
3		This button labeled 'Load config' upon selection allows the user to load previously created image layout XML files
4		This button labeled 'Save config' upon selection allows the user to save image layout XML files
5		This button labeled 'Build' upon selection allows build of the image
6		This allows the user to make context sensitive searches inside Intel® MFIT for features and setting options (i.e. eSPI, SMBus, PCIe, AMT etc.)

Table 2-1. - Initial Screen Layout (Sheet 2 of 8)




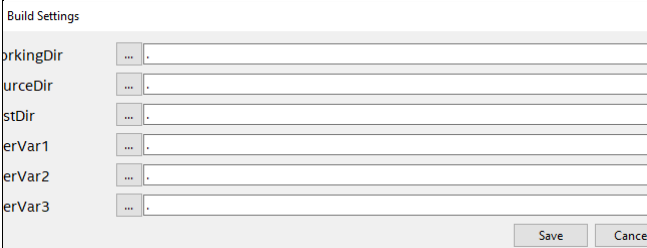

7		<p>The following settings control the output of information in the bottom display window of the Intel® Modular FIT tool.</p> <p>i Displays Intel® Modular FIT specific output information (i.e. Status, Platform Layout being used etc.).</p> <p>? Displays context sensitive help text information on specific settings when the mouse cursor hovering over the setting.</p> <p>! This setting turns off all output information bottom display window of the Intel® Modular FIT tool.</p>
8		<p>This option allows the user to display the Intel® Modular FIT output log file.</p>
9		<p>This option allows the user to configure the build settings for configuring source and output paths.</p> 
10		<p>This option allows the user to displays the license information for Intel® Modular FIT.</p>

Table 2-1. - Initial Screen Layout (Sheet 3 of 8)

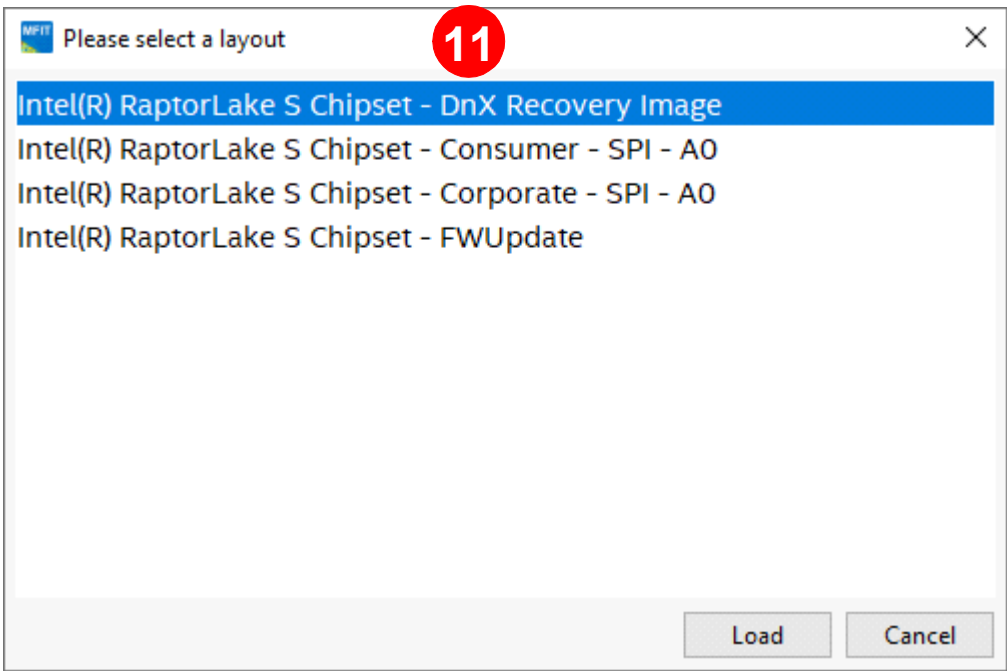

		
#	Label	Description
11	New image from layout 	On selection of the 'New image from layout' radio button you will be presented with the menu for selection for which platform chipset type the image is going to be based on. Note: Setting options which are specific to Corporate SKU configurations will not be shown in the GUI when a Consumer SKU Layout is selected.

Table 2-1. - Initial Screen Layout (Sheet 4 of 8)

#	Label	Contents
12	Build Settings	Build Settings which contains (see Table 2-2) <ul style="list-style-type: none"> ● Build Results ● Harness Global Data
13	Flash Layout	Flash Layout which contains (see Table 2-3): <ul style="list-style-type: none"> ● EC Region ● Descriptor Region ● GbE Region ● IFWI: Intel® ME and PMC Region ● Sub Partitions ● PDR Region ● BIOS Region
14	Flash Settings	Flash Settings which contains (see Table 2-4): <ul style="list-style-type: none"> ● Flash Configuration ● Host CPU / BIOS Master Access ● Intel® ME Master Access ● GBE Master Access ● EC Master Access ● BIOS Configuration ● Flash Components ● VSCC Table - VSCC Entries ● FPF Configuration ● RPMC Configuration
15	GPIO Tab	GPIO which contains (see Table 2-5): <ul style="list-style-type: none"> ● GPIO VCCIO Voltage Control

Table 2-1. - Initial Screen Layout (Sheet 5 of 8)

#	Label	Contents
16	Internal PCH Buses Tab	Internal PCH Buses which contains (see Table 2-6): <ul style="list-style-type: none">● SMBus / SMLink Configuration● eSPI Configuration● OPI / DMI Configuration● DMI Configuration● PCH Timer Configuration
17	Power Tab	Power which contains (see Table 2-7): <ul style="list-style-type: none">● Platform Power● Deep Sx● PCH Thermal Reporting

Table 2-1. - Initial Screen Layout (Sheet 6 of 8)

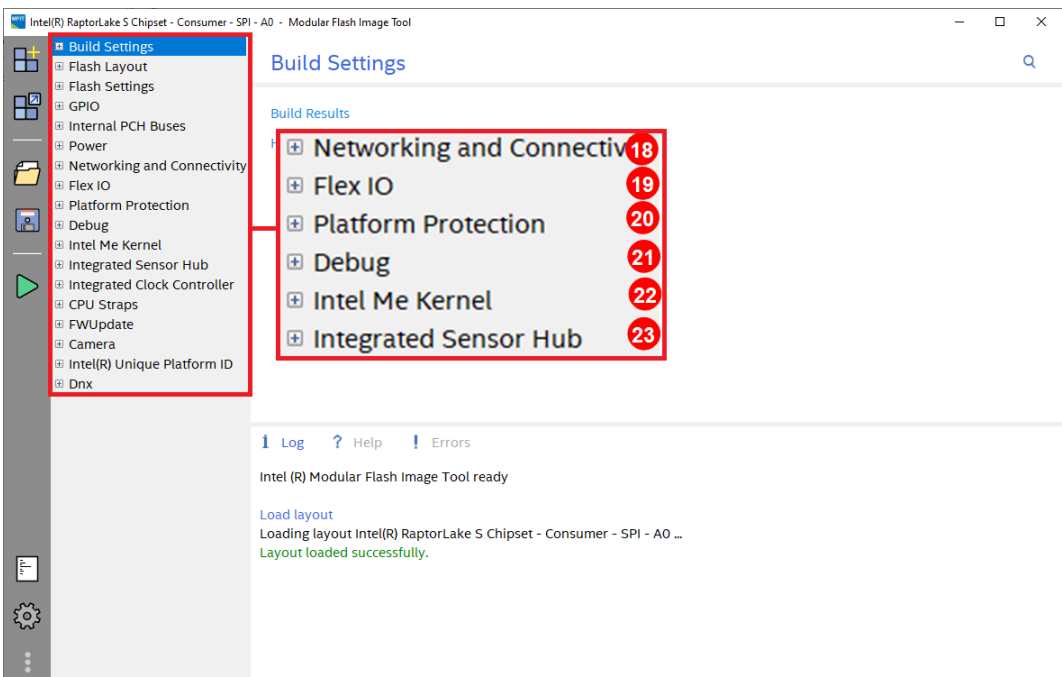
		
#	Label	Contents
18	Networking & Connectivity Tab	Networking & Connectivity which contains (see Table 2-8): <ul style="list-style-type: none"> Wired LAN Configuration Wireless LAN Configuration Time Sensitive Networking Configuration Networking Configuration
19	Flex I/O Tab	Flex I/O which contains (see Table 2-9): <ul style="list-style-type: none"> USB3 Port Configuration USB2 Port Configuration SATA / PCIe Combo Port Configuration PCIe Port Configuration Power Delivery PD Controller Configuration Type-C Subsystem Configuration SPHY Configuration PCH HSIO Tuning
20	Platform Protection Tab	Platform Protection which contains (see Table 2-10): <ul style="list-style-type: none"> TPM Over SPI Bus Configuration BIOS Guard Configuration Descriptor Configuration Exclusion Ranges Hash Key Configuration Bootguard / ISH Crypto Hardware Support Trusted Device Setup Intel® PTT Configuration Content Protection Boot Guard Configuration TXT Configuration

Table 2-1. - Initial Screen Layout (Sheet 7 of 8)

21	Debug Tab	Debug which contains (see Table 2-11): <ul style="list-style-type: none"> ● eSPI Feature Overrides ● Intel® ME Firmware Debugging Overrides ● Direct Connection Interface Configuration ● Intel® Trace Hub Technology ● Early USB DBC over Type-A Configuration ● IDLM ● Delayed Authentication Mode Configuration
22	Intel® ME Kernel Tab	Intel® ME Kernel which contains (see Table 2-12): <ul style="list-style-type: none"> ● Reserved ● Processor ● Intel® ME Firmware Update ● Image Identification ● Intel® ME Measured Boot Configuration ● MCTP Configuration ● Firmware Diagnostics ● End of Manufacturing Configuration ● Intel® ME Boot Configuration
23	Integrated Sensor Hub Tab	Integrated Sensor Hub which contains (see Table 2-13): <ul style="list-style-type: none"> ● Integrated Sensor Hub ● ISH Image ● ISH Data
24	Integrated Clock Controller	Integrated Clock Controller which contains (see Table 2-14): <ul style="list-style-type: none"> ● Integrated Clock Controller Policies

Table 2-1. - Initial Screen Layout (Sheet 8 of 8)

#	Label	Contents
25	CPU Straps Tab	CPU Straps which contain a detailed list of parameters (see Table 2-15) <ul style="list-style-type: none"> CPU Straps
26	FWUpdate	FWUpdate which contains (see Table 2-16): <ul style="list-style-type: none"> FW Update Image Build
27	Camera	Camera which contains (see Table 2-19): <ul style="list-style-type: none"> IPU Security Configuration
28	Intel® Unique Platform ID	Intel® Unique Platform ID contains (see Table 2-20): <ul style="list-style-type: none"> Entitlement Configuration Intel® Unique Platform ID Configuration
29	DnX	DnX which contains (see Table 2-21): <ul style="list-style-type: none"> DnX Fuses

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

Select Build Settings option on the left side menu then click Build Results on the right to expand:


Build Results 1 			
	Intel(R) Manifest Extension Utility Path	<input type="text"/>	...
	Open SSL Signing Tool Path	<input type="text"/>	...
	Signing Enabled	Disabled	▼
	Descriptor Debug Signing Key	<input type="text"/>	...
	Sku	No Emulation	▼
	Factory Defaults Restoration Status	Disabled	▼
	Region Order	53241	
	Output Path	\$DestDir\$image.bin	...
	Output Config XML Path	\$DestDir\$Untitled.xml	...
	Number of Flash Components	1	
	Flash Components Sizes	32	
	Flash Components Sizes Unit	MB	▼
	Total Image Size	32	
	Redundancy Enabled	false	▼
	Ifwi Image Version	0x0	
#	Parameter	Platform	Settings
1	Build Results		
	Intel® Manifest Extension Utility Path (Intel® MEU) This setting configures the path location for the Intel® Manifest Extension Utility.	RPL-S	Path to Intel® MEU
	Open SSL Signing Tool Path This setting configures the path location for the Open SSL signing tool.	RPL-S	Path to Open SSL Signing tool
	Signing Enabled Values: Disabled / Enabled This drop down selection allow the user enables / disables image signing checks. Note: The recommended configuration for this setting is Enabled.	RPL-S	Enabled

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

	Descriptor Debug Signing Key This is the path to the private debug key used to sign the Descriptor, while public key hash of it is included in the OEM hash manifest. Note: This setting is operative only when Flash Descriptor Verification is enabled (See Descriptor Configuration).		DescDbg Binary (Optional)
	Sku Values: No Emulation / Q770 / W780 / Z790 / H770 / B760 This drop down allows selection of platform SKU to selected. Note: This setting should be configured to the target platform SKU for the customer design.	RPL-S	OEM Determined
	Factory Defaults Restoration Status Values: Disabled / Enabled Enable data restore support to manufacturing defaults.	RPL-S	OEM Determined
	Region Order This setting determines the order of the various regions for the IFWI image (i.e. Descriptor, BIOS, Intel® CSME, GbE etc.). Note: The default order for the regions is 5324.	RPL-S	53241
	Output Path This setting configures the output path for the image being generated by MFIT.	RPL-S	OEM Designated path
	Output Config XML Path This setting configures the output path for the MFIT configuration XML file.	RPL-S	OEM Designated path
	Number of Flash Components Values: 1 / 2 Number of output binaries. In case of multiple binaries, their names will be exactly as the name of the first binary with a suffix number, for example: image.bin (1st binary) ,image1.bin, image2.bin etc.	RPL-S	1
	Flash Component Sizes Values: Decimal Input Size of each output binary, the values should be separated by ',' (comma). For example if Number of Flash Components is 2 then a possible value would be '32,8'. Use NA to build without size restriction and set NumberOfFlashComponents to 1.	RPL-S	32
	Flash Components Sizes Unit Values: Bytes, KB, MB, GB This setting configures the unit size of the flash component(s) being used.	RPL-S	MB
	Total Image Size Total sum of all flash components sizes (this setting will not appear in the configuration XML file).	RPL-S	Sum of SPI sizes
	Default Data Partition Enabled Values: false / true This setting enables Intel® CSE Default Data partition.	RPL-S	false
	Redundancy Enabled Values: false / true This setting enables redundancy support for critical firmware layout components.	RPL-S	false
	IFWI Build Version Values: Hex This setting allow the OEM to configure a 32-bit value to use as the IFWI build version number.	Yes	0x0
Select Build Settings option on the left side menu then click Harness Global Data on the right to expand:			

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

<div> <div>Harness Global Data</div> <div>2</div> <div></div> </div>			
	Harness Project	RPP-S PCH A0 (w/RPL-S A0 CPU) RDL v1.0.1.8	
	Harness Label	v0.37 RPP-S w/RPL-S (Harness #25)	
	Harness Revision	#25	
	Selected RVP	<div> <div></div> <div>RPL-S DDR5 UDIMM (RPP-S + RPL-S)</div> <div></div> </div>	
#	Parameter	Platform	Settings
2	Harness Global Data		
	Harness Project This setting displays the platform designation for the Harness project.	RPL-S	Platform Project designation
	Harness Label This setting displays the Harness version label that the Intel® mFIT tool is based on.	RPL-S	Version label
	Harness Revision This setting displays the Harness revision number that the Intel® mFIT tool is based on.	RPL-S	Revision number
	Selected RVP Values: Simics, RPL-S DDR4 UDIMM (RPP-S + RPL-S), RPL-S DDR5 UDIMM (RPP-S + RPL-S), RPL-S DDR5 UDIMM (RPP-S + RPL-S), RPL-S DDR5 UDIMM (RPP-S + RPL-S) S19 This setting allows the user to select the appropriate RVP the image that will be created by the Intel® mFIT tool. Note: This selection will depend on which RVP is being used.	RPL-S	RVP (User Selected)

Table 2-3. - Flash Layout (Sheet 1 of 5)

Select Flash Layout option on the left side menu then click EC Region on the right to expand:

EC Region
1
?

EC Region Pointer File

EC Binary File

EC Region Enable

EC Length

...

...

▼

0x0

#	Parameter	Platform	Settings
1	EC Region - Click to expand		
	EC Region Pointer File This loads a binary file containing the 16 byte Embedded Controller pointer value at the start of the flash descriptor Note: The EC Region Pointer File is needed for some eSPI Embedded Controllers. Check with your specific EC manufacturer to determine the EC pointer has to be populated.	RPL-S	EC Pointer Binary
	EC Binary File Navigate to path to load EC bin file. This loads the Embedded Controller binary used for eSPI that will be merged into the output image generated by the Intel® FIT tool.	RPL-S	EC Binary
	EC Region Enable Values: Enabled/Disabled This option allows the user to enable or disable the Embedded Controller data region.	RPL-S	Enabled
	EC Region - Length This value will be automatically populated by Intel® FIT during image build.		

Select Flash Layout option on the left side menu then click Descriptor Region on the right to expand:

Descriptor Region
2
?

OEM Section Binary

...

#	Parameter	Platform	Settings
2	Descriptor Region - Click to expand		
	OEM Section Binary This loads the OEM Section binary that will be merged into the output image generated by the MFIT tool.	RPP-S	OEM Binary (optional)

Click on GbE Region Flash Layout under the Flash Layout option on the left side menu on the right to expand:

Table 2-3. - Flash Layout (Sheet 2 of 5)

<div> <div>GbE Region</div> <div>3</div> <div></div> </div>			
<div> <div>GbE Binary File</div> <div>...</div> <div>GbE Region Enable</div> <div>Disabled</div> <div>GbE Length</div> <div>0x0</div> <div>Image Id</div> <div>0x0</div> <div>Major Version</div> <div>0x0</div> <div>Minor Version</div> <div>0x0</div> </div>			
#	Parameter	Platform	Settings
3	GbE Region - Click to expand This loads the Intel® Integrated LAN binary that will be merged into the output image generated by the Intel® FIT tool.		
	GbE Binary File Navigate to your Source Directory (as specified in Table 2-2) and switch to the GbE subdirectory. Choose the appropriate Intel GbE LAN Firmware binary image. If not using Intel LAN then load the GbE image before disabling the region along with changing additional settings below. This loads the Intel® integrated LAN binary that will be merged into the output image generated by the Intel® FIT tool. Note: If loading gbeimage.bin file, check that the GbE region is enabled in tool before building image.	RPL-S	gbeimage.bin
	GbE Region Enable Values: Enabled/Disabled This option allows the user to enable or disable the Gigabit Ethernet Region. Note: If choosing a configuration that does not include the GbE LAN the following settings need to be adjusted: LAN Power Well: Core Well Intel® Integrated Wired LAN Enabled: No GbE PCIe Port Select: None GbE MAC SMBus Address: No Intel® PHY over PCIe Enabled: No LAN PHY Power Control GDP11 Signal Configuration: Enable as GDP11	RPL-S	Enabled
	GbE Region - Length This value will be automatically populated by Intel® FIT during image build.		
	Image Id This displays the Image ID of the currently loaded Intel® Integrated LAN binary.		
	Major Version This displays the Major revision number of the currently loaded Intel® Integrated LAN binary.		
	Minor Version This displays the Minor revision number of the currently loaded Intel® Integrated LAN binary.		
Select Flash Layout option on the left side menu then click Ifiw: Intel® ME and PMC Region on the right to expand:			

Table 2-3. - Flash Layout (Sheet 3 of 5)

Ifwi: Intel(R) Me and Pmc Region

4

Q

Intel(R) ME Binary File

Major Version

Minor Version

Hotfix Version

Build Version

PMC Binary File

PMC Version

Chipset Initialization Binary

Chipset Initialization Version

...

...

...

#	Parameter	Platform	Settings
<div style="background-color: red; color: white; border-radius: 50%; width: 20px; height: 20px; display: flex; align-items: center; justify-content: center; font-weight: bold;">4</div>	Ifwi: Intel® ME and PMC Region - Click on the right to expand		
	Intel® ME Binary File Navigate to your Source Directory (as specified in Table 2-2) and switch to the Intel® CSME subdirectory. Choose the appropriate Intel® CSME Firmware binary image. This loads the Intel® CSME binary that will be merged into the into the output image generated by the MFIT tool.	RPL-S	meimage.bin
	Major Version This displays Major revision number of the currently loaded Intel® CSME binary.		
	Minor Version This displays Minor revision number of the currently loaded Intel® CSME binary.		
	Hotfix Version This displays Hot-Fix revision number of the currently loaded Intel® CSME binary.		
	Build Version This displays Build version number of the currently loaded Intel® CSME binary.		
	PMC Binary File This loads the PMC binary that will be merged into the output image generated by the Intel® FIT tool.	RPL-S	PMC.bin
	Version This displays the version of PMC		
	Chipset Initialization Binary This loads the Chipset Initialization binary that will be merged into the output image generated by the MFIT.	RPL-S	Chipset.bin
	Chipset Initialization Version This displays the current Chipset Initialization version contained in the currently in the Intel® CSME binary.		

Select Flash Layout option > Sub Partition on the left side menu then click PCH Configuration Sub-Partition on the right to expand:

Table 2-3. - Flash Layout (Sheet 4 of 5)

PCH Configuration Sub-Partition 5

PCH Configuration File

...

PCH Configuration Version

#	Parameter	Platform	Settings
5	PCH Configuration Sub-Partition - Click to expand This loads the PCH Configuration binary that will be merged in the output image generated by the Intel® FIT tool.		
	PCH Configuration File Navigate to path to load PCHC.bin file. This loads the PCH Configuration binary.	RPL-S	PCHC.bin
	Version - This displays the version of PCH Configuration binary		

Select Flash Layout option > Sub Partition on the left side menu then click on IUnit Sub-Partition on the right to expand:

IUnit Sub-Partition 6

IUnit Binary File

...

IUnit Version

#	Parameter	Platform	Settings
6	IUNIT Sub-Partition - Click to expand		
	IUNIT Sub-Partition Binary This loads the IUnit Sub Partition binary that will be merged into the output image generated by the Intel® MFIT tool.	RPL-S	Iunit.bin (Optional)
	Version - This displays the version of IUnit Binary		

Select Flash Layout option > Sub Partition on the left side menu then click on GBST Configuration Sub-Partition on the right to expand:

GBST Configuration Sub-Partition 7

GBST Configuration File

...

GBST Version

#	Parameter	Platform	Settings
7	GBST Configuration Sub-Partition This loads the GBST Configuration binary that will be merged in the output image generated by the Intel® FIT tool. Note: The GBST sub-partition is used to enabling FuSa safety standards and is not applicable for client platforms.		

Table 2-3. - Flash Layout (Sheet 5 of 5)

	GBST Configuration File Navigate to path to load GBST.bin file. This loads the GBST Configuration binary.	RPL-S	GBST.bin (Optional)
	Version - This displays the version of IUnit Binary		
Select Flash Layout option on the left side menu then click PDR under the Flash Layout on the right to expand:			
<div> <div>PDR Region</div> <div>8</div> <div>Q</div> <div> <div>PDR Binary File</div> <div></div> <div>...</div> </div> <div> <div>PDR Region Enable</div> <div>Disabled</div> <div>▼</div> </div> <div> <div>PDR Length</div> <div>0x0</div> </div> </div>			
#	Parameter	Platform	Settings
8	PDR Region This loads the Platform Data region binary that will be merged into the output image generated by the Intel® FIT tool.		
	PDR Binary File Navigate to path to load pdrimage.bin file if required and available.	RPP-S	PDR.bin (Optional)
	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.	RPP-S	Disabled
	PDR Region - Length Region is disabled by default. Displays Region size information when Binary input file is specified.		
Select Flash Layout option on the left side menu then click BIOS on the right to expand:			
<div> <div>BIOS Region</div> <div>9</div> <div>Q</div> <div> <div>BIOS Binary File</div> <div></div> <div>...</div> </div> <div> <div>BIOS Length</div> <div>0x0</div> </div> </div>			
#	Parameter	Platform	Settings
9	BIOS Region		
	BIOS Region - Length This displays the length of the BIOS binary. Note: This value will be automatically populated by Intel® FIT during image build.		
	BIOS Binary File Navigate to path to load bios.rom file. This loads the BIOS binary that will be merged into the output image generated by the Intel® FIT tool.	RPP-S	biosimage.bin biosimage.bin

Table 2-4. - Flash Settings (Sheet 1 of 10)

Select Flash Settings option on the left side menu then click Flash Settings on the right to expand:			
<div>Flash Configuration 1 Q</div> <div> <div>Dual I/O Read Enable</div> <div>No</div> </div> <div> <div>Dual Output Read Enable</div> <div>No</div> </div> <div> <div>Quad Output Read Enable</div> <div>No</div> </div> <div> <div>Quad I/O Read Enable</div> <div>No</div> </div> <div> <div>Fast Read Supported</div> <div>Yes</div> </div> <div> <div>Fast Read Clock Frequency</div> <div>50MHz</div> </div> <div> <div>Write and Erase Clock Frequency</div> <div>50MHz</div> </div> <div> <div>Read ID and Read Status Clock Frequency</div> <div>50MHz</div> </div> <div> <div>Invalid Instruction 0</div> <div>0x21</div> </div> <div> <div>Invalid Instruction 1</div> <div>0x42</div> </div> <div> <div>Invalid Instruction 2</div> <div>0x60</div> </div> <div> <div>Invalid Instruction 3</div> <div>0xAD</div> </div> <div> <div>Invalid Instruction 4</div> <div>0xB7</div> </div> <div> <div>Invalid Instruction 5</div> <div>0xB9</div> </div> <div> <div>Invalid Instruction 6</div> <div>0xC4</div> </div> <div> <div>Invalid Instruction 7</div> <div>0xC7</div> </div>			
#	Parameter	Platform	Settings
1	Flash Configuration		
	Dual I/O Read Enabled Values: Yes/No - This setting allows the customer to enable support for Dual I/O Read capabilities for flash components. See Raptor Lake S SPI Programming guide for further details.	RPP-S	Yes
	Dual Output Read Enabled Values: Yes/No - This setting allows the customer to enable support for Dual Output Read capabilities for flash components. See Raptor Lake S SPI Programming guide for further details.	RPP-S	Yes
	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 Raptor Lake S SPI Programming guide for further details.	RPP-S	Yes
#	Parameter	Platform	Settings

Table 2-4. - Flash Settings (Sheet 2 of 10)

	Quad Output Read Enabled Values: Yes/No - This setting allows the customer to enable support for Quad Output Read capabilities for flash components. See Raptor Lake S SPI Programming guide for further details.	RPP-S	Yes
	Fast Read Supported Values: Yes/No - This setting allows the customer to enable support for Fast Read capabilities for flash components. See Raptor Lake S 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.	RPP-S	Yes
	Fast Read Clock Frequency Values: 14MHz, 25MHz, 33MHz, 50MHz, 100MHz - This setting allows the customer to configure the flash component clock frequency setting for Fast Read. See Raptor Lake S SPI Programming guide for further details. Note: The 100MHz frequency setting not valid on client platforms	RPP-S	50MHz
	Read ID and Read Status clock frequency Values: 14MHz, 25MHz, 33MHz, 50MHz, 100MHz - This setting allows the customer to configure the flash component clock frequency setting for Read ID and Read Status clock. See Raptor Lake S SPI Programming guide for further details. Note: The 100MHz frequency setting not valid on client platforms	RPP-S	50MHz
	Write and Erase clock frequency Values: 14MHz, 25MHz, 33MHz, 50MHz, 100MHz - This setting allows the customer to configure the flash component clock frequency setting for Write and Erase. See Raptor Lake S SPI Programming guide for further details. Note: The 100MHz frequency setting not valid on client platforms	RPP-S	50MHz
	Invalid Instruction 0 - This setting allows the customer to configure invalid instruction to protect against Chip Erase. See Raptor Lake S SPI Programming guide for further details. Note: This setting should be set to '0' if there are not Invalid instructions.	RPP-S	0x00000021
	Invalid Instruction 1 - This setting allows the customer to configure invalid instruction to protect against Chip Erase. See Raptor Lake S SPI Programming guide for further details. Note: This setting should be set to '0' if there are not Invalid instructions.	RPP-S	0x00000042
	Invalid Instruction 2 - This setting allows the customer to configure invalid instruction to protect against Chip Erase. See Raptor Lake S SPI Programming guide for further details. Note: This setting should be set to '0' if there are not Invalid instructions.	RPP-S	0x00000060
	Invalid Instruction 3 - This setting allows the customer to configure invalid instruction to protect against Chip Erase. See Raptor Lake S SPI Programming guide for further details. Note: This setting should be set to '0' if there are not Invalid instructions.	RPP-S	0x000000AD
	Invalid Instruction 4 - This setting allows the customer to configure invalid instruction to protect against Chip Erase. See Raptor Lake S SPI Programming guide for further details. Note: This setting should be set to '0' if there are not Invalid instructions.	RPP-S	0x000000B7
	Invalid Instruction 5 - This setting allows the customer to configure invalid instruction to protect against Chip Erase. See Raptor Lake S SPI Programming guide for further details. Note: This setting should be set to '0' if there are not Invalid instructions.	RPP-S	0x000000B9
	Invalid Instruction 6 - This setting allows the customer to configure invalid instruction to protect against Chip Erase. See Raptor Lake S SPI Programming guide for further details. Note: This setting should be set to '0' if there are not Invalid instructions.	RPP-S	0x000000C4
	Invalid Instruction 7 - This setting allows the customer to configure invalid instruction to protect against Chip Erase. See Raptor Lake S SPI Programming guide for further details. Note: This setting should be set to '0' if there are not Invalid instructions.	RPP-S	0x000000C7
Select Flash Settings option on the left side menu then click Host CPU / BIOS Master Access on the right to expand:			

Table 2-4. - Flash Settings (Sheet 3 of 10)

Host CPU / BIOS Master Access 2 Q			
Host CPU / BIOS Write Access Intel Recommended		0xFFFF	
Host CPU / BIOS Write Access Custom		0x0	
Host CPU / BIOS Read Access Intel Recommended		0xFFFF	
Host CPU / BIOS Read Access Custom		0x0	
#	Parameter	Platform	Settings
2	Host CPU / BIOS Master Access Note: Host CPU / BIOS Master Access options will be greyed out and not configurable unless the EOM on First Boot Enabled setting is set to "Yes".		
	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 Note: For further details on Region Access Control see Raptor Lake S SPI Programming guide further details.	RPP-S	0xFFFF
	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	RPP-S	Hex Input
	Host CPU / BIOS Read Access Values: 0xFFFF, 0x00F, 0x01F, 0x10F, 0x11F This setting determines read access control for the BIOS region. 0xFFFF = Debug/Manufacturing 0x00F = Production 0x01F = Production with access to PDR (should ONLY be used if PDR region is implemented). 0x10F = Production with access to EC 0x11F = Production with access to EC and PDR Custom = User custom Host / BIOS Read Access values For further details on Region Access Control see Raptor Lake S SPI Programming guide.	RPP-S	0xFFFF 0xFFFF

Table 2-4. - Flash Settings (Sheet 4 of 10)

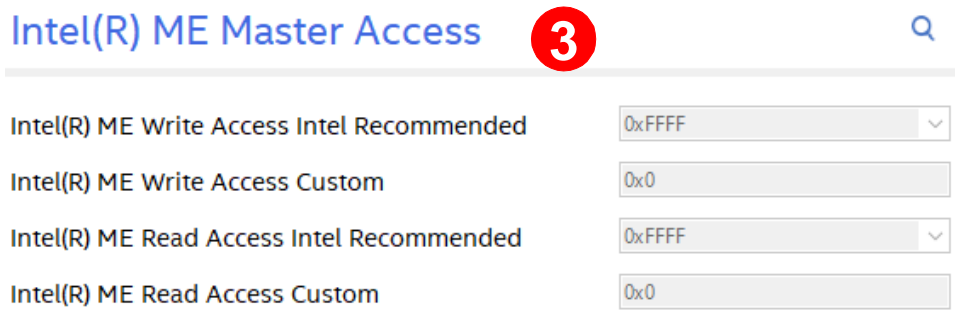
	Host CPU / BIOS Read Access Custom This setting allows free form user customized Host CPU / BIOS Read Access regions permissions Note: This setting is grayed out unless Custom is selected under the Host CPU / BIOS Read Access Intel Recommended drop down menu. Warning: Setting region access permission values outside of Intel recommendation could result in compromised platform security	RPP-S	Hex Input
Select Flash Settings option on the left side menu then click Intel® ME Master on the right to expand:			
			
#	Parameter	Platform	Settings
3	Intel® ME Master Access Note: Intel® ME Master Access options will be greyed out and not configurable unless the EOM on First Boot Enabled setting is set to "Yes".		
	Intel® ME Write Access Intel Recommended Values: 0xFFFF, 0x0004 This setting determines write access control for the Intel® CSME Region. 0xFFFF = Debug/Manufacturing 0x0004 = Production Custom = User custom Intel® ME Write Access values For further details on Region Access Control see Raptor Lake S SPI Programming guide further details.	RPP-S	0xFFFF 0xFFFF
	Intel® ME Write Access Custom This setting allows free form user customized Intel® ME Write Access regions permissions Note: This setting is grayed out unless Custom is selected under the Intel® CSME Write Access Intel Recommended drop down menu. Warning: Setting region access permission values outside of Intel recommendation could result in compromised platform security	RPP-S	Hex Input
	Intel® ME Read Access Intel Recommended Values: 0xFFFF, 0x000D This setting determines read access control for the Intel® CSME Region. 0xFFFF = Debug/Manufacturing 0x000D = Production Custom = User custom Intel® CSME Read Access values For further details on Region Access Control see Raptor Lake S SPI Programming guide further details.	RPP-S	0xFFFF 0xFFFF

Table 2-4. - Flash Settings (Sheet 5 of 10)

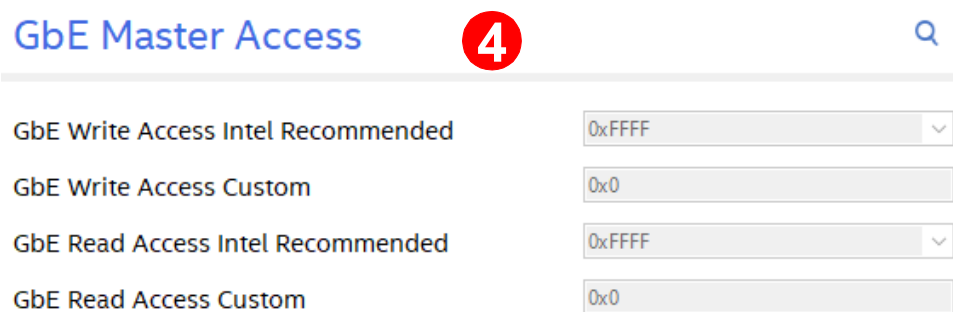
	Intel® ME Read Access Custom This setting allows free form user customized Intel® ME Read Access regions permissions Note: This setting is grayed out unless Custom is selected under the Intel® CSME Read Access Intel Recommended drop down menu. Warning: Setting region access permission values outside of Intel recommendation could result in compromised platform security	RPP-S	Hex Input
Select Flash Settings option on the left side menu then click GbE Master Access on the right to expand:			
			
#	Parameter	Platform	Settings
4	GbE Master Access Note: GbE Master Access options will be greyed out and not configurable unless the EOM on First Boot Enabled setting is set to "Yes".		
	GbE Write Access Intel Recommended Values: 0xFFFF, 0x0008 This setting determines write access control for the Gigabit Ethernet Region. 0xFFFF = Debug/Manufacturing 0x0008 = Production Custom = User custom GbE Write Access values Note: For further details on Region Access Control see Raptor Lake S SPI Programming guide further details.	RPP-S	0xFFFF 0xFFFF
	GbE Write Access Custom This setting allows free form user customized GbE Write Access regions permissions Note: This setting is grayed out unless Custom is selected under the GbE Write Access Intel Recommended drop down menu. Warning: Setting region access permission values outside of Intel recommendation could result in compromised platform security	RPP-S	Hex Input
	GbE Read Access Intel Recommended Values: 0xFFFF, 0x0009 This setting determines read access control for the Gigabit Ethernet Region. 0xFFFF = Debug/Manufacturing 0x0009 = Production Custom = User custom GbE Read Access values Note: For further details on Region Access Control see Raptor Lake S SPI Programming guide further details.	RPP-S	0xFFFF 0xFFFF

Table 2-4. - Flash Settings (Sheet 6 of 10)

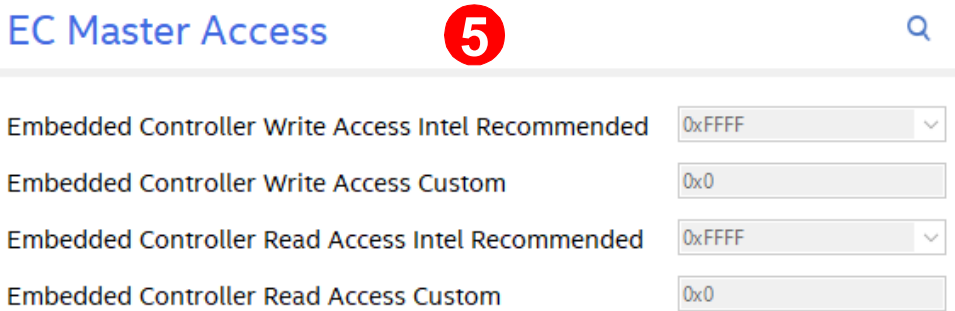
	GbE Read Access Custom This setting allows free form user customized GbE Read Access regions permissions Note: This setting is grayed out unless Custom is selected under the GbE Read Access Intel Recommended drop down menu. Warning: Setting region access permission values outside of Intel recommendation could result in compromised platform security	RPP-S	Hex Input
Select Flash Settings option on the left side menu then click EC Master Access on the right to expand:			
			
#	Parameter	Platform	Settings
5	EC Master Access Note: EC Master Access options will be greyed out and not configurable unless the EOM on First Boot Enabled setting is set to "Yes".		
	EC Write Access Intel Recommended Values: 0xFFFF, 0x0100 This setting determines write access control for the Embedded Controller Region. 0xFFFF = Debug/Manufacturing 0x0100 = Production Custom = User custom EC Write Access values Note: For further details on Region Access Control see Raptor Lake S SPI Programming guide further details.	RPP-S	0xFFFF
	EC Write Access Custom This setting allows free form user customized EC Write Access regions permissions Note: This setting is grayed out unless Custom is selected under the EC Write Access Intel Recommended drop down menu. Warning: Setting region access permission values outside of Intel recommendation could result in compromised platform security	RPP-S	Hex Input
	EC Read Access Intel Recommended Values: 0xFFFF, 0x0101, 0x0103 This setting determines read access control for the Embedded Controller Region. 0xFFFF = Debug/Manufacturing 0x0101 = Production 0x0103 = Production with EC BIOS Read Access Custom = User custom EC Read Access values Note: For further details on Region Access Control see Raptor Lake S SPI Programming guide further details.	RPP-S	0xFFFF

Table 2-4. - Flash Settings (Sheet 7 of 10)

	EC Read Access Custom This setting allows free form user customized EC Read Access regions permissions Note: This setting is grayed out unless Custom is selected under the EC Read Access Intel Recommended drop down menu. Warning: Setting region access permission values outside of Intel recommendation could result in compromised platform security	RPP-S	Hex Input
Select Flash Settings option on the left side menu then click BIOS Configuration on the right to expand:			
<div> <div>BIOS Configuration</div> <div>6</div> <div> <div>Top Swap Block Size</div> <div>4MB</div> </div> <div> <div>BIOS Redundancy Assistance</div> <div>Disabled</div> </div> </div>			
#	Parameter	Platform	
6	BIOS Configuration		
	BIOS Redundancy Assistance Values: Enabled, Disabled In cases of BIOS boot failure, Intel®CSME will configure the platform to boot with backup BIOS using Top Swap when this setting is enabled. Note: This option is only applicable when Boot Guard is enabled.	RPP-S	Disabled
	Top Swap Block Size Values: 64KB, 128KB, 256KB, 512KB, 1MB This configures the Top Swap Block size for the platform. For further details see Alder Point S Platform Controller Hub EDS.	RPP-S	4MB
Select Flash Settings option on the left side menu then click Flash Components on the right to expand:			
<div> <div>Flash Components</div> <div>7</div> <div> <div>SPI Resume Hold-off Delay</div> <div>4us</div> </div> <div> <div>SPI Suspend / Resume Enabled</div> <div>No</div> </div> <div> <div>SPI Out of Order operation Enabled</div> <div>Yes</div> </div> <div> <div>SPI Max write / erase Resume to Suspend intervals</div> <div>No Ceiling</div> </div> <div> <div>SPI Idle to Deep Power Down Timeout</div> <div>0x5</div> </div> <div> <div>SPI Global Protected Range</div> <div>0x0</div> </div> <div> <div>Software Re-Binding Enabled</div> <div>No</div> </div> </div>			
#	Parameter	Platform	Settings
7	Flash Components		

Table 2-4. - Flash Settings (Sheet 8 of 10)

#	Parameter	Platform	Settings
	SPI Resume Hold-off Delay Values: 0us, 2us, 4us, 6us, 8us, 10us, 12us, 14us 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.	RPP-S	4us
	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.	RPP-S	Yes
	SPI Out of Order operation Enabled Values: Yes/No 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.	RPP-S	Yes
	SPI Max write / erase Resume to Suspend intervals Values: 128us, 256us, 512us, No Ceiling This setting specifies the maximum value for the write and erase Resume to Suspend intervals.	RPP-S	No Ceiling
	SPI Idle to Deep Power Down Timeout Values: Hex - 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.	RPP-S	0x5
	SPI Global Protected Range Values: Hex This sets the default value of the Global Protected Range register in the SPI Flash Controller.	RPP-S	0x0
	Software Re-Binding Enabled Values: Yes / No When enabled this settings will allow for SPI re-binding to a new PCH during manufacturing and re-manufacturing flows prior to platform EOM. Note: Re-binding to a replacement PCH can only be done a maximum of 5 times before the SPI part needs to be re-flashed.	RPP-S	No
Select Flash Settings option on the left side menu then click VSCC Entry on the right to expand:			
<div> <div>VSCC Entry</div> <div>8</div> <div> <div>Active</div> <div>true</div> </div> <div> <div>Part Name</div> <div>W25Q256</div> </div> <div> <div>Vendor ID</div> <div>0xEF</div> </div> <div> <div>Device ID 0</div> <div>0x40</div> </div> <div> <div>Device ID 1</div> <div>0x19</div> </div> </div>			
#	Parameter	Platform	Settings
8	VSCC Entry The table can hold up to 32 separate unique VSCC entries by default MFIT only has one VSCC entry enabled.		
	Active Values: True / False This setting enables / disables the specific VSCC entry. If set to disabled values contained in the entry will not be populated into the VSCC table contained in the flash descriptor.	RPP-S	True

Table 2-4. - Flash Settings (Sheet 9 of 10)

	Part Name Values: OEM Populated 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.	RPP-S	W25Q256
	Vendor ID Values: Hex Value This configures the JEDEC vendor specific byte ID of the SPI flash component. Note: See Raptor Lake S SPI Programming guide for further details.	RPP-S	0xEF
	Device ID 0 Values: Hex Value This configures the JEDEC device specific byte ID 0 of the SPI flash component. Note: See Raptor Lake S SPI Programming guide for further details.	RPP-S	0x40
	Device ID 1 Values: Hex Value This configures the JEDEC device specific byte ID 1 of the SPI flash component. Note: See Raptor Lake S SPI Programming guide for further details.	RPP-S	0x19
	+ Add VSCC Entry		
Select Flash Settings option on the left side menu then click FPF Configuration on the right to expand:			
<div> <div>FPF Configuration</div> <div>9</div> <div>Hardware Binding Enabled</div> <div>Disabled</div> </div>			
9	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. Note: For Revenue parts this setting will be ignored and FPF Hardware binding will take place when close manufacturing flow is executed.	RPP-S	Disabled
Select Flash Settings option on the left side menu then click RPMC Configuration on the right to expand:			
<div> <div>RPMC Configuration</div> <div>10</div> <div>RPMC Supported</div> <div>Yes</div> <div>RPMC Rebinding Enabled</div> <div>Yes</div> </div>			
10	RPMC Configuration		

Table 2-4. - Flash Settings (Sheet 10 of 10)

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

Table 2-5. - GPIO (Sheet 1 of 2)

Select GPIO option on the left side menu then click GPIO VCCIO Voltage Control on the right to expand:

GPIO VCCIO Voltage Control

1

GPP_D Group Master Voltage Select

3.3Volts

GPP_E Group Master Voltage Select

3.3Volts

GPP_K Group Master Voltage Select

3.3Volts

GPP_F Group Master Voltage Select

3.3Volts

GPP_C Group Master Voltage Select

3.3Volts

GPP_B Group Master Voltage Select

3.3Volts

GPP_G Group Master Voltage Select

3.3Volts

GPP_H Group Master Voltage Select

3.3Volts

Clockout 48 Mode Configuration

CLKOUT_48

GPP_I Group Master Voltage Select

1.8Volts

Intel(R) HD Audio Voltage Select

1.8Volts

GPP_J Group Master Voltage Select

1.8Volts

#	Parameter	Platform	Settings
1	GPIO VCCIO Voltage Control		
	GPP_D Group Master Voltage Select Values: 3.3Volts/1.8Volts This setting controls configures the VCCIO voltage all of the GPP_D GPIO pins.	RPP-S	3.3Volts
	GPP_E Group Master Voltage Select Values: 3.3Volts/1.8Volts This setting controls configures the VCCIO voltage all of the GPP_E GPIO pins.	RPP-S	3.3Volts
	GPP_K Group Master Voltage Select Values: 3.3Volts/1.8Volts This setting controls configures the VCCIO voltage all of the GPP_K GPIO pins.	RPP-S	3.3Volts
	GPP_F Group Master Voltage Select Values: 3.3Volts/1.8Volts This setting controls configures the VCCIO voltage all of the GPP_F GPIO pins.	RPP-S	3.3Volts
	GPP_C Group Master Voltage Select Values: 3.3Volts/1.8Volts This setting controls configures the VCCIO voltage all of the GPP_C GPIO pins.	RPP-S	3.3Volts
	GPP_B Group Master Voltage Select Values: 3.3Volts/1.8Volts This setting controls configures the VCCIO voltage all of the GPP_B GPIO pins.	RPP-S	3.3Volts

Table 2-5. - GPIO (Sheet 2 of 2)

	GPP_G Group Master Voltage Select Values: 3.3Volts/1.8Volts This setting controls configures the VCCIO voltage all of the GPP_G GPIO pins.	RPP-S	3.3Volts
	GPP_H Group Master Voltage Select Values: 3.3Volts/1.8Volts This setting controls configures the VCCIO voltage all of the GPP_H GPIO pins.	RPP-S	3.3Volts
	Clockout 48 Mode Configuration Values: CLKOUT_48/GPP_B6 This setting determines the native mode of operation for the CLKOUT_48 signal.	RPP-S	CLKOUT_48
	GPP_I Group Master Voltage Select Values: 3.3Volts/1.8Volts This setting controls configures the VCCIO voltage all of the GPP_I GPIO pins.	RPP-S	1.8Volts
	Intel® HD Audio Voltage Select Values: 3.3Volts/1.8Volts This setting controls configures the VCCIO voltage for all of the Intel® HD Audio GPIO pins.	RPP-S	1.8 Volts
	GPP_J Group Master Voltage Select Values: 3.3Volts/1.8Volts This setting controls configures the VCCIO voltage all of the GPP_J GPIO pins.	RPP-S	1.8Volts
Select Camera Pins option on the left side menu then click Camera privacy GPIO Pin on the right to expand:			
<div> <div>Camera Pins</div> <div>2</div> <div> <div>Camera privacy GPIO Pin</div> <div>None</div> </div> </div>			
#	Parameter	Platform	Settings
2	Camera Pins		
	Camera privacy GPIO Pin Values: GPIO drop down list This setting defines which GPIO is used to provide the current privacy state to the camera device. Note: This setting is only applicable when Camera privacy feature control disabled is set to 'false'.	RPP-S	None
Select Camera Pins option on the left side menu then click ME Feature Pins on the right to expand:			
<div> <div>ME Feature Pins</div> <div>3</div> <div> <div>CPU Detection</div> <div>None</div> </div> </div>			
#	Parameter	Platform	Settings
3	ME Feature Pins		
	CPU Detection Values: GPIO Pool This setting determines the GPIO to be used by Intel® CSME for the Missing Processor Detection Alert feature.	RPP-S	None

Table 2-6. - Internal PCH Buses (Sheet 1 of 7)

Select Internal PCH Buses option on the left side menu then click SMBus / SMLink Configuration on the right to expand:			
<div> <div>SMBus / SMLink Configuration</div> <div>1</div> <div></div> </div> <div> <div>Intel(R) SMBus ASD Mode Configuration</div> <div>Enable as GPP_C2</div> </div> <div> <div>SMBus / SMLink TCO Slave Connection</div> <div>Intel(R) SMBus</div> </div> <div> <div>Intel(R) SMBus I2C Address</div> <div>0x0</div> </div> <div> <div>Intel(R) SMBus ASD Address</div> <div>0x0</div> </div> <div> <div>Intel(R) SMBus I2C Address Enabled</div> <div>No</div> </div> <div> <div>Intel(R) SMBus ASD Address Enabled</div> <div>No</div> </div> <div> <div>Intel(R) SMBus Subsystem Vendor and Device ID for ASF</div> <div>0x0</div> </div> <div> <div>SMLink0 Enabled</div> <div>Yes</div> </div> <div> <div>Intel(R) SMLink0 MCTP Address</div> <div>0x0</div> </div> <div> <div>Intel(R) SMLink0 MCTP Address Enabled</div> <div>No</div> </div> <div> <div>SMLink0 Frequency</div> <div>1 MHz</div> </div> <div> <div>SMLink1 Enabled</div> <div>No</div> </div> <div> <div>SMLink1 GP Target Address Enabled</div> <div>No</div> </div> <div> <div>SMLink1 GP Target Address</div> <div>0x0</div> </div> <div> <div>SMLink1 I2C Target Address</div> <div>0x0</div> </div> <div> <div>SMLink1 I2C Target Address Enabled</div> <div>No</div> </div> <div> <div>SMLink1 Frequency</div> <div>100 KHz</div> </div>			
#	Parameter	Platform	Settings
1	SMBus / SMLink Configuration		
	Intel® SMBus ASD Mode Configuration Values: Enable as GPP_C2/Enable as Intel® SMBus ASD This setting determines the native mode of operation for the Intel® SMBus ASD signal.	RPP-S	Enable as GPP_C2
	SMBus / SMLink TCO Slave Connection Values: Intel® SMBus, SMLink0 This setting configures the TCO Slave connection to ether the Intel® SMBus or SMLink0. Note: For further details see Raptor Lake S Platform Controller Hub EDS.	RPP-S	Intel® SMBus

Table 2-6. - Internal PCH Buses (Sheet 2 of 7)

#	Parameter	Platform	Settings
	Intel® SMBus I2C Address Values: Hex Value This setting configures the Intel® SMBus I2C Address. Note: This setting is only used for testing purposes. The recommended setting is "0000000".	RPP-S	0x00000000
	Intel® SMBus ASD Address Values: Hex Value This setting configures the Intel® SMBus Alert Sending device Address. Note: For details see Raptor Lake S SPI Programming guide for further details.	RPP-S	0x00000000
	Intel® SMBus I2C Address Enabled Values: Yes/No This setting enables / disables the Intel® SMBus I2C Address. Note: This setting is only used for testing purposes. The recommended setting is "No".	RPP-S	No
	Intel® SMBus ASD Address Enabled Values: Yes/No This setting enables / disables the Intel® SMBus Alert Sending device. Note: For details see Raptor Lake S SPI Programming guide for further details.	RPP-S	No
	Intel® SMBus Subsystem Vendor & device ID for ASF Values: Hex Value This setting configures the Intel® SMBus Subsystem Vendor & device ID for ASF. Note: For details see Raptor Lake S SPI Programming guide further details.	RPP-S	0x00000000
	SMLink0 Enabled Values: Yes/No This setting enables / disables SMLink0 interface. Note: For further details see Raptor Lake S Platform Controller Hub EDS.	RPP-S	Yes
	Intel® SMLnk0 MCTP Address Values: Hex Value This setting configures the Intel® SMLink0 MCTP Address. Note: For details see Raptor Lake S SPI Programming guide for further details.	RPP-S	0x00000000
	Intel® SMLink0 MCTP Address Enabled Value: Yes/No This setting configures the Intel® SMLink0b MCTP Address. Note: This setting is only used for testing.	RPP-S	No
	SMLink0 Frequency Values: 100KHz, 400KHz, 1 MHz This setting determines the frequency at which the SMLink0 will operate. Note: The recommended setting is "1MHz".	RPP-S	1 MHz
	SMLink1 Enabled Values: Yes/No This setting enables / disables SMLink1 interface. For further details see Raptor Lake S Platform Controller Hub EDS. Note: This setting must be set to "Yes" if using PCH / MCP Thermal reporting.	RPP-S	Yes
	SMLink1 GP Target Address Values: Hex Value This setting configures SMLink1 GP Target Address. Note: For further details see Raptor Lake S Platform Controller Hub EDS.	RPP-S	0x00000000

Table 2-6. - Internal PCH Buses (Sheet 3 of 7)

#	Parameter	Platform	Settings
	SMLink1 GP Target Address Enabled Values: Yes/No This setting enables / disables SMLink1 GP Target Address interface. For further details see Raptor Lake S Platform Controller Hub EDS. Note: This setting must be set to "Yes" if using PCH / MCP Thermal reporting.	RPP-S	Yes
	SMLink1 I2C Target Address Values: Hex Value This setting configures SMLink1 I2C Target Address. Note: For further details see Raptor Lake S Platform Controller Hub EDS.	RPP-S	0x00000000
	SMLink1 I2C Target Address Enabled Values: Yes/No - This setting configures SMLink1 I2C Target Address. Note: For further details see Raptor Lake S Platform Controller Hub EDS.	RPP-S	No
	SMLink1 Frequency Values: 100KHz, 400KHz, 1 MHz - This setting determines the frequency at which the SMLink1 will operate. Note: The recommended setting is "100KHz".	RPP-S	100 KHz
Select PCH Internal Buses option on the left side menu then click eSPI Configuration on the right to expand:			

Table 2-6. - Internal PCH Buses (Sheet 4 of 7)

eSPI Configuration 2 Q			
eSPI / EC Bus Frequency	20MHz		
eSPI / EC CRC Check Enabled	Yes		
eSPI / EC Maximum I/O Mode	Single		
eSPI / EC Slave 1 Device Enabled	No		
eSPI / EC Slave 1 Device Bus Frequency	50MHz		
eSPI / EC Slave 1 Device Maximum I/O Mode	Single, Dual and Quad		
eSPI / EC Slave 1 Device CRC Check Enable	Yes		
eSPI / EC Slave Attached Flash Multiple Outstanding Requests Enable	Single Outstanding Reque		
eSPI / EC Slave Attached Flash Channel OOO Enable	In-Order SAF Requests		
eSPI / EC Max Outstanding Request for Master Attached Flash Channel	2		
eSPI / EC Slave 2 Device Enabled	No		
eSPI / EC Slave 2 Device CRC Check Enable	No		
eSPI / EC Slave 2 Device Maximum I/O Mode	Single		
eSPI / EC Slave 2 Device Bus Frequency	20MHz		
eSPI / EC Slave 3 Device Enabled	No		
eSPI / EC Slave 3 Device CRC Check Enable	No		
eSPI / EC Slave 3 Device Maximum I/O Mode	Single		
eSPI / EC Slave 3 Device Bus Frequency	20MHz		
#	Parameter	Platform	Settings
2	eSPI Configuration		
	eSPI / EC Bus Frequency Value: 20MHz / 25MHz / 33MHz / 50MHz Indicates the maximum frequency of the eSPI bus that is supported by the eSPI Master and platform configuration (trace length, number of Slaves, etc.). The actual frequency of the eSPI bus will be the minimum of this field and the Slave's maximum frequency advertised in its General Capabilities register.	RPP-S	20MHz
	eSPI / EC CRC Check Enabled Values: Yes / No This setting enables CRC checking on eSPI Slave 0 channel.	RPP-S	Yes

Table 2-6. - Internal PCH Buses (Sheet 5 of 7)

#	Parameter	Platform	Settings
	eSPI / EC Maximum I/O Mode Values: Single / Single and Dual / Single and Quad / Single Dual and Quad Indicates the maximum IO Mode (Single/Dual/Quad) of the eSPI bus that is supported by the eSPI Master and specific platform configuration. The actual IO Mode of the eSPI bus will be the minimum of this field and the Slave's maximum IO Mode advertised in its General Capabilities register.	RPP-S	Single
	eSPI / EC Slave 1 Device Enabled Values: Yes / No This setting enables the Slave device on the eSPI interface.	RPP-S	No
	eSPI / EC Slave 1 Device Bus Frequency Value: 20MHz / 25MHz / 33MHz / 50MHz This setting configures the maximum operating frequency of the Slave device.	RPP-S	50MHz
	eSPI / EC Slave 1 Device Maximum I/O Mode Values: Single / Single and Dual / Single and Quad / Single Dual and Quad This setting configures the maximum I/O mode of the Slave device.	RPP-S	Single, Dual, Quad
	eSPI / EC Slave 1 CRC Check Enable Values: Yes / No This setting determines if CRC checking is enabled on the eSPI / EC Slave 1 Device channel.	RPP-S	Yes
	eSPI / EC Slave Attached Flash Multiple Outstanding Requests Enable Values: Single Outstanding Request/Multiple Outstanding Requests This setting enables multiple outstanding requests for the eSPI / EC Slave Attached Flash device.	RPP-S	Single Outstanding Request
	eSPI / EC Slave Attached Flash Channel OOO Enable Values: In-Order SAF Requests / Out-of-Order SAF Requests This setting enables Out of Order requests on the eSPI / EC Slave Attached Flash device.	RPP-S	In-Order SAF Requests
	eSPI / EC Max Outstanding Request for Master Attached Flash Channel Values: 1 / 2 This setting determines the Maximum outstanding requests on the eSPI / EC Master Attached Flash Channel.	RPP-S	2
	eSPI / EC Slave 2 Device Enabled Values: Yes / No This setting enables the Slave device on the eSPI interface.	RPP-S	No
	eSPI / EC Slave 2 CRC Check Enable Values: Yes / No This setting determines if CRC checking is enabled on the eSPI / EC Slave 2 Device channel.	RPP-S	No
	eSPI / EC Slave 2 Device Maximum I/O Mode Values: Single, Single and Dual, Single and Quad, Single Dual and Quad This setting configures the maximum I/O mode of the Slave device.	RPP-S	Single
	eSPI / EC Slave 2 Device Bus Frequency Value: 20MHz / 25MHz / 33MHz / 50MHz This setting configures the maximum operating frequency of the Slave device.	RPP-S	20MHz
	eSPI / EC Slave 3 Device Enabled Values: Yes / No This setting enables the Slave device on the eSPI interface.	RPP-S	No
	eSPI / EC Slave 3 CRC Check Enable Values: Yes / No This setting determines if CRC checking is enabled on the eSPI / EC Slave 2 Device channel.	RPP-S	No
	eSPI / EC Slave 3 Device Maximum I/O Mode Values: Single / Single and Dual / Single and Quad / Single Dual and Quad This setting configures the maximum I/O mode of the Slave device.	RPP-S	Single

Table 2-6. - Internal PCH Buses (Sheet 6 of 7)

eSPI / EC Slave 3 Device Bus Frequency Value: 20MHz / 25MHz / 33MHz / 50MHz This setting configures the maximum operating frequency of the Slave device.		RPP-S	25MHz
Select PCH Internal Buses option on the left side menu then click DMI /PCIe Configuration on the right to expand:			
<div> <div>DMI / PCIe Configuration</div> <div>3</div> <div>Q</div> </div> <div> <div>DMI Lane Reversal</div> <div>No</div> </div> <div> <div>DMI AC Coupling Select</div> <div>No</div> </div> <div> <div>DMI Lane Width</div> <div>DMI x8</div> </div> <div> <div>DMI / PCIe Port Staggering Enabled</div> <div>Yes</div> </div>			
#	Parameter	Platform	Settings
3	DMI /PCIe Configuration		
	DMI Lane Reversal Values: Yes / No This setting allows the DMI Lane signals to be reversed. Note: For further details see Raptor Lake S Platform Controller Hub EDS.	RPP-S	No
	DMI AC Coupling Values: Yes / No This determines if DMI is operating in AC or DC coupled mode Note: For further details see Raptor Lake S Platform Controller Hub EDS.	RPP-S	No
	DMI Lane Width Values: DMI x4 / DMI x8 This setting determines the number of DMI lanes available Note: For further details see Raptor Lake S Platform Controller Hub EDS.	RPP-S	DMI x8
	DMI Port Staggering Values: Yes / No This setting configures DMI for Port Staggering. Note: For further details see Raptor Lake S Platform Controller Hub EDS.	RPP-S	Yes
Select Internal PCH Buses option on the left side menu then click PCH Timer Configuration on the right to expand:			

Table 2-6. - Internal PCH Buses (Sheet 7 of 7)

PCH Timer Configuration 4 Q			
PCH clock output stable to PROCPWRGD high (tPCH45)		100ms	
PROCPWRGD and SYS_PWROK high to SUS_STAT# de-assertion (tPCH46)		1ms	
Over Clocking Watchdog Self Start Enable		OC WDT Disabled	
APWROK Timing		2ms	
PCIe Power Stable Timer (tPCH33)		Disabled	
#	Parameter	Platform	Settings
4	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 Raptor Lake S Platform Controller Hub EDS.	RPP-S	100ms
	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 Raptor Lake S Platform Controller Hub EDS.	RPP-S	1ms
	Over Clocking Watchdog Self Start Enable Values: OC WDT Disabled / OC WDT 3 Second Timeout / OC WDT 5 Second Timeout, OC WDR 10 Second Timeout / OC WDT 15 Second Timeout / OC WDT 30 Second Timeout / OC WDT 45 Second Timeout / OC WDT 60 Second Timeout This setting affect whether the Over Clocking Watchdog Timer is enabled to automatically start on Host power cycle	RPP-S	OC WDT Disabled
	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 Raptor Lake S Platform Controller Hub EDS.	RPP-S	2ms
	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".	RPP-S	Disabled

Table 2-7. - Power (Sheet 1 of 2)

Select Power option on the left side menu then click Platform Power on the right to expand:			
<div> <div>Platform Power</div> <div>1</div> <div> <div>SLP_S3# / GPD4 Signal Configuration</div> <div>Enable as SLP_S3#</div> </div> <div> <div>SLP_S4# / GPD5 Signal Configuration</div> <div>Enable as SLP_S4#</div> </div> <div> <div>SLP_A# / GPD6 Signal Configuration</div> <div>Enable as SLP_A#</div> </div> <div> <div>SLP_S5# / GPD10 Signal Configuration</div> <div>Enable as SLP_S5#</div> </div> <div> <div>SLP_S0# Tunnel</div> <div>Disabled</div> </div> </div>			
#	Parameter	Platform	Settings
1	Platform Power		
	SLP_S3# / GPD4 Signal Configuration Values: SLP_S3# / GPD4 This setting allows the customer to assign the SLP_S3# Power Control signal as SLP_S3# or as GDP4. Note: For further details see Raptor Lake S Platform Controller Hub EDS.	RPP-S	SLP_S3#
	SLP_S4# / GPD5 Signal Configuration Values: SLP_S4# / GPD5 This setting allows the customer to assign the SLP_S4# Power Control signal as SLP_S4# or as GDP5. Note: For further details see Raptor Lake S Platform Controller Hub EDS.	RPP-S	SLP_S4#
	SLP_A# / GPD6 Signal Configuration Values: SLP_A# / GPD6 This setting allows the customer to assign the SLP_A# Power Control signal as SLP_A# or as GDP6. Note: For further details see Raptor Lake S Platform Controller Hub EDS.	RPP-S	SLP_A#
	SLP_S5# / GPD10 Signal Configuration Values: SLP_S5# / GPD10 This setting allows the customer to assign the SLP_S5# Power Control signal as SLP_S5# or as GDP10. Note: For further details see Raptor Lake S Platform Controller Hub EDS.	RPP-S	SLP_S5#
	SLP_S0# Tunnel Values: Yes / No This setting Enables / Disables the tunneling of the SLP_S0# pin over ESPI to the EC when in ESPI mode.	RPP-S	Disabled
Select Power option on the left side menu then click Deep Sx on the right to expand:			

Table 2-7. - Power (Sheet 2 of 2)

<div> <div>Deep Sx</div> <div>2</div> <div></div> </div> <div> <div>Deep Sx Enabled</div> <div>No</div> </div>			
#	Parameter	Platform	Settings
2	Deep Sx		
	Deep Sx Enabled Values: Yes / No This setting enables / disables support for Deep Sx operation. For further details see Raptor Lake S Platform Controller Hub EDS. Note: Support for Deep Sx is board design dependent.	RPP-S	Yes
Select Power option on the left side menu then click PCH Thermal Reporting on the right to expand:			
<div> <div>PCH Thermal Reporting</div> <div>3</div> <div></div> </div> <div> <div>Thermal Power Reporting Enabled</div> <div>Yes</div> </div>			
#	Parameter	Platform	Settings
3	PCH Thermal Reporting		
	Thermal Power Reporting Enabled Values: Yes / No 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.	RPP-S	Yes Yes

Table 2-8. - Networking & Connectivity (Sheet 1 of 3)

Select Networking and Connectivity option on the left side menu then click Wireless LAN Configuration on the right to expand:			
<div> <div>Wireless Lan Configuration</div> <div> <div>SLP_WLAN# / GDP9 Signal Configuration</div> <div>Enable as SLP_WLAN#</div> </div> <div> <div>CNVi WLAN Card Enabled</div> <div>Enabled</div> </div> <div> <div>Intel(R) ME CLINK Signal Enabled</div> <div>Yes</div> </div> <div> <div>WLAN Power Well</div> <div>SLP_WLAN#</div> </div> <div> <div>WLAN Microcode</div> <div>0x2725 SOLAR</div> </div> </div>			
#	Parameter	Platform	Settings
1	Wireless LAN Configuration		
	SLP_WLAN# / GDP9 Signal Configuration Values: SLP_WLAN# / GDP9 This setting allows the customer to assign the WLAN Power Control signal to WLAN or GDP9. Note: If using Intel® Wireless LAN this setting should be set to "Enable as SLP_WLAN#".	RPP-S	Enable as SLP_WLAN#
	CNVi WLAN Card Enabled Values: Enabled / Disabled This setting determine whether the platform support CNVi based WLAN card or not. Note: This setting should be set to enabled on either Corporate or Consumer platforms to avoid issues if WLAN card is changed in the future.	RPP-S	Enabled
	Intel® ME CLINK Enabled Values: Yes / No This setting allows customers to enable / disable the Wireless LAN CLINK signal through Intel® ME firmware. Note: For using Intel® vPro™ Wireless solutions this should be set to "Yes".	RPP-S	No
	WLAN Power Well Values: Disabled / Core Well SLP_S3# / Primary Well SLP_SUS# / SLP_A# / SLP_WLAN# This setting allows OEMs to configure the power well that will be used by Intel® Wireless LAN. Note: Recommended setting is SLP_WLAN#.	RPP-S	SLP_WLAN#
	WLAN Microcode This setting allows OEMs to configure which Intel® Wireless LAN card microcode to load into the firmware image. Valid WLAN cards for Raptor Lake: 0x2725 TyP 0x1002 Grp2 0x1004 Gr4	RPL-S	0x2725 SOLAR
Select Networking and Connectivity option on the left side menu then click Wired LAN Configuration on the right to expand:			

Table 2-8. - Networking & Connectivity (Sheet 2 of 3)

Wired Lan Configuration 2

LAN PHY Power Control GPD11 Signal Configuration

GbE MAC SMBus Address

GbE MAC SMBus Address Enabled

GbE PHY SMBus Address

PHY Connection

GbE PCIe Port Select

LAN PHY Power Up Time

Intel(R) Integrated Wired LAN Enabled

LAN Power Well

Enable as LANPHYPC

0x70

Yes

0x64

No PHY Connected

Port3

100ms

Yes

SLP_LAN#

#	Parameter	Platform	Settings
2	Wired LAN Configuration		
	LAN Power Well Values: Core Well, Sus Well, ME Well, SLP_LAN This setting allows customers to configure the power well that will be used by Intel® Integrated LAN. Note: Recommended setting is SLP_LAN#.	RPP-S	SLP_LAN#
	LAN PHY Power Up Time Values: 50ms, 100ms This bit determines how long the delay for LAN PHY to power up after de-assertion of SLP_LAN#.	RPP-S	100ms
	Intel® Integrated Wired LAN Enable Values: Enabled/Disabled This setting enables or disables the Intel® Integrated LAN.	RPP-S	Enabled
	GbE PCIe Port Select Values: None / PORT3 / PORT7 / PORT15 This setting allows customers to configure the PCIe Port that will Intel® Integrated LAN will operate on.	RPP-S	Port 7
	GbE PHY SMBus Address Values: Hex Value This setting configures Intel® Integrated Wired LAN SMBus address to accept SMBus cycles from the MAC. Note: Recommended setting is 64h.	RPP-S	0x64
	GbE SMBus Address Enabled Values: Yes / No This enables the Intel® Integrated Wired LAN MAC SMBus address. Note: This setting must be enabled if using Intel® Integrated LAN.	RPP-S	Yes

Table 2-8. - Networking & Connectivity (Sheet 3 of 3)

	GbE MAC SMBus Address Values: Hex Value This setting configures Intel(R) Integrated Wired LAN MAC SMBus address to accept SMBus cycles from the PHY. Note: Recommended setting is 70h.	RPP-S	0x70
	PHY Connection Values: No PHY connected / PHY on SMLink0 This selects which SMBus network is used to connect GbE PHY to MAC / PCH.	RPP-S	PHY on SMLink0
	LAN PHY Power Control GPD11 Signal Configuration Values: GPD11, LANPHYPC This setting allows the customer to assign the LAN PHY Power Control signal to GbE or as GDP11. Note: If using Intel® Integrated LAN this setting should be set to "Enable as LANPHYPC".	RPP-S	LANPHYPC
Select Networking and Connectivity option on the left side menu then click Time Sensitive Networking Configuration on the right to expand:			
<div> <div>Time Sensitive Networking Configuration</div> <div>3</div> <div> <div>Time Sensitive Networking Link Speed Select</div> <div>TSN 1 and TSN 2 1 Gig</div> </div> <div> <div>Time Sensitive Networking</div> <div>TSN 1 and 2 Disabled</div> </div> </div>			
#	Parameter	Platform	Settings
3	Time Sensitive Networking Configuration		
	Time Sensitive Network Link Speed Select Values: TSN 1 and TSN2 1 Gig / TSN1 1 Gig and TSN 2 2.5 Gig / TSN 1 2.5 Gig and TSN2 1 Gig / TSN 1 and TSN 2 2.5 Gig This setting configures the Link speed for TSN ports 1 and 2. Note: Not applicable for client platforms	RPP-S	TSN 1 and TSN2 1 Gig
	Time Sensitive Networking Values: TSN 1 and 2 Disabled / TSN 1 Enabled TSN 2 Disabled / TSN 1 Disabled TSN 2 Enabled / TSN 1 and 2 Enabled This setting Enables / Disables TSN ports 1 and 2 on the platform. Note: Not applicable for client platforms Note: Time Sensitive Networking and Wired LAN are mutually exclusive only one other these features can enabled on the platform.	RPP-S	Disabled

Table 2-9. - Flex I/O Straps (Sheet 1 of 21)

Select Flex I/O option on the left side menu then click USB3 Port Configuration on the right to expand:

Table 2-9. - Flex I/O Straps (Sheet 2 of 21)

USB3 Port Configuration 1 Q			
USB3 Port 1 Connector Type Select		Type C	
USB3 Port 2 Connector Type Select		Type C	
USB3 Port 3 Connector Type Select		Type A / Type C	
USB3 Port 4 Connector Type Select		Type A / Type C	
USB3 Port 5 Connector Type Select		Type A / Type C	
USB3 Port 6 Connector Type Select		Type A / Type C	
USB3 Port 7 Connector Type Select		Type C	
USB3 Port 8 Connector Type Select		Type C	
USB3 Port 9 Connector Type Select		Type A / Type C	
USB3 Port 10 Connector Type Select		Type A / Type C	
USB3.2 Ports 1 and 2 Speed Select and Pairing		Paired	
USB3.2 Ports 3 and 4 Speed Select and Pairing		USB 3.2 Port 1 and 2 Gen 2x1	
USB3.2 Ports 5 and 6 Speed Select and Pairing		USB 3.2 Port 1 and 2 Gen 2x1	
USB3.2 Ports 7 and 8 Speed Select and Pairing		Paired	
USB3.2 Ports 9 and 10 Speed Select and Pairing		USB 3.2 Port 1 and 2 Gen 2x1	
#	Parameter	Platform	Settings
1	USB3 Port Configuration		
	USB3 Port 1 Connector Type Select Values: Type C, Type A / Type C This setting configures the physical connector type to be used for USB 3.1 Port 1.	RPP-S	Type C
	USB3 Port 2 Connector Type Select Values: Type C, Type A / Type C This setting configures the physical connector type to be used for USB 3.1 Port 1.	RPP-S	Type C
	USB3 Port 3 Connector Type Select Values: Type C, Type A / Type C This setting configures the physical connector type to be used for USB 3.1 Port 1.	RPP-S	Type A / Type C
	USB3 Port 4 Connector Type Select Values: Type C, Type A / Type C This setting configures the physical connector type to be used for USB 3.1 Port 1.	RPP-S	Type A / Type C
	USB3 Port 5 Connector Type Select Values: Type C, Type A / Type C This setting configures the physical connector type to be used for USB 3.1 Port 1.	RPP-S	Type A / Type C
	USB3 Port 6 Connector Type Select Values: Type C, Type A / Type C This setting configures the physical connector type to be used for USB 3.1 Port 1.	RPP-S	Type A / Type C
	USB3 Port 7 Connector Type Select Values: Type C, Type A / Type C This setting configures the physical connector type to be used for USB 3.1 Port 1.	RPP-S	Type C

Table 2-9. - Flex I/O Straps (Sheet 3 of 21)

	USB3 Port 8 Connector Type Select Values: Type C, Type A / Type C This setting configures the physical connector type to be used for USB 3.1 Port 1.	RPP-S	Type C
	USB3 Port 9 Connector Type Select Values: Type C, Type A / Type C This setting configures the physical connector type to be used for USB 3.1 Port 1.	RPP-S	Type A / Type C
	USB3 Port 10 Connector Type Select Values: Type C, Type A / Type C This setting configures the physical connector type to be used for USB 3.1 Port 1.	RPP-S	Type A / Type C
	USB 3.2 Ports 1 and 2 Speed Select and Pairing Values: Not Paired, Paired, Paired Tx1/Tx2 Rx1/Rx2 Orientation, USB 3.2 Port 1 and 2 Gen 1x1, USB 3.2 Port 1 and 2 Gen 2x1, USB 3.2 Port 1 1x1 Port 2 Gen 2x1, USB3.2 Port 1 2x1 Port 2 Gen 1x1 This setting configures USB3.2 Ports 1 and 2 Speed selection and lane pairing modes.	RPP-S	Paired
	USB 3.2 Ports 3 and 4 Speed Select and Pairing Values: Not Paired, Paired, Paired Tx1/Tx2 Rx1/Rx2 Orientation, USB 3.2 Port 1 and 2 Gen 1x1, USB 3.2 Port 1 and 2 Gen 2x1, USB 3.2 Port 1 1x1 Port 2 Gen 2x1, USB3.2 Port 1 2x1 Port 2 Gen 1x1 This setting configures USB3.2 Ports 3 and 4 Speed selection and lane pairing modes.	RPP-S	USB 3.2 Port 1 and 2 Gen 2x1
	USB 3.2 Ports 5 and 6 Speed Select and Pairing Values: Not Paired, Paired, Paired Tx1/Tx2 Rx1/Rx2 Orientation, USB 3.2 Port 1 and 2 Gen 1x1, USB 3.2 Port 1 and 2 Gen 2x1, USB 3.2 Port 1 1x1 Port 2 Gen 2x1, USB3.2 Port 1 2x1 Port 2 Gen 1x1 This setting configures USB3.2 Ports 5 and 6 Speed selection and lane pairing modes.	RPP-S	USB 3.2 Port 1 and 2 Gen 2x1
	USB 3.2 Ports 7 and 8 Speed Select and Pairing Values: Not Paired, Paired, Paired Tx1/Tx2 Rx1/Rx2 Orientation, USB 3.2 Port 1 and 2 Gen 1x1, USB 3.2 Port 1 and 2 Gen 2x1, USB 3.2 Port 1 1x1 Port 2 Gen 2x1, USB3.2 Port 1 2x1 Port 2 Gen 1x1 This setting configures USB3.2 Ports 7 and 8 Speed selection and lane pairing modes.	RPP-S	Paired
	USB 3.2 Ports 9 and 10 Speed Select and Pairing Values: Not Paired, Paired, Paired Tx1/Tx2 Rx1/Rx2 Orientation, USB 3.2 Port 1 and 2 Gen 1x1, USB 3.2 Port 1 and 2 Gen 2x1, USB 3.2 Port 1 1x1 Port 2 Gen 2x1, USB3.2 Port 1 2x1 Port 2 Gen 1x1 This setting configures USB3.2 Ports 9 and 10 Speed selection and lane pairing modes.	RPP-S	USB 3.2 Port 1 and 2 Gen 2x1
Select Flex I/O option on the left side menu then click USB2 Port Configuration on the right to expand:			

Table 2-9. - Flex I/O Straps (Sheet 4 of 21)

USB2 Port Configuration 2 Q			
<div> <div>USB2 Port 1 Connector Type Select</div> <div>Type C</div> </div> <div> <div>USB2 Port 2 Connector Type Select</div> <div>Type A / Type C</div> </div> <div> <div>USB2 Port 3 Connector Type Select</div> <div>Type A / Type C</div> </div> <div> <div>USB2 Port 4 Connector Type Select</div> <div>Type A / Type C</div> </div> <div> <div>USB2 Port 5 Connector Type Select</div> <div>Type A / Type C</div> </div> <div> <div>USB2 Port 6 Connector Type Select</div> <div>Type A / Type C</div> </div> <div> <div>USB2 Port 7 Connector Type Select</div> <div>Type A / Type C</div> </div> <div> <div>USB2 Port 8 Connector Type Select</div> <div>Type A / Type C</div> </div> <div> <div>USB2 Port 9 Connector Type Select</div> <div>Type C</div> </div> <div> <div>USB2 Port 10 Connector Type Select</div> <div>Type A / Type C</div> </div> <div> <div>USB2 Port 11 Connector Type Select</div> <div>Type A / Type C</div> </div> <div> <div>USB2 Port 12 Connector Type Select</div> <div>Type A / Type C</div> </div> <div> <div>USB2 Port 13 Connector Type Select</div> <div>Type A / Type C</div> </div> <div> <div>USB2 Port 14 Connector Type Select</div> <div>Express Card / M.2 S2</div> </div>			
#	Parameter	Platform	Settings
2	Flex I/O - USB2 Port Configuration		
	USB2 Port 1 Connector Type Select Values: Type A / Type C This setting configures the physical connector type to be used for USB2 Port 1.	RPP-S	Type-C
	USB2 Port 2 Connector Type Select Values: Type A / Type C This setting configures the physical connector type to be used for USB2 Port 2.	RPP-S	Type A / Type C
	USB2 Port 3 Connector Type Select Values: Type A / Type C This setting configures the physical connector type to be used for USB2 Port 3.	RPP-S	Type A / Type C
	USB2 Port 4 Connector Type Select Values: Type A / Type C This setting configures the physical connector type to be used for USB2 Port 4.	RPP-S	Type A / Type C
	USB2 Port 5 Connector Type Select Values: Type A / Type C This setting configures the physical connector type to be used for USB2 Port 5.	RPP-S	Type A / Type C

Table 2-9. - Flex I/O Straps (Sheet 5 of 21)

	USB2 Port 6 Connector Type Select Values: Type A / Type C This setting configures the physical connector type to be used for USB2 Port 6.	RPP-S	Type A / Type C																				
	USB2 Port 7 Connector Type Select Values: Type A / Type C This setting configures the physical connector type to be used for USB2 Port 7.	RPP-S	Type A / Type C																				
	USB2 Port 8 Connector Type Select Values: Type A / Type C This setting configures the physical connector type to be used for USB2 Port 8.	RPP-S	Type A / Type C																				
	USB2 Port 9 Connector Type Select Values: Type A / Type C This setting configures the physical connector type to be used for USB2 Port 9.	RPP-S	Type C																				
	USB2 Port 10 Connector Type Select Values: Type A / Type C This setting configures the physical connector type to be used for USB2 Port 10.	RPP-S	Type A / Type C																				
	USB2 Port 11 Connector Type Select Values: Type A / Type C This setting configures the physical connector type to be used for USB2 Port 11.	RPP-S	Type A / Type C																				
	USB2 Port 12 Connector Type Select Values: Type A / Type C This setting configures the physical connector type to be used for USB2 Port 12.	RPP-S	Type A / Type C																				
	USB2 Port 13 Connector Type Select Values: Type A / Type C This setting configures the physical connector type to be used for USB2 Port 13.	RPP-S	Type A / Type C																				
	USB2 Port 14 Connector Type Select Values: Type A / Type C This setting configures the physical connector type to be used for USB2 Port 14.	RPP-S	Express Card / M.2 S2																				
Select Flex I/O option on the left side menu then click SATA / PCIe Combo Port Configuration on the right to expand:																							
<div>SATA / PCIe Combo Port Configuration<div>3</div><div></div></div> <table><tr><td>SATA / PCIe Combo Port 0 Mode Select</td><td>PCIe CLKREQ#</td></tr><tr><td>SATA / PCIe Combo Port 1 Mode Select</td><td>PCIe CLKREQ#</td></tr><tr><td>SATA / PCIe Combo Port 2 Mode Select</td><td>PCIe CLKREQ#</td></tr><tr><td>SATA / PCIe Combo Port 3 Mode Select</td><td>PCIe CLKREQ#</td></tr><tr><td>SATA / PCIe Combo Port 4 Mode Select</td><td>PCIe CLKREQ#</td></tr><tr><td>SATA / PCIe Combo Port 5 Mode Select</td><td>PCIe CLKREQ#</td></tr><tr><td>SATA / PCIe Combo Port 6 Mode Select</td><td>PCIe CLKREQ#</td></tr><tr><td>SATA / PCIe Combo Port 7 Mode Select</td><td>PCIe CLKREQ#</td></tr><tr><td>SATA / PCIe Combo Port's 0-3 values configuration.</td><td>PCIe</td></tr><tr><td>SATA / PCIe Combo Port's 4-7 values configuration.</td><td>SATA</td></tr></table>				SATA / PCIe Combo Port 0 Mode Select	PCIe CLKREQ#	SATA / PCIe Combo Port 1 Mode Select	PCIe CLKREQ#	SATA / PCIe Combo Port 2 Mode Select	PCIe CLKREQ#	SATA / PCIe Combo Port 3 Mode Select	PCIe CLKREQ#	SATA / PCIe Combo Port 4 Mode Select	PCIe CLKREQ#	SATA / PCIe Combo Port 5 Mode Select	PCIe CLKREQ#	SATA / PCIe Combo Port 6 Mode Select	PCIe CLKREQ#	SATA / PCIe Combo Port 7 Mode Select	PCIe CLKREQ#	SATA / PCIe Combo Port's 0-3 values configuration.	PCIe	SATA / PCIe Combo Port's 4-7 values configuration.	SATA
SATA / PCIe Combo Port 0 Mode Select	PCIe CLKREQ#																						
SATA / PCIe Combo Port 1 Mode Select	PCIe CLKREQ#																						
SATA / PCIe Combo Port 2 Mode Select	PCIe CLKREQ#																						
SATA / PCIe Combo Port 3 Mode Select	PCIe CLKREQ#																						
SATA / PCIe Combo Port 4 Mode Select	PCIe CLKREQ#																						
SATA / PCIe Combo Port 5 Mode Select	PCIe CLKREQ#																						
SATA / PCIe Combo Port 6 Mode Select	PCIe CLKREQ#																						
SATA / PCIe Combo Port 7 Mode Select	PCIe CLKREQ#																						
SATA / PCIe Combo Port's 0-3 values configuration.	PCIe																						
SATA / PCIe Combo Port's 4-7 values configuration.	SATA																						
#	Parameter	Platform	Settings																				

Table 2-9. - Flex I/O Straps (Sheet 6 of 21)

3	SATA / PCIe Combo Port Configuration Note: Port configuration works in 4 lane granularity. SATA and PCIe modes are mutually exclusive only one mode type can be active at a time across each set of 4 lanes (i.e. SATA / PCIe Combo Ports 0-3 and SATA / PCIe Combo Ports 4-7).		
	SATA / PCIe Combo Port 0 Mode Select Values: PCIe CLKREQ#, DEVSLP# The corresponding CLKREQ# GPIO can only function as DEVSLP# if SATA / PCIe Combo Port 0 is assigned to SATA, and SATA / PCIe Combo Port 0 Mode Select is configured to SATA.	RPP-S	PCIe CLKREQ#
	SATA / PCIe Combo Port 1 Mode Select Values: PCIe CLKREQ#, DEVSLP# The corresponding CLKREQ# GPIO can only function as DEVSLP# if SATA / PCIe Combo Port 0 is assigned to SATA, and SATA / PCIe Combo Port 1 Mode Select is configured to SATA.	RPP-S	PCIe CLKREQ#
	SATA / PCIe Combo Port 2 Mode Select Values: PCIe CLKREQ#, DEVSLP# The corresponding CLKREQ# GPIO can only function as DEVSLP# if SATA / PCIe Combo Port 0 is assigned to SATA, and SATA / PCIe Combo Port 2 Mode Select is configured to SATA.	RPP-S	PCIe CLKREQ#
	SATA / PCIe Combo Port 3 Mode Select Values: PCIe CLKREQ#, DEVSLP# The corresponding CLKREQ# GPIO can only function as DEVSLP# if SATA / PCIe Combo Port 0 is assigned to SATA, and SATA / PCIe Combo Port 2 Mode Select is configured to SATA.	RPP-S	PCIe CLKREQ#
	SATA / PCIe Combo Port 4 Mode Select Values: PCIe CLKREQ#, DEVSLP# The corresponding CLKREQ# GPIO can only function as DEVSLP# if SATA / PCIe Combo Port 0 is assigned to SATA, and SATA / PCIe Combo Port 4 Mode Select is configured to SATA.	RPP-S	PCIe CLKREQ#
	SATA / PCIe Combo Port 5 Mode Select Values: PCIe CLKREQ#, DEVSLP# The corresponding CLKREQ# GPIO can only function as DEVSLP# if SATA / PCIe Combo Port 0 is assigned to SATA, and SATA / PCIe Combo Port 5 Mode Select is configured to SATA.	RPP-S	PCIe CLKREQ#
	SATA / PCIe Combo Port 6 Mode Select Values: PCIe CLKREQ#, DEVSLP# The corresponding CLKREQ# GPIO can only function as DEVSLP# if SATA / PCIe Combo Port 0 is assigned to SATA, and SATA / PCIe Combo Port 6 Mode Select is configured to SATA.	RPP-S	PCIe CLKREQ#
	SATA / PCIe Combo Port 7 Mode Select Values: PCIe CLKREQ#, DEVSLP# The corresponding CLKREQ# GPIO can only function as DEVSLP# if SATA / PCIe Combo Port 0 is assigned to SATA, and SATA / PCIe Combo Port 7 Mode Select is configured to SATA.	RPP-S	PCIe CLKREQ#
	SATA / PCIe Combo Port's 0-3 values configurations Values: SATA / PCIe / GPIO Polarity PCIe / GPIO Polarity SATA This option enables usage of SATA / PCIe Combo Port's 0-3 values. Setting this value will apply the same to all 'SATA / PCIe Combo Port's.	RPP-S	PCIe
	SATA / PCIe Combo Port's 4-7 values configurations Values: SATA / PCIe / GPIO Polarity PCIe / GPIO Polarity SATA This option enables usage of SATA / PCIe Combo Port's 4-7 values. Setting this value will apply the same to all 'SATA / PCIe Combo Port's.	RPP-S	SATA
Select Flex I/O option on the left side menu then click PCIe Port Configuration on the right to expand:			

Table 2-9. - Flex I/O Straps (Sheet 7 of 21)

PCle Port Configuration 4 Q			
PCle Controller 1 (Port 1-4)		1x4	▼
PCle Controller 2 (Port 5-8)		1x2, 2x1	▼
PCle Controller 3 (Port 9-12)		1x4	▼
PCle Controller 4 (Port 13-16)		1x4	▼
PCle Controller 5 (Port 17-20)		4x1	▼
PCle Controller 6 (Port 21-24)		1x4 Lane Reversed	▼
PCle Controller 7 (Port 25-28)		1x4	▼
#	Parameter	Platform	Settings
4	PCle Port Configuration		
	PCle Controller 1 (Port 1-4) Values: 4x1, 1x2, 2x1, 2x2, 1x4, 1x4 Lane Reversed This setting controls PCIe Port configurations for PCIe Controller 1. Note: For further details on supported PCIe port configurations see Raptor Lake S Platform Controller Hub EDS.	RPP-S	1x4
	PCle Controller 2 (Port 5-8) Values: 4x1, 1x2, 2x1, 2x2, 1x4, 1x4 Lane Reversed This setting controls PCIe Port configurations for PCIe Controller 2. Note: For further details on supported PCIe port configurations see Raptor Lake S Platform Controller Hub EDS.	RPP-S	1x2, 2x1
	PCle Controller 3 (Port 9-12) Values: 4x1, 1x2, 2x1, 2x2, 1x4, 1x4 Lane Reversed This setting controls PCIe Port configurations for PCIe Controller 3. Note: For further details on supported PCIe port configurations see Raptor Lake S Platform Controller Hub EDS.	RPP-S	1x4
	PCle Controller 4 (Port 13-16) Values: 4x1, 1x2, 2x1, 2x2, 1x4, 1x4 Lane Reversed This setting controls PCIe Port configurations for PCIe Controller 4. Note: For further details on supported PCIe port configurations see Raptor Lake S Platform Controller Hub EDS.	RPP-S	1x4
	PCle Controller 5 (Port 17-20) Values: 4x1, 1x2, 2x1, 2x2, 1x4, 1x4 Lane Reversed This setting controls PCIe Port configurations for PCIe Controller 5. Note: For further details on supported PCIe port configurations see Raptor Lake S Platform Controller Hub EDS.	RPP-S	4x1
	PCle Controller 6 (Port 21-24) Values: 4x1, 1x2, 2x1, 2x2, 1x4, 1x4 Lane Reversed This setting controls PCIe Port configurations for PCIe Controller 6. Note: For further details on supported PCIe port configurations see Raptor Lake S Platform Controller Hub EDS.	RPP-S	1x4 Lane Reversed

Table 2-9. - Flex I/O Straps (Sheet 8 of 21)

	PCIe Controller 7 (Port 25-28) Values: 4x1, 1x2, 2x1, 2x2, 1x4, 1x4 Lane Reversed This setting controls PCIe Port configurations for PCIe Controller 7. Note: For further details on supported PCIe port configurations see Raptor Lake S Platform Controller Hub EDS.	RPP-S	1x4
Select Flex I/O option on the left side menu then click Power Delivery PD Controller Configuration on the right to expand:			

Table 2-9. - Flex I/O Straps (Sheet 9 of 21)

Power Delivery PD Controller Configuration 4 Q	
PMC-PD Controller USB Type-C Mode	PMC / SMBus
Re-timer Power Gating Enabled	No
Type-C port 1 Enabled	Yes
Type-C Port 1 Re-Timer Present	No
Type-C Port 1 Re-timer Configuration Enabled	No
Type C Port 1 SMBus Address	0x38
Type-C Port 1 Re-timer SMBus Address	0x0
USB2 Port Number associated for Type-C Port 1	USB2 Port 9
USB3 Port Number associated for Type-C Port 1	Type-C Port 1
Type-C Port 1 Re-Timer Configuration Type	1 Re-Timer
Type-C Port 1 USB3 Ownership	PCH
Type-C port 2 Enabled	Yes
Type-C Port 2 Re-Timer Present	No
Type-C Port 2 Re-timer Configuration Enabled	No
Type-C Port 2 SMBus Address	0x3F
Type-C Port 2 Re-timer SMBus Address	0x0
USB2 Port Number associated for Type-C Port 2	USB2 Port 1
USB3 Port Number associated for Type-C Port 2	Type-C Port 7
Type-C Port 2 Re-Timer Configuration Type	1 Re-Timer
Type-C Port 2 USB3 Ownership	PCH
Type-C port 3 Enabled	No
Type-C Port 3 Re-Timer Present	No
Type-C Port 3 Re-timer Configuration Enabled	No
Type-C Port 3 SMBus Address	0x0
Type-C Port 3 Re-timer SMBus Address	0x0
USB2 Port Number associated for Type-C Port 3	USB2 Port 6
USB3 Port Number associated for Type-C Port 3	Type-C Port 3
Type-C Port 3 Re-Timer Configuration Type	1 Re-Timer
Type-C Port 3 USB3 Ownership	CPU
Type-C port 4 Enabled	No
Type-C Port 4 Re-Timer Present	No
Type-C Port 4 Re-timer Configuration Enabled	No
Type-C Port 4 SMBus Address	0x0
Type-C Port 4 Re-timer SMBus Address	0x0
USB2 Port Number associated for Type-C Port 4	USB2 Port 7
USB3 Port Number associated for Type-C Port 4	Type-C Port 4
Type-C Port 4 Re-Timer Configuration Type	1 Re-Timer
Type-C Port 4 USB3 Ownership	CPU

Table 2-9. - Flex I/O Straps (Sheet 10 of 21)

#	Parameter	Platform	Settings
5	Power Delivery PD Controller Configuration		
	PMC-PD controller USB-C Mode Values: PMC / SMBus, PMC / eSPI This bit defines how the PMC interfaces with the Type-C components on the board. Note: When this setting is set to PMC / SMBus the Type-C Default State setting can be used to determine Type-C connection behavior.	RPP-S	PMC / SMBus
	Re-timer Power Gating Enabled Values: Yes / No This setting indicates whether platform Re-timer power gating is enabled.	RPP-S	No
	Type-C port 1 Enabled Values: Yes / No This setting indicates whether the associated Type-C port1 is enabled.	RPP-S	Yes
	Type-C Port 1 Re-timer Present Values: Yes / No This indicates whether a re-timer is present for the associated Type-C port.	RPP-S	No
	Type-C Port 1 Re-timer Configuration Enabled Values: Yes / No Indicates whether the associated re-timer requires configuration. Yes = configuration done via PMC; No = configuration done via PD Controller.	RPP-S	No
	Type-C Port 1 SMBus Address Value: Hex This indicates the SMBus address for the associated Type-C port. Note: It is recommended that OEMs set a unique SMBus address allocation for Type-C port and Re-timer associated.	RPP-S	0x38
	Type-C Port 1 Re-timer SMBus Address Value: Hex This indicates the SMBus address for the associated re-timer.	RPP-S	0x0
	USB2 Port Number associated for Type-C Port 1 Values: USB2 Port 1,USB2 Port 2,USB2 Port 3,USB2 Port 4,USB2 Port 5,USB2 Port 6,USB2 Port 7,USB2 Port 8,USB2 Port 9,USB2 Port 10 This indicates the USB2 port number for the associated Type-C port1. Notes: <ol style="list-style-type: none"> 1. This parameter is applicable only when Type-C port 1 Enabled is set to yes. 2. Once user selects USB2 port number associated with Type-C port1,the respective USB2 port connector selection will be greyed out and auto set to Type-C under the USB2 Port Configuration section. example: if USB2 Port number associated for Type-C Port 1 is set to "USB2 Port 2" ,Parameter under Flex I/O->USB2 Port Configuration->USB2 Port 2 Connector Type Select will be grayed out and auto set to "Type C". 3. OEMs are recommended to configure different USB-C connectors with increasing port numbers (TCP0_*, TCP1_*, TCP2_*, TCP3_*), should be paired with increasing number of USB2 ports from PCH. (this is needed to make split xDCI controller work functionally)E.g. (TCP0_*, USB2*_1), (TCP1_*, USB2*_3), (TCP2_*, USB2*_4), (TCP3_*, USB2*_5) 	RPP-S	USB2 Port 9

Table 2-9. - Flex I/O Straps (Sheet 11 of 21)

USB3 Port number associated for Type-C Port 1 Values: Type-C Port 1, Type-C Port 2, Type-C Port 3, Type-C Port 4, Type-C Port 5, Type-C Port 6, Type-C Port 7, Type-C Port 8, Type-C Port 9, Type-C Port 10 This indicates the USB3 port number for the associated Type-C port1. Notes: <ol style="list-style-type: none"> 1. This parameter is applicable only when Type-C port 1 Enabled is set to yes. 2. Once user selects USB3 port number associated with Type-C port1,the respective USB3 port connector selection will be greyed out and auto set to Type-C under the USB3 Port Configuration section. example: if USB Port number associated for Type-C Port 1 is set to "USB3 Port 6" ,Parameter under Flex I/O->USB3 Port Configuration->USB3 Port 6 Connector Type Select will be grayed out and auto set to "Type C". 3. OEMs are recommended to configure different USB-C connectors with increasing port numbers (TCP0_*, TCP1_*, TCP2_*, TCP3_*), should be paired with increasing number of USB2 ports from PCH. (this is needed to make split xDCI controller work functionally)E.g. (TCP0_*, USB2*_1), (TCP1_*, USB2*_3), (TCP2_*, USB2*_4), (TCP3_*, USB2*_5) 	RPP-S	Type-C Port 1
Type-C Port 1 Connector Type Select Values: 1 Re-Timer, 2 Re-Timers This setting determines the number of Re-Timers being used for Type-C Port 1	RPP-S	1 Re-Timer
Type-C Port 1 USB3 Ownership Values: CPU / PCH This setting determines if the Type-C Port 1 USB3 is owned by CPU or PCH.	RPP-S	PCH
Type-C port 2 Enabled Values: Yes / No This setting indicates whether the associated Type-C port is enabled.	RPP-S	Yes
Type-C Port 2 Re-timer Present Values: Yes / No This indicates whether a re-timer is present for the associated Type-C port.	RPP-S	No
Type-C Port 2 Re-timer Configuration Enabled Values: Yes / No Indicates whether the associated re-timer requires configuration. Yes = configuration done via PMC; No = configuration done via PD Controller.	RPP-S	No
Type-C Port 2 SMBus Address Value: Hex This indicates the SMBus address for the associated Type-C port. Note: It is recommended that OEMs set a unique SMBus address allocation for Type-C port and Re-timer associated.	RPP-S	0x3F
Type-C Port 2 Re-timer SMBus Address Value: Hex This indicates the SMBus address for the associated re-timer.	RPP-S	0x0
USB2 Port Number associated for Type-C Port 2 Values: USB2 Port 1,USB2 Port 2,USB2 Port 3,USB2 Port 4,USB2 Port 5,USB2 Port 6,USB2 Port 7,USB2 Port 8,USB2 Port 9,USB2 Port 10 This indicates the USB2 port number for the associated Type-C port. Notes: <ol style="list-style-type: none"> 1. This parameter is applicable only when Type-C port 2 Enabled is set to yes. 2. Once user selects USB2 port number associated with Type-C port2,the respective USB2 port connector selection will be greyed out and auto set to Type-C under the USB2 Port Configuration section. example: if USB2 Port number associated for Type-C Port 2 is set to "USB2 Port 2" ,Parameter under Flex I/O->USB2 Port Configuration->USB2 Port 2 Connector Type Select will be grayed out and auto set to "Type C". 3. OEMs are recommended to configure different USB-C connectors with increasing port numbers (TCP0_*, TCP1_*, TCP2_*, TCP3_*), should be paired with increasing number of USB2 ports from PCH. (this is needed to make split xDCI controller work functionally)E.g. (TCP0_*, USB2*_1), (TCP1_*, USB2*_3), (TCP2_*, USB2*_4), (TCP3_*, USB2*_5) 	RPP-S	USB2 Port 1

Table 2-9. - Flex I/O Straps (Sheet 12 of 21)

USB3 Port number associated for Type-C Port 2 Values: Type-C Port 1, Type-C Port 2, Type-C Port 3, Type-C Port 4, Type-C Port 5, Type-C Port 6, Type-C Port 7, Type-C Port 8, Type-C Port 9, Type-C Port 10 This indicates the USB3 port number for the associated Type-C port. Notes: <ol style="list-style-type: none"> 1. This parameter is applicable only when Type-C port 2Enabled is set to yes. 2. Once user selects USB3 port number associated with Type-C port2,the respective USB3 port connector selection will be greyed out and auto set to Type-C under the USB3 Port Configuration section. example: if USB Port number associated for Type-C Port 2is set to "USB3 Port 6" ,Parameter under Flex I/O->USB3 Port Configuration->USB3 Port 6 Connector Type Select will be grayed out and auto set to "Type C". 3. OEMs are recommended to configure different USB-C connectors with increasing port numbers (TCP0_*, TCP1_*, TCP2_*, TCP3_*), should be paired with increasing number of USB2 ports from PCH. (this is needed to make split xDCI controller work functionally)E.g. (TCP0_*, USB2*_1), (TCP1_*, USB2*_3), (TCP2_*, USB2*_4), (TCP3_*, USB2*_5) 	RPP-S	Type-C Port 7
Type-C Port 2 Connector Type Select Values: 1 Re-Timer, 2 Re-Timers This setting determines the number of Re-Timers being used for Type-C Port 2	RPP-S	1 Re-Timer
Type-C Port 2 USB3 Ownership Values: CPU / PCH This setting determines if the Type-C Port 2 USB3 is owned by CPU or PCH.	RPP-S	PCH
Type-C port 3 Enabled Values: Yes / No This setting indicates whether the associated Type-C port is enabled.	RPP-S	No
Type-C Port 3 Re-timer Present Values: Yes / No This indicates whether a re-timer is present for the associated Type-C port.	RPP-S	Yes
Type-C Port 3 Re-timer Configuration Enabled Values: Yes / No Indicates whether the associated re-timer requires configuration. Yes = configuration done via PMC; No = configuration done via PD Controller.	RPP-S	No
Type-C Port 3 SMBus Address Value: Hex This indicates the SMBus address for the associated Type-C port. Note: It is recommended that OEMs set a unique SMBus address allocation for Type-C port and Re-timer associated.	RPP-S	0x0
Type-C Port 3 Re-timer SMBus Address Value: Hex This indicates the SMBus address for the associated re-timer.	RPP-S	0x0
USB2 Port Number associated for Type-C Port 3 Values: USB2 Port 1,USB2 Port 2,USB2 Port 3,USB2 Port 4,USB2 Port 5,USB2 Port 6,USB2 Port 7,USB2 Port 8,USB2 Port 9,USB2 Port 10 This indicates the USB2 port number for the associated Type-C port. Notes: <ol style="list-style-type: none"> 1. This parameter is applicable only when Type-C port 3 Enabled is set to yes. 2. Once user selects USB2 port number associated with Type-C port3 ,the respective USB2 port connector selection will be greyed out and auto set to Type-C under the USB2 Port Configuration section. example: if USB2 Port number associated for Type-C Port 3 is set to "USB2 Port 2" ,Parameter under Flex I/O->USB2 Port Configuration->USB2 Port 2 Connector Type Select will be grayed out and auto set to "Type C". 3. OEMs are recommended to configure different USB-C connectors with increasing port numbers (TCP0_*, TCP1_*, TCP2_*, TCP3_*), should be paired with increasing number of USB2 ports from PCH. (this is needed to make split xDCI controller work functionally)E.g. (TCP0_*, USB2*_1), (TCP1_*, USB2*_3), (TCP2_*, USB2*_4), (TCP3_*, USB2*_5) 	RPP-S	USB2 Port 6

Table 2-9. - Flex I/O Straps (Sheet 13 of 21)

USB3 Port number associated for Type-C Port 3 Values: Type-C Port 1, Type-C Port 2, Type-C Port 3, Type-C Port 4, Type-C Port 5, Type-C Port 6, Type-C Port 7, Type-C Port 8, Type-C Port 9, Type-C Port 10 This indicates the USB3 port number for the associated Type-C port. Notes: <ol style="list-style-type: none"> 1. This parameter is applicable only when Type-C port 3 Enabled is set to yes. 2. Once user selects USB3 port number associated with Type-C port3,the respective USB3 port connector selection will be greyed out and auto set to Type-C under the USB3 Port Configuration section. example: if USB Port number associated for Type-C Port 3 is set to "USB3 Port 6" ,Parameter under Flex I/O->USB3 Port Configuration->USB3 Port 6 Connector Type Select will be grayed out and auto set to "Type C". 3. OEMs are recommended to configure different USB-C connectors with increasing port numbers (TCP0_*, TCP1_*, TCP2_*, TCP3_*), should be paired with increasing number of USB2 ports from PCH. (this is needed to make split xDCI controller work functionally)E.g. (TCP0_*, USB2*_1), (TCP1_*, USB2*_3), (TCP2_*, USB2*_4), (TCP3_*, USB2*_5) 	RPP-S	USB3 Port 3
Type-C Port 3 Connector Type Select Values: 1 Re-Timer, 2 Re-Timers This setting determines the number of Re-Timers being used for Type-C Port 3	RPP-S	1 Re-Timer
Type-C Port 3 USB3 Ownership Values: CPU / PCH This setting determines if the Type-C Port 3 USB3 is owned by CPU or PCH.	RPP-S	PCH
Type-C port 4 Enabled Values: Yes / No This setting indicates whether the associated Type-C port is enabled.	RPP-S	No
Type-C Port 4 Re-timer Present Values: Yes / No This indicates whether a re-timer is present for the associated Type-C port.	RPP-S	No
Type-C Port 4 Re-timer Configuration Enabled Values: Yes / No Indicates whether the associated re-timer requires configuration. Yes = configuration done via PMC; No = configuration done via PD Controller.	RPP-S	No
Type-C Port 4 SMBus Address Value: Hex This indicates the SMBus address for the associated Type-C port. Note: It is recommended that OEMs set a unique SMBus address allocation for Type-C port and Re-timer associated.	RPP-S	0x0
Type-C Port 4 Re-timer SMBus Address Value: Hex This indicates the SMBus address for the associated re-timer.	RPP-S	0x0
USB2 Port Number associated for Type-C Port 4 Values: USB2 Port 1,USB2 Port 2,USB2 Port 3,USB2 Port 4,USB2 Port 5,USB2 Port 6,USB2 Port 7,USB2 Port 8,USB2 Port 9,USB2 Port 10 This indicates the USB2 port number for the associated Type-C port. Notes: <ol style="list-style-type: none"> 1. This parameter is applicable only when Type-C port 4 Enabled is set to yes. 2. Once user selects USB2 port number associated with Type-C port4,the respective USB2 port connector selection will be greyed out and auto set to Type-C under the USB2 Port Configuration section. example: if USB2 Port number associated for Type-C Port 4 is set to "USB2 Port 2" ,Parameter under Flex I/O->USB2 Port Configuration->USB2 Port 2 Connector Type Select will be grayed out and auto set to "Type C". 3. OEMs are recommended to configure different USB-C connectors with increasing port numbers (TCP0_*, TCP1_*, TCP2_*, TCP3_*), should be paired with increasing number of USB2 ports from PCH. (this is needed to make split xDCI controller work functionally)E.g. (TCP0_*, USB2*_1), (TCP1_*, USB2*_3), (TCP2_*, USB2*_4), (TCP3_*, USB2*_5) 	RPP-S	USB2 Port 7

Table 2-9. - Flex I/O Straps (Sheet 14 of 21)

	USB3 Port number associated for Type-C Port 4 Values: Type-C Port 1, Type-C Port 2, Type-C Port 3, Type-C Port 4, Type-C Port 5, Type-C Port 6, Type-C Port 7, Type-C Port 8, Type-C Port 9, Type-C Port 10 This indicates the USB3 port number for the associated Type-C port. Notes: <ol style="list-style-type: none"> 1. This parameter is applicable only when Type-C port 4 Enabled is set to yes. 2. Once user selects USB3 port number associated with Type-C port4,the respective USB3 port connector selection will be greyed out and auto set to Type-C under the USB3 Port Configuration section. example: if USB Port number associated for Type-C Port 4 is set to "USB3 Port 6" ,Parameter under Flex I/O->USB3 Port Configuration->USB3 Port 6 Connector Type Select will be grayed out and auto set to "Type C". 3. OEMs are recommended to configure different USB-C connectors with increasing port numbers (TCP0_*, TCP1_*, TCP2_*, TCP3_*), should be paired with increasing number of USB2 ports from PCH. (this is needed to make split xDCI controller work functionally)E.g. (TCP0_*, USB2*_1), (TCP1_*, USB2*_3), (TCP2_*, USB2*_4), (TCP3_*, USB2*_5) 	RPP-S	USB3 Port 4
	Type-C Port 4 Connector Type Select Values: 1 Re-Timer, 2 Re-Timers This setting determines the number of Re-Timers being used for Type-C Port 4	RPP-S	1 Re-Timer
	Type-C Port 4 USB3 Ownership Values: CPU / PCH This setting determines if the Type-C Port 4 USB3 is owned by CPU or PCH.	RPP-S	PCH
Select Flex I/O option on the left side menu then click Type-C Subsystem Configuration on the right to expand:			
<div> <div>Type-C Subsystem Configuration 6</div> <div> <div>NPHY Binary File</div> <div>NPHY version</div> </div> </div>			
#	Parameter	Platform	Settings
6	Type-C Subsystem Configuration		
	NPHY Binary File This loads the NPHY binary that will be merged into the output image generated by the Intel® FIT.	RPP-S	NPHY Binary
	NPHY Version - This displays the version of NPHY binary.		
Select Flex I/O option on the left side menu then click SPHY Configuration on the right to expand:			
<div> <div>SPHY Configuration 7</div> <div> <div>PHY Binary Configuration File</div> <div>SPHY version</div> </div> </div>			
#	Parameter	Platform	Settings
7	SPHY Configuration		

Table 2-9. - Flex I/O Straps (Sheet 15 of 21)

	SPHY Binary Configuration File - This loads the SPHY binary that will be merged into the output image generated by the Intel® FIT.	RPP-S	SPHY binary
	SPHY Version - This displays the version of SPHY		
Select Flex I/O option on the left side menu then click PCH HSIO Tuning on the right to expand:			
Click OEM SPHY Version on the right to expand:			
<div> <div>OEM SPHY Version</div> <div>8</div> <div>Q</div> <div> <div>Major Version</div> <div>0x10</div> </div> <div> <div>Minor Version</div> <div>0x2</div> </div> <div> <div>Hotfix Version</div> <div>0x99</div> </div> <div> <div>Build Version</div> <div>0x0</div> </div> </div>			
#	Parameter	Platform	Settings
8	OEM SPHY Version		
	Major Version - This displays the Major version number for the OEM SPHY binary.	RPP-S	0x10
	Minor Version - This displays the Minor version number for the OEM SPHY binary.	RPP-S	0x2
	Hotfix Version - This displays the Hotfix version number for the OEM SPHY binary.	RPP-S	0x99
	Build Version Values: Hex Input This setting allow users to select a build number for the OEM_SPHY binary for version tracking. Note: The build number needs to be any whole number from 0 to 65535	RPP-S	0x0
Click PCIe HSIO PHY Settings on the right to expand:			
<div> <div>PCIe HSIO PHY Settings</div> <div>9</div> <div>Q</div> <div> <div>PCIe Lanes [4:1] TX_Vboost</div> <div>Default</div> </div> <div> <div>PCIe Lanes [8:5] TX_Vboost</div> <div>Default</div> </div> <div> <div>PCIe Lanes [12:9] TX_Vboost</div> <div>Default</div> </div> <div> <div>PCIe Lanes [20:13] TX_Vboost</div> <div>Default</div> </div> <div> <div>PCIe Lanes [24:21] TX_Vboost</div> <div>Default</div> </div> <div> <div>PCIe Lanes [28:25] TX_Vboost</div> <div>Default</div> </div> </div>			
#	Parameter	Platform	Settings

Table 2-9. - Flex I/O Straps (Sheet 16 of 21)

9	PCIe HSIO PHY Settings		
	PCIe Lanes [4:1] TX_Vboost Values: Default / 800mVpdd / 900mVpdd / 1000mVpdd / 1100mVpdd This setting configures the voltage swing on PCIe lanes 1 to 4.	RPP-S	Default
	PCIe Lanes [8:5] TX_Vboost Values: Default / 800mVpdd / 900mVpdd / 1000mVpdd / 1100mVpdd This setting configures the voltage swing on PCIe lanes 5 to 8.	RPP-S	Default
	PCIe Lanes [12:9] TX_Vboost Values: Default / 800mVpdd / 900mVpdd / 1000mVpdd / 1100mVpdd This setting configures the voltage swing on PCIe lanes 9 to 12.	RPP-S	Default
	PCIe Lanes [20:13] TX_Vboost Values: Default / 800mVpdd / 900mVpdd / 1000mVpdd / 1100mVpdd This setting configures the voltage swing on PCIe lanes 13 to 20.	RPP-S	Default
	PCIe Lanes [24:21] TX_Vboost Values: Default / 800mVpdd / 900mVpdd / 1000mVpdd / 1100mVpdd This setting configures the voltage swing on PCIe lanes 21 to 24.	RPP-S	Default
	PCIe Lanes [28:25] TX_Vboost Values: Default / 800mVpdd / 900mVpdd / 1000mVpdd / 1100mVpdd This setting configures the voltage swing on PCIe lanes 25 to 28.	RPP-S	Default
Click SATA HSIO PHY Settings on the right to expand:			

Table 2-9. - Flex I/O Straps (Sheet 17 of 21)

SATA HSIO PHY Settings

10
Q

SATA Lanes [7:0] TX_Vboost	Default
SATA Lane [0] RX_CTLE_Boost	Default
SATA Lane [1] RX_CTLE_Boost	Default
SATA Lane [2] RX_CTLE_Boost	Default
SATA Lane [3] RX_CTLE_Boost	Default
SATA Lane [4] RX_CTLE_Boost	Default
SATA Lane [5] RX_CTLE_Boost	Default
SATA Lane [6] RX_CTLE_Boost	Default
SATA Lane [7] RX_CTLE_Boost	Default
SATA Lane [0] TX_EQ_Cm	Default
SATA Lane [0] TX_EQ_C0	Default
SATA Lane [0] TX_EQ_Cp	Default
SATA Lane [1] TX_EQ_Cm	Default
SATA Lane [1] TX_EQ_C0	Default
SATA Lane [1] TX_EQ_Cp	Default
SATA Lane [2] TX_EQ_Cm	Default
SATA Lane [2] TX_EQ_C0	Default
SATA Lane [2] TX_EQ_Cp	Default
SATA Lane [3] TX_EQ_Cm	Default
SATA Lane [3] TX_EQ_C0	Default
SATA Lane [3] TX_EQ_Cp	Default
SATA Lane [4] TX_EQ_Cm	Default
SATA Lane [4] TX_EQ_C0	Default
SATA Lane [4] TX_EQ_Cp	Default
SATA Lane [5] TX_EQ_Cm	Default
SATA Lane [5] TX_EQ_C0	Default
SATA Lane [5] TX_EQ_Cp	Default
SATA Lane [6] TX_EQ_Cm	Default
SATA Lane [6] TX_EQ_C0	Default
SATA Lane [6] TX_EQ_Cp	Default
SATA Lane [7] TX_EQ_Cm	Default
SATA Lane [7] TX_EQ_C0	Default
SATA Lane [7] TX_EQ_Cp	Default

Table 2-9. - Flex I/O Straps (Sheet 18 of 21)

#	Parameter	Platform	Settings
10	SATA HSIO PHY Settings		
	SATA Lanes [7:0] TX_Vboost Values: Default / 800mVpdd / 900mVpdd / 1000mVpdd / 1100mVpdd This setting configures the voltage swing on SATA lanes 0 to 7.	RPP-S	Default
	SATA Lane [0] RX_CTLE_Boost Values: Default / 7dB / 8dB / 9dB / 10dB / 11dB / 12dB / 13dB / 14dB / 15dB / 16dB / 17dB / 18dB / 19dB / 20dB This setting configures the Gen3 RX CTLE Boost on SATA Lane [0].	RPP-S	Default
	SATA Lane [1] RX_CTLE_Boost Values: Default / 7dB / 8dB / 9dB / 10dB / 11dB / 12dB / 13dB / 14dB / 15dB / 16dB / 17dB / 18dB / 19dB / 20dB This setting configures the Gen3 RX CTLE Boost on SATA Lane [1].	RPP-S	Default
	SATA Lane [2] RX_CTLE_Boost Values: Default / 7dB / 8dB / 9dB / 10dB / 11dB / 12dB / 13dB / 14dB / 15dB / 16dB / 17dB / 18dB / 19dB / 20dB This setting configures the Gen3 RX CTLE Boost on SATA Lane [2].	RPP-S	Default
	SATA Lane [3] RX_CTLE_Boost Values: Default / 7dB / 8dB / 9dB / 10dB / 11dB / 12dB / 13dB / 14dB / 15dB / 16dB / 17dB / 18dB / 19dB / 20dB This setting configures the Gen3 RX CTLE Boost on SATA Lane [3].	RPP-S	Default
	SATA Lane [4] RX_CTLE_Boost Values: Default / 7dB / 8dB / 9dB / 10dB / 11dB / 12dB / 13dB / 14dB / 15dB / 16dB / 17dB / 18dB / 19dB / 20dB This setting configures the Gen3 RX CTLE Boost on SATA Lane [4].	RPP-S	Default
	SATA Lane [5] RX_CTLE_Boost Values: Default / 7dB / 8dB / 9dB / 10dB / 11dB / 12dB / 13dB / 14dB / 15dB / 16dB / 17dB / 18dB / 19dB / 20dB This setting configures the Gen3 RX CTLE Boost on SATA Lane [5].	RPP-S	Default
	SATA Lane [6] RX_CTLE_Boost Values: Default / 7dB / 8dB / 9dB / 10dB / 11dB / 12dB / 13dB / 14dB / 15dB / 16dB / 17dB / 18dB / 19dB / 20dB This setting configures the Gen3 RX CTLE Boost on SATA Lane [6].	RPP-S	Default
	SATA Lane [7] RX_CTLE_Boost Values: Default / 7dB / 8dB / 9dB / 10dB / 11dB / 12dB / 13dB / 14dB / 15dB / 16dB / 17dB / 18dB / 19dB / 20dB This setting configures the Gen3 RX CTLE Boost on SATA Lane [7].	RPP-S	Default
	SATA Lane [0] TX_EQ_Cm Values: Default / 0dB / 1dB / 2dB / 3dB / 4dB / 5dB / 6dB / 7dB / 8dB / 9dB / 10dB / 11dB / 12dB / 13dB / 14dB / 15dB This setting configures the Gen3 TX EQ Coefficient Pre-shoot (Cm) on SATA Lane [0]. If adjusted the associated SATA Lane [0] C0 and Cp values must be set to a desired value or a user error will be flagged and MFIT will be blocked from building an image.	RPP-S	Default
	SATA Lane [0] TX_EQ_C0 Values: Default / 0dB / 1dB / 2dB / 3dB / 4dB / 5dB / 6dB / 7dB / 8dB / 9dB / 10dB / 11dB / 12dB / 13dB / 14dB / 15dB This setting configures the Gen3 TX EQ Coefficient Pre-shoot (C0) on SATA Lane [0]. If adjusted the associated SATA Lane [0] Cm and Cp values must be set to a desired value or a user error will be flagged and MFIT will be blocked from building an image.	RPP-S	Default

Table 2-9. - Flex I/O Straps (Sheet 19 of 21)

	SATA Lane [0] TX_EQ_Cp Values: Default / 0dB / 1dB / 2dB / 3dB / 4dB / 5dB / 6dB / 7dB / 8dB / 9dB / 10dB / 11dB / 12dB / 13dB / 14dB / 15dB This setting configures the Gen3 TX EQ Coefficient Pre-shoot (Cp) on SATA Lane [0]. If adjusted the associated SATA Lane [0] Cm and C0 values must be set to a desired value or a user error will be flagged and MFIT will be blocked from building an image.	RPP-S	Default
	SATA Lane [1] TX_EQ_Cm Values: Default / 0dB / 1dB / 2dB / 3dB / 4dB / 5dB / 6dB / 7dB / 8dB / 9dB / 10dB / 11dB / 12dB / 13dB / 14dB / 15dB This setting configures the Gen3 TX EQ Coefficient Pre-shoot (Cm) on SATA Lane [1]. If adjusted the associated SATA Lane [1] C0 and Cp values must be set to a desired value or a user error will be flagged and MFIT will be blocked from building an image.	RPP-S	Default
	SATA Lane [1] TX_EQ_C0 Values: Default / 0dB / 1dB / 2dB / 3dB / 4dB / 5dB / 6dB / 7dB / 8dB / 9dB / 10dB / 11dB / 12dB / 13dB / 14dB / 15dB This setting configures the Gen3 TX EQ Coefficient Pre-shoot (C0) on SATA Lane [1]. If adjusted the associated SATA Lane [1] Cm and Cp values must be set to a desired value or a user error will be flagged and MFIT will be blocked from building an image.	RPP-S	Default
	SATA Lane [1] TX_EQ_Cp Values: Default / 0dB / 1dB / 2dB / 3dB / 4dB / 5dB / 6dB / 7dB / 8dB / 9dB / 10dB / 11dB / 12dB / 13dB / 14dB / 15dB This setting configures the Gen3 TX EQ Coefficient Pre-shoot (Cp) on SATA Lane [1]. If adjusted the associated SATA Lane [0] Cm and C0 values must be set to a desired value or a user error will be flagged and MFIT will be blocked from building an image.	RPP-S	Default
	SATA Lane [2] TX_EQ_Cm Values: Default / 0dB / 1dB / 2dB / 3dB / 4dB / 5dB / 6dB / 7dB / 8dB / 9dB / 10dB / 11dB / 12dB / 13dB / 14dB / 15dB This setting configures the Gen3 TX EQ Coefficient Pre-shoot (Cm) on SATA Lane [2]. If adjusted the associated SATA Lane [1] C0 and Cp values must be set to a desired value or a user error will be flagged and MFIT will be blocked from building an image.	RPP-S	Default
	SATA Lane [2] TX_EQ_C0 Values: Default / 0dB / 1dB / 2dB / 3dB / 4dB / 5dB / 6dB / 7dB / 8dB / 9dB / 10dB / 11dB / 12dB / 13dB / 14dB / 15dB This setting configures the Gen3 TX EQ Coefficient Pre-shoot (C0) on SATA Lane [2]. If adjusted the associated SATA Lane [1] Cm and Cp values must be set to a desired value or a user error will be flagged and MFIT will be blocked from building an image.	RPP-S	Default
	SATA Lane [2] TX_EQ_Cp Values: Default / 0dB / 1dB / 2dB / 3dB / 4dB / 5dB / 6dB / 7dB / 8dB / 9dB / 10dB / 11dB / 12dB / 13dB / 14dB / 15dB This setting configures the Gen3 TX EQ Coefficient Pre-shoot (Cp) on SATA Lane [2]. If adjusted the associated SATA Lane [0] Cm and C0 values must be set to a desired value or a user error will be flagged and MFIT will be blocked from building an image.	RPP-S	Default
	SATA Lane [3] TX_EQ_Cm Values: Default / 0dB / 1dB / 2dB / 3dB / 4dB / 5dB / 6dB / 7dB / 8dB / 9dB / 10dB / 11dB / 12dB / 13dB / 14dB / 15dB This setting configures the Gen3 TX EQ Coefficient Pre-shoot (Cm) on SATA Lane [3]. If adjusted the associated SATA Lane [1] C0 and Cp values must be set to a desired value or a user error will be flagged and MFIT will be blocked from building an image.	RPP-S	Default
	SATA Lane [3] TX_EQ_C0 Values: Default / 0dB / 1dB / 2dB / 3dB / 4dB / 5dB / 6dB / 7dB / 8dB / 9dB / 10dB / 11dB / 12dB / 13dB / 14dB / 15dB This setting configures the Gen3 TX EQ Coefficient Pre-shoot (C0) on SATA Lane [3]. If adjusted the associated SATA Lane [1] Cm and Cp values must be set to a desired value or a user error will be flagged and MFIT will be blocked from building an image.	RPP-S	Default

Table 2-9. - Flex I/O Straps (Sheet 20 of 21)

	SATA Lane [3] TX_EQ_Cp Values: Default / 0dB / 1dB / 2dB / 3dB / 4dB / 5dB / 6dB / 7dB / 8dB / 9dB / 10dB / 11dB / 12dB / 13dB / 14dB / 15dB This setting configures the Gen3 TX EQ Coefficient Pre-shoot (Cp) on SATA Lane [3]. If adjusted the associated SATA Lane [0] Cm and C0 values must be set to a desired value or a user error will be flagged and MFIT will be blocked from building an image.	RPP-S	Default
	SATA Lane [4] TX_EQ_Cm Values: Default / 0dB / 1dB / 2dB / 3dB / 4dB / 5dB / 6dB / 7dB / 8dB / 9dB / 10dB / 11dB / 12dB / 13dB / 14dB / 15dB This setting configures the Gen3 TX EQ Coefficient Pre-shoot (Cm) on SATA Lane [4]. If adjusted the associated SATA Lane [1] C0 and Cp values must be set to a desired value or a user error will be flagged and MFIT will be blocked from building an image.	RPP-S	Default
	SATA Lane [4] TX_EQ_C0 Values: Default / 0dB / 1dB / 2dB / 3dB / 4dB / 5dB / 6dB / 7dB / 8dB / 9dB / 10dB / 11dB / 12dB / 13dB / 14dB / 15dB This setting configures the Gen3 TX EQ Coefficient Pre-shoot (C0) on SATA Lane [4]. If adjusted the associated SATA Lane [1] Cm and Cp values must be set to a desired value or a user error will be flagged and MFIT will be blocked from building an image.	RPP-S	Default
	SATA Lane [4] TX_EQ_Cp Values: Default / 0dB / 1dB / 2dB / 3dB / 4dB / 5dB / 6dB / 7dB / 8dB / 9dB / 10dB / 11dB / 12dB / 13dB / 14dB / 15dB This setting configures the Gen3 TX EQ Coefficient Pre-shoot (Cp) on SATA Lane [4]. If adjusted the associated SATA Lane [0] Cm and C0 values must be set to a desired value or a user error will be flagged and MFIT will be blocked from building an image.	RPP-S	Default
	SATA Lane [5] TX_EQ_Cm Values: Default / 0dB / 1dB / 2dB / 3dB / 4dB / 5dB / 6dB / 7dB / 8dB / 9dB / 10dB / 11dB / 12dB / 13dB / 14dB / 15dB This setting configures the Gen3 TX EQ Coefficient Pre-shoot (Cm) on SATA Lane [5]. If adjusted the associated SATA Lane [1] C0 and Cp values must be set to a desired value or a user error will be flagged and MFIT will be blocked from building an image.	RPP-S	Default
	SATA Lane [5] TX_EQ_C0 Values: Default / 0dB / 1dB / 2dB / 3dB / 4dB / 5dB / 6dB / 7dB / 8dB / 9dB / 10dB / 11dB / 12dB / 13dB / 14dB / 15dB This setting configures the Gen3 TX EQ Coefficient Pre-shoot (C0) on SATA Lane [5]. If adjusted the associated SATA Lane [1] Cm and Cp values must be set to a desired value or a user error will be flagged and MFIT will be blocked from building an image.	RPP-S	Default
	SATA Lane [5] TX_EQ_Cp Values: Default / 0dB / 1dB / 2dB / 3dB / 4dB / 5dB / 6dB / 7dB / 8dB / 9dB / 10dB / 11dB / 12dB / 13dB / 14dB / 15dB This setting configures the Gen3 TX EQ Coefficient Pre-shoot (Cp) on SATA Lane [5]. If adjusted the associated SATA Lane [0] Cm and C0 values must be set to a desired value or a user error will be flagged and MFIT will be blocked from building an image.	RPP-S	Default
	SATA Lane [6] TX_EQ_Cm Values: Default / 0dB / 1dB / 2dB / 3dB / 4dB / 5dB / 6dB / 7dB / 8dB / 9dB / 10dB / 11dB / 12dB / 13dB / 14dB / 15dB This setting configures the Gen3 TX EQ Coefficient Pre-shoot (Cm) on SATA Lane [6]. If adjusted the associated SATA Lane [1] C0 and Cp values must be set to a desired value or a user error will be flagged and MFIT will be blocked from building an image.	RPP-S	Default
	SATA Lane [6] TX_EQ_C0 Values: Default / 0dB / 1dB / 2dB / 3dB / 4dB / 5dB / 6dB / 7dB / 8dB / 9dB / 10dB / 11dB / 12dB / 13dB / 14dB / 15dB This setting configures the Gen3 TX EQ Coefficient Pre-shoot (C0) on SATA Lane [6]. If adjusted the associated SATA Lane [1] Cm and Cp values must be set to a desired value or a user error will be flagged and MFIT will be blocked from building an image.	RPP-S	Default

Table 2-9. - Flex I/O Straps (Sheet 21 of 21)

	SATA Lane [6] TX_EQ_Cp Values: Default / 0dB / 1dB / 2dB / 3dB / 4dB / 5dB / 6dB / 7dB / 8dB / 9dB / 10dB / 11dB / 12dB / 13dB / 14dB / 15dB This setting configures the Gen3 TX EQ Coefficient Pre-shoot (Cp) on SATA Lane [6]. If adjusted the associated SATA Lane [0] Cm and C0 values must be set to a desired value or a user error will be flagged and MFIT will be blocked from building an image.	RPP-S	Default
	SATA Lane [7] TX_EQ_Cm Values: Default / 0dB / 1dB / 2dB / 3dB / 4dB / 5dB / 6dB / 7dB / 8dB / 9dB / 10dB / 11dB / 12dB / 13dB / 14dB / 15dB This setting configures the Gen3 TX EQ Coefficient Pre-shoot (Cm) on SATA Lane [7]. If adjusted the associated SATA Lane [1] C0 and Cp values must be set to a desired value or a user error will be flagged and MFIT will be blocked from building an image.	RPP-S	Default
	SATA Lane [7] TX_EQ_C0 Values: Default / 0dB / 1dB / 2dB / 3dB / 4dB / 5dB / 6dB / 7dB / 8dB / 9dB / 10dB / 11dB / 12dB / 13dB / 14dB / 15dB This setting configures the Gen3 TX EQ Coefficient Pre-shoot (C0) on SATA Lane [7]. If adjusted the associated SATA Lane [1] Cm and Cp values must be set to a desired value or a user error will be flagged and MFIT will be blocked from building an image.	RPP-S	Default
	SATA Lane [7] TX_EQ_Cp Values: Default / 0dB / 1dB / 2dB / 3dB / 4dB / 5dB / 6dB / 7dB / 8dB / 9dB / 10dB / 11dB / 12dB / 13dB / 14dB / 15dB This setting configures the Gen3 TX EQ Coefficient Pre-shoot (Cp) on SATA Lane [7]. If adjusted the associated SATA Lane [0] Cm and C0 values must be set to a desired value or a user error will be flagged and MFIT will be blocked from building an image.	RPP-S	Default
Click USB3.2 HSIO PHY Settings on the right to expand:			
<div> <div>USB3.2 HSIO PHY Settings</div> <div>11</div> <div> <div>USB 3.2 Lanes [4:1] TX_Vboost</div> <div>Default</div> </div> <div> <div>USB 3.2 Lanes [6:5] TX_Vboost</div> <div>Default</div> </div> <div> <div>USB 3.2 Lanes [10:7] TX_Vboost</div> <div>Default</div> </div> </div>			
#	Parameter	Platform	Settings
11	USB3.2 HSIO PHY Settings		
	USB 3.2 Lanes [4:1] TX_Vboost Values: Default / 800mVpdd / 900mVpdd / 1000mVpdd / 1100mVpdd This setting configures the voltage swing on USB 3.2 Lanes 1 to 4.	RPP-S	Default
	USB 3.2 Lanes [6:5] TX_Vboost Values: Default / 800mVpdd / 900mVpdd / 1000mVpdd / 1100mVpdd This setting configures the voltage swing on USB 3.2 Lanes 5 and 6.	RPP-S	Default
	USB 3.2 Lanes [10:7] TX_Vboost Values: Default / 800mVpdd / 900mVpdd / 1000mVpdd / 1100mVpdd This setting configures the voltage swing on USB 3.2 Lanes 7 to 10.	RPP-S	Default

Table 2-10. - Platform Protection (Sheet 1 of 7)

Select Platform Protection on the left side menu then click TPM Over SPI Bus Configuration on the right to expand:			
<div> <div>TPM Over SPI Bus Configuration</div> <div> <div>TPM Clock Frequency</div> <div>14MHz</div> </div> <div> <div>TPM Over SPI Bus Enabled</div> <div>No</div> </div> </div>			
#	Parameter	Platform	Settings
1	TPM Over SPI Bus Configuration		
	TPM Clock Frequency Values: 14MHz / 25MHz / 48MHz This setting determines the clock frequency setting to be used for the TPM over SPI bus.	RPP-S	14MHz
	TPM Over SPI Bus Enabled Values: Yes/No This setting determines if TPM over SPI bus is enabled on the platform.	RPP-S	No
Select Platform Protection on the left side menu then click BIOS Guard Configuration on the right to expand:			
<div> <div>BIOS Guard Configuration</div> <div> <div>BIOS Guard Protection Override Enabled</div> <div>Yes</div> </div> </div>			
#	Parameter	Platform	Settings
2	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).	RPP-S	No No
Select Platform Protection on the left side menu then click Descriptor Configuration on the right to expand:			
<div> <div>Descriptor Configuration</div> <div> <div>Exclude master access in the signature</div> <div>Yes</div> </div> <div> <div>Flash Descriptor Verification Enabled</div> <div>No</div> </div> </div>			
#	Parameter	Platform	Settings
3	Descriptor Configuration These settings are used for FuSa safety standards and are not applicable for client platforms.		

Table 2-10. - Platform Protection (Sheet 2 of 7)

	Flash Descriptor Verification Enabled Values: Yes/No This setting enables / disables Flash Descriptor Verification.	RPP-S	No
	Exclude Master access in the signature Values: Yes/No Include/exclude master access in the signature.	RPP-S	No
Select Platform Protection on the left side menu then click Exclusion Ranges on the right to expand:			
<div><div>Exclusion Ranges</div><div>4</div><div><div>Range 1 offset</div><div>0x800</div></div><div><div>Range 1 size</div><div>0x400</div></div><div><div>Range 2 offset</div><div>0x80</div></div><div><div>Range 2 size</div><div>0x20</div></div><div><div>Range 3 offset</div><div>0x0</div></div><div><div>Range 3 size</div><div>0x0</div></div><div><div>Range 4 offset</div><div>0x0</div></div><div><div>Range 4 size</div><div>0x0</div></div><div><div>Range 5 offset</div><div>0x0</div></div><div><div>Range 5 size</div><div>0x0</div></div><div><div>Range 6 offset</div><div>0x0</div></div><div><div>Range 6 size</div><div>0x0</div></div><div><div>Range 7 offset</div><div>0x0</div></div><div><div>Range 7 size</div><div>0x0</div></div><div><div>Range 8 offset</div><div>0x0</div></div><div><div>Range 8 size</div><div>0x0</div></div></div>			
#	Parameter	Platform	Settings
4	Exclusion Ranges These settings are used for FuSa safety standards and are not applicable for client platforms.		
	Range 1 offset Range 1 offset covers manifest, cannot be changed	RPP-S	0x800
	Range 1 size Range 1 size covers manifest, cannot be changed.	RPP-S	0x400
#	Parameter	Platform	Settings

Table 2-10. - Platform Protection (Sheet 3 of 7)

	Range 2 offset Range 2 offset covers manifest, cannot be changed	RPP-S	0x80
	Range 2 size Range 2 size covers manifest, cannot be changed.	RPP-S	0x20
	Range 3 offset Values: Hex Range 3 offset covers OEM defined unprotected range start.	RPP-S	0x0
	Range 3 size Values: Hex Range 3 size covers OEM defined unprotected range length	RPP-S	0x0
	Range 4 offset Values: Hex Range 4 offset covers OEM defined unprotected range start.	RPP-S	0x0
	Range 4 size Values: Hex Range 4 size covers OEM defined unprotected range length	RPP-S	0x0
	Range 5 offset Values: Hex Range 5 offset covers OEM defined unprotected range start.	RPP-S	0x0
	Range 5 size Values: Hex Range 5 size covers OEM defined unprotected range length	RPP-S	0x0
	Range 6 offset Values: Hex Range 6 offset covers OEM defined unprotected range start.	RPP-S	0x0
	Range 6 size Values: Hex Range 6 size covers OEM defined unprotected range length	RPP-S	0x0
	Range 7 offset Values: Hex Range 7 offset covers OEM defined unprotected range start.	RPP-S	0x0
	Range 7 size Values: Hex Range 7 size covers OEM defined unprotected range length	RPP-S	0x0
	Range 8 offset Values: Hex Range 8 offset covers OEM defined unprotected range start.	RPP-S	0x0
	Range 8 size Values: Hex Range 8 size covers OEM defined unprotected range length	RPP-S	0x0
Select Platform Protection on the left side menu then click Hash Key Configuration for Bootguard / ISH on the right to expand:			

Table 2-10. - Platform Protection (Sheet 4 of 7)

Hash Key Configuration for Bootguard / ISH

5

Skip OEM Keys Check

No

OEM Key Manifest Binary

Oem Key Revocation Enable

No

OEM Public Key Hash

00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00

Second OEM key hash

00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00

#	Parameter	Platform	Settings
5	Hash Key Configuration for Bootguard / ISH		
	Skip OEM Key Check Values: Yes/No This is meant for debugging purposes only. Enabling this parameter impacts image creation procedure in MFIT tool only.	RPP-S	No
	OEM Key Manifest Binary Signed manifest file containing hashes of keys used for signing components of image.	RPP-S	OEM KM Binary
	OEM Key Revocation Enabled Values: Yes/No This setting enables firmware OEM Key Revocation capabilities.	RPP-S	No
	OEM Public Key Hash Values: Hex Value Raw hash string for the SHA-384 hash of the OEM public key corresponding to the private key used to sign the OEM Key hash manifest. When manufacture is completed, this hash value is burned into an FPF, and is permanent. This value is used to verify the OEM Key hash, and also DnX images. OEM signing is disabled when this hash is set to all 0s. Note: Please see Appendix D for further details.	RPP-S	0x00000000
	Second OEM Key hash Values: Hex Value Raw hash string for the SHA-384 hash of the Secondary OEM public key. Note: Please see Appendix D for further details.	RPP-S	0x00000000

Select Platform Protection on the left side menu then click Crypto Hardware Support on the right to expand:

Crypto Hardware Support

6

Crypto HW Support

Yes

#	Parameter	Platform	Settings
6	Crypto HW Support		

Table 2-10. - Platform Protection (Sheet 5 of 7)

#	Parameter	Platform	Settings
	Crypto HW Support Values: Yes/No - This setting can be used to disable Intel® CSME cryptographic functionality. Caution: Configuring this setting to "No" will disables all Intel® CSME cryptographic related features.	RPP-S	Yes
Select Platform Protection on the left side menu then click Trusted Device Setup on the right to expand:			
<div> Trusted Device Setup 7 </div> <div> Enable TDS Capabilities <input type="text" value="No"/> </div>			
#	Parameter	Platform	Settings
7	Trusted Device Setup		
	Enable TDS Capabilities Values: Yes/No This setting enables Intel® Trusted Device Setup on the platform.	RPP-S	No
Select Platform Protection on the left side menu then click Intel® PTT Configuration on the right to expand:			
<div> Intel(R) PTT Configuration 8 </div> <div> SMx State <input type="text" value="Enabled"/> </div> <div> Rsa 1K State <input type="text" value="Disabled"/> </div> <div> Intel(R) PTT Supported <input type="text" value="Yes"/> </div> <div> Intel(R) PTT initial power-up state <input type="text" value="Enabled"/> </div> <div> Intel(R) PTT Supported [FPF] <input type="text" value="Yes"/> </div>			
#	Parameter	Platform	Settings
8	Intel® PTT Configuration		
	SMx Support state Values: Enabled/Disabled This setting enables/disables SMx support.	RPL-S	Enabled

Table 2-10. - Platform Protection (Sheet 6 of 7)

	Rsa 1K State Values: Enabled / Disabled This setting allows the user to enable / disable RSA 1024 bit encryption Intel highly recommends that customers leave this set to "Disabled" due to security concerns. Note: Having RSA 1024 bit encryption disabled impacts Windows* HLK TPM testing. Several tests have RSA 1024 dependencies. To avoid these failures this setting should be set to "Enabled" during HLK testing and then set to "Disabled" for the manufacturing image.	RPL-S	Disabled
	Intel® PTT Supported Values: Yes/No This setting permanently disables Intel® PTT in the firmware image.	RPP-S	Yes
	Intel® PTT initial power-up state Values: Enabled/Disabled This setting determines if Intel® PTT is enabled on platform power-up.	RPP-S	Enabled
	Intel® PTT Supported [FPF] Values: Yes/No This setting will permanently disable Intel® PTT through platform FPFs. Caution: Setting this option to Yes will permanently disable Intel® PTT on the platform hardware.	RPP-S	Yes
Select Platform Protection on the left side menu then click Content Protection on the right to expand:			
<div> <div>Content Protection</div> <div>9</div> <div>PAVP Supported</div> <div>Yes</div> <div>HDCP Internal Display Port 1 - 5K</div> <div>PortA</div> <div>HDCP Internal Display Port 2 - 5K</div> <div>None</div> </div>			
#	Parameter	Platform	Settings
9	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.	RPP-S	Yes
	HDCP Internal Display Port 1 - 5K Values: None, Port A, Port B, Port C, Port D 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.	RPP-S	PortA
	HDCP Internal Display Port 2 - 5K Values: None, Port A, Port B, Port C, Port D 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.	RPP-S	None
Select Platform Protection on the left side menu then click Boot Guard Configuration on the right to expand:			

Table 2-10. - Platform Protection (Sheet 7 of 7)

Boot Guard Configuration 10

CPU Debugging Disabled

BSP Initialization Enabled

Key Manifest ID 0x0

Boot Guard Profile Configuration Boot Guard Profile 0 - No_FVME

#	Parameter	Platform	Settings
10	Boot Guard Configuration		
	CPU Debugging Values: Enabled/Disabled This setting determines if CPU debug modes will be displayed. When set to 'Enabled' CPU debugging is enabled.	RPP-S	Disabled
	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).	RPP-S	Enabled
	Key Manifest ID Values: This option is for entering the hash of another public key, used by the ACM to verify the Boot Policy Manifest.	RPP-S	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.	RPP-S	Boot Guard Profile 0 - No_FVME

Select Platform Protection on the left side menu then click TXT Configuration on the right to expand:

TXT Configuration 11

TXT Supported No

#	Parameter	Platform	Settings
11	TXT Configuration		
	TXT Supported This setting determines if enabled for the platform.	RPP-S	No

Table 2-11. - Debug (Sheet 1 of 6)

Select Debug on the left side menu then click eSPI Feature Overrides on the right to expand:			
<div> <div>eSPI Feature Overrides</div> <div> <div>eSPI / EC Low Frequency Debug Override</div> <div>No</div> </div> </div>			
#	Parameter	Platform	Settings
1	eSPI Feature Overrides		
	eSPI / EC Low Frequency Debug Override When enabled this setting will divide eSPI clock frequency by 8. Note: This setting should only be used for debugging purposes. Leaving this setting enable will impact eSPI performance.	RPP-S	No
Select Debug on the left side menu then click Intel® ME Debugging Overrides on the right to expand:			
<div> <div>Intel(R) ME Firmware Debugging Overrides</div> <div> <div>Firmware ROM Bypass</div> <div>No</div> </div> <div> <div>Intel(R) ME Reset Behavior</div> <div>Intel(R) ME will Halt</div> </div> <div> <div>AFS Idle Flash Reclaim Enabled</div> <div>Yes</div> </div> <div> <div>Debug Override Pre-Production Silicon</div> <div>0x0</div> </div> <div> <div>Debug Override Production Silicon</div> <div>0x0</div> </div> </div>			
#	Parameter	Platform	Settings
2	Intel® ME Firmware Debugging Overrides		
	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.	RPP-S	No
	Intel® ME Reset Behavior Values: Intel® ME wil Halt / Intel® ME Alternate image boot This setting determines Intel® ME behavior when boot image errors are encountered. Warning: This setting should be used for debug purposes only. Incorrect configuration of this setting may block normal Firmware functional flows.	RPP-S	Intel® ME Alternate image boot

Table 2-11. - Debug (Sheet 2 of 6)

#	Parameter	Platform	Settings
	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.	RPP-S	Yes
	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® ME 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.	RPP-S	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.	RPP-S	0x00000000
Select Debug on the left side menu then click Direct Connection Interface Configuration on the right to expand:			

Table 2-11. - Debug (Sheet 3 of 6)


Direct Connect Interface Configuration 3 			
	Intel(R) DCI DbC Interface Enabled	No	▼
	DCI OOB over USB3 Port1 Enabled	Yes	▼
	DCI OOB over USB3 Port2 Enabled	Yes	▼
	DCI OOB over USB3 Port3 Enabled	Yes	▼
	DCI OOB over USB3 Port4 Enabled	Yes	▼
	DCI OOB over USB3 Port5 Enabled	Yes	▼
	DCI OOB over USB3 Port6 Enabled	Yes	▼
	DCI OOB over USB3 Port7 Enabled	Yes	▼
	DCI OOB over USB3 Port8 Enabled	Yes	▼
	DCI OOB over USB3 Port9 Enabled	Yes	▼
	DCI OOB over USB3 Port10 Enabled	Yes	▼
#	Parameter	Platform	Settings
3	Direct Connection Interface Configuration		
	Intel® DCI DbC Interface Enabled Values: Yes/No This setting enables / disables the Intel® DCI DbC interface.	RPP-S	No
	DCI OOB over USB3 Port1 Enabled Values: Yes / No This setting determines if the USB port being enabled for DCI OOB. If disabled it will block DCI OOB connection.	RPP-S	Yes
	DCI OOB over USB3 Port 2 Enabled Values: Yes / No This setting determines if the USB port being enabled for DCI OOB. If disabled it will block DCI OOB connection.	RPP-S	Yes
	DCI OOB over USB3 Port 3 Enabled Values: Yes / No This setting determines if the USB port being enabled for DCI OOB. If disabled it will block DCI OOB connection.	RPP-S	No
	DCI OOB over USB3 Port 4 Enabled Values: Yes / No This setting determines if the USB port being enabled for DCI OOB. If disabled it will block DCI OOB connection.	RPP-S	No
	DCI OOB over USB3 Port 5 Enabled Values: Yes / No This setting determines if the USB port being enabled for DCI OOB. If disabled it will block DCI OOB connection.	RPP-S	No

Table 2-11. - Debug (Sheet 4 of 6)

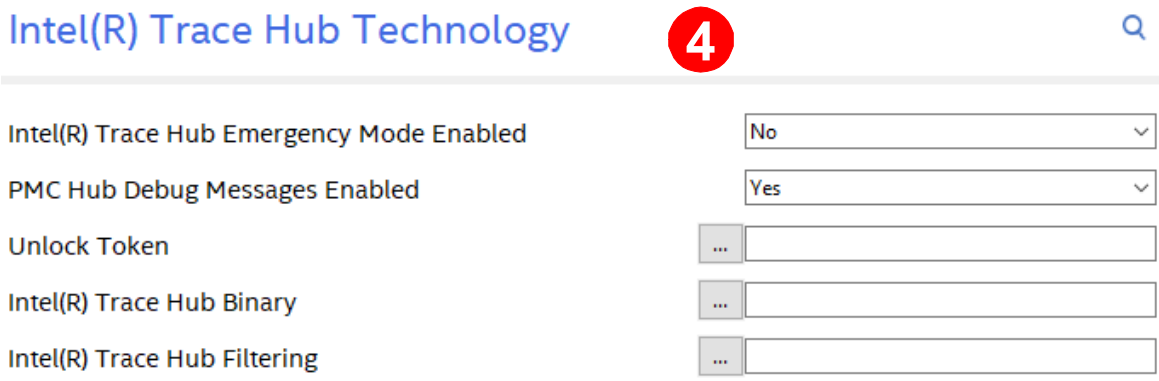
	DCI OOB over USB3 Port 6 Enabled Values: Yes / No This setting determines if the USB port being enabled for DCI OOB. If disabled it will block DCI OOB connection.	RPP-S	No
	DCI OOB over USB3 Port 7 Enabled Values: Yes / No This setting determines if the USB port being enabled for DCI OOB. If disabled it will block DCI OOB connection.	RPP-S	No
	DCI OOB over USB3 Port 8 Enabled Values: Yes / No This setting determines if the USB port being enabled for DCI OOB. If disabled it will block DCI OOB connection.	RPP-S	No
	DCI OOB over USB3 Port 9 Enabled Values: Yes / No This setting determines if the USB port being enabled for DCI OOB. If disabled it will block DCI OOB connection.	RPP-S	No
	DCI OOB over USB3 Port 10 Enabled Values: Yes / No This setting determines if the USB port being enabled for DCI OOB. If disabled it will block DCI OOB connection.	RPP-S	No
Select Debug on the left side menu then click Intel® Trace Hub Technology on the right to expand:			
			
#	Parameter	Platform	Settings
4	Intel® Trace Hub Technology		
	Intel® Trace Hub Emergency Mode Enabled Values: Yes/No This setting enable / disables Intel® Trace Hub in the firmware base image.	RPP-S	No
	PMC Hub Debug Message Enabled Values: Yes/No This setting enables/disables the PMC FW trace debug messages to the Intel® Trace Hub.	RPP-S	Yes
	Unlock Token This allows the OEM to input an Unlock Token binary file for closed chassis debug.	RPP-S	
	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.	RPP-S	Trace Hub Binary
	Intel® Trace Hub Filtering This setting allows a user input binary for filtering of output messages for Intel® Trace Hub.	RPP-S	Filter Binary (optional)

Table 2-11. - Debug (Sheet 5 of 6)

Select Debug on the left side menu then click Early USB DBC Type-A Configuration on the right to expand:			
<div> <div>Early USB2 DBC over Type-A Configuration</div> <div>5</div> <div> <div>USB2 DbC Auto Detect</div> <div>Disabled</div> </div> <div> <div>USB2 DbC port enable</div> <div>No USB2 Ports</div> </div> <div> <div>USB Connectors Associated USB3 Port enable</div> <div>No USB3 Ports</div> </div> <div> <div>Enable early USB2 DbC connection</div> <div>No</div> </div> </div>			
#	Parameter	Platform	Settings
5	Early USB DBC Type-A Configuration		
	USB2 DbC Auto Detect Values: Enabled / Disabled This setting allows USB2 DbC to be dynamically enabled when a Debug Accessory Mode cable is detected.	RPP-S	Disabled
	USB2 DbC port enable Values: No USB2 Ports, USB2 Port 1, USB2 Port 2, USB2 Port 3, USB2 Port 4, USB2 Port 5, USB2 Port 6, USB2 Port 7, USB2 Port 8, USB2 Port 9, USB2 Port 10, USB2 Port 11, USB2 Port 12, USB2 Port 13, USB2 Port 14 This setting determines which USB2 ports are enabled for Early DbC debugging.	RPP-S	No USB2 Ports
	USB Connectors associated USB3 Port enable Values: No USB3 Ports, USB3 Port 1, USB3 Port 2, USB3 Port 3, USB3 Port 4, USB3 Port 5, USB3 Port 6, USB3 Port 7, USB3 Port 8, USB3 Port 9, USB3 Port 10 This setting determines which USB3 ports goes to the target USB2 ports connector for Early DbC debugging.	RPP-S	No USB3 Ports
	Enabled early USB2 DbC connection Values: Yes / No This setting enabled a delay during Intel® ME firmware bring-up to allow USB2 DbC connection to be established	RPP-S	No
Select Debug on the left side menu then click IDLM on the right to expand:			
<div> <div>IDLM</div> <div>6</div> <div> <div>IDLM Binary</div> <div></div> <div>...</div> </div> </div>			
#	Parameter	Platform	Settings
6	IDLM		
	IDLM Binary This allows an IDLM binary to be merged into output image built by Intel® FIT.	RPP-S	IDLM Binary (Optional)
Select Debug on the left side menu then click Delayed Authentication Mode Configuration on the right to expand:			

Table 2-11. - Debug (Sheet 6 of 6)


Delayed Authentication Mode Configuration 7 			
Delayed Authentication Mode Enabled		<input type="text" value="No"/>	
#	Parameter	Platform	Settings
7	Delayed Authentication Mode Configuration		
	Delayed Authentication Mode Enabled Values: Yes/No - This setting enable / disables Delayed Authentication Mode on the platform.	RPP-S	No

Table 2-12. - Intel® ME Kernel (Sheet 1 of 5)

Select Intel® ME Kernel on the left side menu then click Reserved on the right to expand:			
<div>Reserved 1</div> <div>Reserved No</div>			
1	Reserved		
	Reserved Values: Yes/No <i>Note: Leave at default value</i>	RPP-S	No
Select Intel® ME Kernel on the left side menu then click Processor on the right to expand:			
<div>Processor 2</div> <div>Processor Emulation No Emulation</div> <div>Missing Processor Detection Alert No</div>			
#	Parameter	Platform	Settings
2	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 E (R) branded Processor EMULATE Intel® Xeon W (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. It is necessary to set this to Emulate Intel® vPro™ Processor in order to enable Intel® AMT.	RPP-S	EMULATE Intel® Core (TM) branded Processor
	Missing Processor Detection Alert Values: Yes / No This setting determines if missing processor detection is enabled on Desktop / Workstation platforms. <i>Note: This feature will only work if the platform has the appropriate glue logic present. In addition when this feature is enabled the CPU detection GPIO also needs to be configured.</i>	RPP-S	No
Select Intel® ME Kernel on the left side menu then click Intel® ME Firmware Update on the right to expand:			

Table 2-12. - Intel® ME Kernel (Sheet 2 of 5)

Intel(R) ME Firmware Update 3

Hide MEBx Firmware Update Control

No

Firmware Update OEM ID

00000000-0000-0000-0000-000000000000

OEM FW Version

0x0

Intel(R) ME Region Flash Protection Override

No

#	Parameter	Platform	Settings
3	Intel® ME Firmware Update		
	Hide Intel® MEBx Firmware Update Control Values: Yes/No This setting allows the customer to hide the Firmware Update option in the Intel® MEBx interface.	RPP-S	No
	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.	RPP-S	0 string
	OEM FW Version Value: Hex Input This setting contains the OEM OIP version	RPP-S	0x0
	Intel® ME Region Flash Protection Override Values: Yes/No This setting enables descriptor unlock of the Intel® CSME Region when the HMRFP0 message is sent to firmware prior to BIOS End of POST.	RPP-S	No

Select Intel® ME Kernel on the left side menu then click Image Identification on the right to expand:

Image Identification 4

OEM Tag

0x0

#	Parameter	Platform	Settings
4	Image Identification		
	OEM Tag This is a free form 32bit field that allows the OEM to configure their own unique identifier in the firmware image.	RPP-S	0x00000000 0x00000000

Select Intel® ME Kernel on the left side menu then click Intel® ME Measured Boot Configuration on the right to expand:

Table 2-12. - Intel® ME Kernel (Sheet 3 of 5)

Intel (R) Me Measured Boot Configuration 5

Intel(R) ME Measured Boot State

Disabled

#	Parameter	Platform	Settings
5	Intel® ME Measured Boot Configuration		
	Intel® ME Measured Boot State Values: Enabled / Disabled When measured boot is enabled firmware will use additional extended registers for all IUPs and Key Manifests that firmware loads and verifies from flash. Note: When measured boot is enabled any IUPs or firmware updates will require a global reset	RPP-S	Disabled

Select Intel® ME Kernel on the left side menu then click MCTP Configuration on the right to expand:

MCTP Configuration 6

MCTP Stack Configuration

0x920030

MCTP PCIe Address

0x0

MctpDevicePortEc

0x2

MctpDevicePortSio

0x0

MctpDevicePortIsh

0x0

MctpDevicePortBmc

0x0

#	Parameter	Platform	Settings
6	MCTP Configuration		
	MCTP Stack Configuration Values: Hex Defines the ME's 8-bits MCTP Endpoint IDs for each SMBus physical interface (SMBus, SMLink0 and SMLink1). These values are needed for FW to communicate with MCTP end points. For each of these 3 bytes, a value of 0x00 means not used, and values 0xFF or 0x01 - 0x07 or 0x20 - 0x2F are not allowed.	RPP-S	0x920030
	MCTP PCIe Address Values: Hex	RPP-S	0x0
	MctpdevicePortEc Values: Hex	RPP-S	0x2
	MctpdevicePortSio Values: Hex	RPP-S	0x00
	MctpdevicePortIsh Values: Hex	RPP-S	0x00

Table 2-12. - Intel® ME Kernel (Sheet 4 of 5)

	MctpdevicePortBmc Values: Hex	RPP-S	0x00
Select Intel® ME Kernel on the left side menu then click Firmware Diagnostics on the right to expand:			
<div> Firmware Diagnostics 7 </div> <div> Automatic Built in Self Test Disabled </div>			
#	Parameter	Platform	Settings
7	Firmware Diagnostics		
	Automatic Built in Self Test Values: Enabled/Disabled This setting enables the firmware Automatic Built in Self Test which is executed during first platform boot after initial image flashing.	RPP-S	Disabled Disabled
Select Intel® ME Kernel on the left side menu then click End of Manufacturing Configuration on the right to expand:			
<div> End of Manufacturing Configuration 8 </div> <div> Flexible EOM setting options Lock Descriptor and OEM Configs </div> <div> EOM on First Boot Enabled No </div>			
#	Parameter	Platform	Settings
8	End of Manufacturing Configuration		
	EOM of First Boot Enabled Value: Yes/No This setting determines if End of Manufacturing will be triggered on first boot of the platform after flashing. Note: When this setting is enabled Intel® CSME will enter End of Manufacturing regardless of the descriptor settings.	RPP-S	No
	Flexible EOM setting options Value: Lock Descriptor and OEM Configs/Lock OEM Configs Only/Lock Descriptor Only/Do not lock Descriptor and OEM Configs This setting determines which settings will be automatically committed during End of Manufacturing flows. Note: The FPFs, RPMB / RPMC and set manufacturing mode settings are mandatory and cannot be overridden revenue parts. Simulation can be done on non-revenue part with the Hardware binding set to disabled.	RPP-S	Lock Descriptor and OEM Configs
Select Intel® ME Kernel on the left side menu then click Intel® ME Boot Configuration on the right to expand:			
<div> Intel(R) ME Boot Configuration 9 </div> <div> Persistent PRTC Backup Power Exists </div>			

Table 2-12. - Intel® ME Kernel (Sheet 5 of 5)

#	Parameter	Platform	Settings
9	Intel® ME Boot Configuration		
	Persistent PRTC Backup Power Values: None / Exists FPF that indicates if the device is designed such that it may lose PRTC power more than 10 times throughout the normal life-cycle of the product and hence has no persistent time or AR protection. At EOM this value is burned to the FPF, and can never be changed	RPP-S	Exists

Table 2-13. - Integrated Sensor Hub (Sheet 1 of 2)

Select Integrated Sensor Hub on the left side menu then click on Integrated Sensor Hub is expanded by default:			
<div> <div>Integrated Sensor Hub</div> <div>1</div> <div>Q</div> </div> <div> <div>Integrated Sensor Hub Supported</div> <div>Yes</div> </div> <div> <div>Integrated Sensor Hub Initial Power State</div> <div>Disabled</div> </div>			
#	Parameter	Platform	Settings
1	Integrated Sensor Hub		
	Integrated Sensor Hub Supported Values: Yes/No This setting allows customers to disable ISH on the platform.	RPP-S	No
	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.	RPP-S	Disabled
Select Integrated Sensor Hub on the left side menu then click ISH Data on the right to expand:			
<div> <div>ISH Data</div> <div>2</div> <div>Q</div> </div> <div> <div>ISH PDT Binary File</div> <div>...</div> </div>			
#	Parameter	Platform	Settings
2	Integrated Sensor Hub - ISH Data		
	PDT Binary File	RPP-S	Path for PDT Binary file
Select Integrated Sensor Hub on the left side menu then click ISH Image on the right to expand:			
<div> <div>ISH Image</div> <div>3</div> <div>Q</div> </div> <div> <div>ISH Input File</div> <div>...</div> </div> <div> <div>ISH Version</div> <div></div> </div> <div> <div>Integrated Sensor Hub Length</div> <div>0x40000</div> </div>			
#	Parameter	Platform	Settings
3	ISH Image		

Table 2-13. - Integrated Sensor Hub (Sheet 2 of 2)

	ISH Input File	RPP-S	ISH Binary (Optional)
	Version - This displays the version of ISH		
	Length - Total size (in bytes) of the ISH code partition including reserved space. It is recommended to be at least 256kb.		

Table 2-14. - Integrated Clock Controller (Sheet 1 of 8)

Select Integrated Clock Controller on the left side menu then click Integrated Clock Controller Policies on the right to expand:			
<div> <div>Integrated Clock Controller Policies</div> <div> <div>1</div> <div> <div>Boot Profile</div> <div>Profile 0</div> </div> <div> <div>Failsafe Boot Profile</div> <div>Profile 0</div> </div> <div> <div>Profile Changeable</div> <div>true</div> </div> <div>Profiles</div> </div> </div>			
#	Parameter	Platform	Settings
1	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.	RPP-S	Profile 0
	Failsafe Profile This parameter specifies the profile index of the fail-safe profile. On boot failure detection or CMOS clear the Intel® ME 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.	RPP-S	Profile 0
	Profile Changeable Values: 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.	RPP-S	True
	Profiles Selecting this option will expand the Profile entry options.		
Click on Profiles expanded on the right to expand:			

Table 2-14. - Integrated Clock Controller (Sheet 2 of 8)


Profile 2 			
Clock Output Configuration Power Management Configuration Hybrid Storage Configuration Profile Active State <input type="text" value="true"/> Profile Name <input type="text" value="Profile 0"/>			
#	Parameter	Platform	Settings
2	Profile		
	Clock Output Configuration Selecting this option will expand the Clock Output Configuration entry options.		
	Power Management Configuration Selecting this option will expand the Power Management Configuration entry options.		
	Hybrid Storage Configuration Selecting this option will expand the Hybrid Storage Configuration entry options.		
	Profile Active State Values: false / true This setting determines if a Profile is active. By default it re-defined "Profile 0" the active profile.	RPP-S	true
	Profile Name Value: User Text String Entry This parameter allows user to customize profile name for easy identification. By default it uses pre-defined profile name like Profile 0.	RPP-S	Profile 0
Click on Clock Output Configuration on the right to expanded:			

Table 2-14. - Integrated Clock Controller (Sheet 3 of 8)

Clock Output Configuration 3 Q			
	PHY_REFCLK_EXTINJ	Internal	▼
	SSCEN	Enabled	▼
	CPUNSSC2	Disabled	▼
	CPUNSSC2 SRC Mapping	SRC1	▼
	CPUBCLK2	Disables 2nd CPUBCLK	▼
	SRC0	Disabled	▼
	SRC1	Disabled	▼
	SRC2	Disabled	▼
	SRC3	Disabled	▼
	SRC4	Disabled	▼
	SRC5	Disabled	▼
	SRC6	Disabled	▼
	SRC7	Disabled	▼
	SRC8	Disabled	▼
	SRC9	Disabled	▼
	SRC10	Disabled	▼
	SRC11	Disabled	▼
	SRC12	Disabled	▼
	SRC13	Disabled	▼
	SRC14	Disabled	▼
	SRC15	Disabled	▼
	SRC16	Disabled	▼
	SRC17	Disabled	▼
#	Parameter	Platform	Settings

Table 2-14. - Integrated Clock Controller (Sheet 4 of 8)

3	Clock Output Configuration		
	PHY_REFCLK_EXT_INJ Values: Internal / External	RPP-S	Internal
	SSCEN Values: Disabled / Enabled	RPP-S	Enabled
	CPUNSSC2 Values: Disabled / Enabled	RPP-S	Disabled
	CPUNSSC2 SRC Mapping Values: SRC1 / SRC2 / SRC3 / SRC4 / SRC5 / SRC6 / SRC7 / SRC8 / SRC9 / SRC10 / SRC11 / SRC12 SRC13 / SRC14 / SRC15 /SRC16 / SRC17	RPP-S	SRC1
	CPUBCLK2 Values: Disables 2nd CPUBCLK / Enables 2nd CPUBCLK	RPP-S	Disables 2nd CPUBCLK
	SRC0[6:17] 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. These parameters are specifically used to Enable/Disable the respective CLKOUT_XXX differential output buffers	RPP-S	Enabled
	SRC1 Values: Enabled/Disabled Enables or Disables the CLKOUT_SRC1 differential output buffer.	RPP-S	Enabled
	SRC2 Values: Enabled/Disabled Enables or Disables the CLKOUT_SRC2 differential output buffer.	RPP-S	Enabled
	SRC3 Values: Enabled/Disabled Enables or Disables the CLKOUT_SRC3 differential output buffer.	RPP-S	Enabled
	SRC4 Values: Enabled/Disabled Enables or Disables the CLKOUT_SRC4 differential output buffer.	RPP-S	Enabled
	SRC5 Values: Enabled/Disabled Enables or Disables the CLKOUT_SRC5 differential output buffer.	RPP-S	Enabled
	SRC6 Values: Enabled/Disabled Enables or Disables the CLKOUT_SRC6 differential output buffer.	RPP-S	Enabled
	SRC7 Values: Enabled/Disabled Enables or Disables the CLKOUT_SRC7 differential output buffer.	RPP-S	Enabled
	SRC8 Values: Enabled/Disabled Enables or Disables the CLKOUT_SRC8 differential output buffer.	RPP-S	Enabled
	SRC9 Values: Enabled/Disabled Enables or Disables the CLKOUT_SRC9 differential output buffer.	RPP-S	Enabled
	SRC10 Values: Enabled/Disabled Enables or Disables the CLKOUT_SRC10 differential output buffer.	RPP-S	Enabled

Table 2-14. - Integrated Clock Controller (Sheet 5 of 8)

	SRC11 Values: Enabled/Disabled Enables or Disables the CLKOUT_SRC11 differential output buffer.	RPP-S	Enabled
	SRC12 Values: Enabled/Disabled Enables or Disables the CLKOUT_SRC12 differential output buffer.	RPP-S	Enabled
	SRC13 Values: Enabled/Disabled Enables or Disables the CLKOUT_SRC13 differential output buffer.	RPP-S	Enabled
	SRC14 Values: Enabled/Disabled Enables or Disables the CLKOUT_SRC14 differential output buffer.	RPP-S	Enabled
	SRC15 Values: Enabled/Disabled Enables or Disables the CLKOUT_SRC15 differential output buffer.	RPP-S	Enabled
	SRC16 Values: Enabled/Disabled Enables or Disables the CLKOUT_SRC16 differential output buffer.	RPP-S	Enabled
	SRC17 Values: Enabled/Disabled Enables or Disables the CLKOUT_SRC17 differential output buffer.	RPP-S	Enabled
Click on Power Management Configuration on the right to expanded:			

Table 2-14. - Integrated Clock Controller (Sheet 6 of 8)

Power Management Configuration 4

SRC0 CLKREQ# Mapping SRCCLKREQB_0	<input type="text" value="GPP_D_0"/>
SRC1 CLKREQ# Mapping SRCCLKREQB_1	<input type="text" value="GPP_D_1"/>
SRC2 CLKREQ# Mapping SRCCLKREQB_2	<input type="text" value="GPP_D_2"/>
SRC3 CLKREQ# Mapping SRCCLKREQB_3	<input type="text" value="GPP_D_3"/>
SRC4 CLKREQ# Mapping SRCCLKREQB_4	<input type="text" value="GPP_D_11"/>
SRC5 CLKREQ# Mapping SRCCLKREQB_5	<input type="text" value="GPP_D_12"/>
SRC6 CLKREQ# Mapping SRCCLKREQB_6	<input type="text" value="GPP_D_13"/>
SRC7 CLKREQ# Mapping SRCCLKREQB_7	<input type="text" value="GPP_D_14"/>
SRC8 CLKREQ# Mapping SRCCLKREQB_8	<input type="text" value="GPP_H_2"/>
SRC9 CLKREQ# Mapping SRCCLKREQB_9	<input type="text" value="GPP_H_3"/>
SRC10 CLKREQ# Mapping SRCCLKREQB_10	<input type="text" value="GPP_H_4"/>
SRC11 CLKREQ# Mapping SRCCLKREQB_11	<input type="text" value="GPP_H_5"/>
SRC12 CLKREQ# Mapping SRCCLKREQB_12	<input type="text" value="GPP_H_6"/>
SRC13 CLKREQ# Mapping SRCCLKREQB_13	<input type="text" value="GPP_H_7"/>
SRC14 CLKREQ# Mapping SRCCLKREQB_14	<input type="text" value="GPP_H_8"/>
SRC15 CLKREQ# Mapping SRCCLKREQB_1	<input type="text" value="GPP_H_9"/>
SRC16 CLKREQ# Mapping SRCCLKREQB_16	<input type="text" value="GPP_J_8"/>
SRC17 CLKREQ# Mapping SRCCLKREQB_17	<input type="text" value="GPP_J_9"/>

#	Parameter	Platform	Settings
4	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 configure CLKREQ parameters accordingly.		

Table 2-14. - Integrated Clock Controller (Sheet 7 of 8)

SRC0[5:0] 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.	RPP-S	GPP_D_0
SRC[15:6] CLKREQ# Mapping - RPL-S Only Possible configuration: Select one of the GPIOs from the list to map it as a CLKREQ# for specific SRC# Output put clock. This parameter controls association of dynamic CLKREQ control with SRC (PCIe) clocks.		
SRC1 CLKREQ# Mapping Assign the CLKREQ# signal associated with CLKOUT_SRC1.	RPP-S	GPP_D_1
SRC2 CLKREQ# Mapping Assign the CLKREQ# signal associated with CLKOUT_SRC2.	RPP-S	GPP_D_2
SRC3 CLKREQ# Mapping Assign the CLKREQ# signal associated with CLKOUT_SRC3.	RPP-S	GPP_D_3
SRC4 CLKREQ# Mapping Assign the CLKREQ# signal associated with CLKOUT_SRC4.	RPP-S	GPP_D_11
SRC5 CLKREQ# Mapping Assign the CLKREQ# signal associated with CLKOUT_SRC5.	RPP-S	GPP_D_12
SRC6 CLKREQ# Mapping Assign the CLKREQ# signal associated with CLKOUT_SRC6.	RPP-S	GPP_D_13
SRC7 CLKREQ# Mapping Assign the CLKREQ# signal associated with CLKOUT_SRC7.	RPP-S	GPP_D_14
SRC8 CLKREQ# Mapping Assign the CLKREQ# signal associated with CLKOUT_SRC8.	RPP-S	GPP_H_2
SRC9 CLKREQ# Mapping Assign the CLKREQ# signal associated with CLKOUT_SRC9.	RPP-S	GPP_H_3
SRC10 CLKREQ# Mapping Assign the CLKREQ# signal associated with CLKOUT_SRC10.	RPP-S	GPP_H_4
SRC11 CLKREQ# Mapping Assign the CLKREQ# signal associated with CLKOUT_SRC11.	RPP-S	GPP_H_5
SRC12 CLKREQ# Mapping Assign the CLKREQ# signal associated with CLKOUT_SRC12.	RPP-S	GPP_H_6
SRC13 CLKREQ# Mapping Assign the CLKREQ# signal associated with CLKOUT_SRC13.	RPP-S	GPP_H_7
SRC14 CLKREQ# Mapping Assign the CLKREQ# signal associated with CLKOUT_SRC14.	RPP-S	GPP_H_8
SRC15 CLKREQ# Mapping Assign the CLKREQ# signal associated with CLKOUT_SRC15.	RPP-S	GPP_H_9
SRC16 CLKREQ# Mapping Assign the CLKREQ# signal associated with CLKOUT_SRC16.	RPP-S	GPP_J_8
SRC17 CLKREQ# Mapping Assign the CLKREQ# signal associated with CLKOUT_SRC17.	RPP-S	GPP_J_9

Click on Hybrid Storage Enable Configuration on the right to expanded:

Hybrid Storage Configuration

5



Hybrid Storage CLKREQ# Mapping (SRCCLKREQB_18)

CLKOUT_SRC_P/N_0

Hybrid Storage Enable

Disabled

Table 2-14. - Integrated Clock Controller (Sheet 8 of 8)

#	Parameter	Platform	Settings
5	Hybrid Storage Enable Configuration		
	Hybrid Storage CLKREQ# Mapping (SRCCLKREQB_18) Values: CLKOUT_SRC_P/N_0, CLKOUT_SRC_P/N_1, CLKOUT_SRC_P/N_2, CLKOUT_SRC_P/N_3, CLKOUT_SRC_P/N_4, CLKOUT_SRC_P/N_5, CLKOUT_SRC_P/N_6, CLKOUT_SRC_P/N_7, CLKOUT_SRC_P/N_8, CLKOUT_SRC_P/N_9, CLKOUT_SRC_P/N_10, CLKOUT_SRC_P/N_11, CLKOUT_SRC_P/N_12, CLKOUT_SRC_P/N_13, CLKOUT_SRC_P/N_14, CLKOUT_SRC_P/N_15, CLKOUT_SRC_P/N_16, CLKOUT_SRC_P/N_17	RPP-S	Internal
	Hybrid Storage Enable Values: Enabled / Disabled	RPP-S	Disabled

Table 2-15. - CPU Straps (Sheet 1 of 3)

Select CPU Straps on the left side menu then click CPU Straps on the right to expand:			
<div> <div>CPU Straps</div> <div>1</div> <div> <div>Disable Hyperthreading</div> <div>No</div> </div> <div> <div>Number of Active Big Cores</div> <div>All Cores Active</div> </div> <div> <div>BIST Initialization</div> <div>No</div> </div> <div> <div>Flex Ratio</div> <div>0x0</div> </div> <div> <div>Processor Boot at P1 Frequency</div> <div>Yes</div> </div> <div> <div>JTAG Power Disable</div> <div>No JTAG Power on C10 and Lower</div> </div> <div> <div>Number of Active Small Cores</div> <div>All Cores Active</div> </div> <div> <div>VCC 1.05v CPU Source</div> <div>VCC 1.05v CPU source Platform Rail</div> </div> <div> <div>VCCP 1.05 CPU PG Exists</div> <div>VCCP 1.05 CPU PG Not present</div> </div> <div> <div>VCCIN AUX IMON Enabled</div> <div>No</div> </div> <div> <div>IA SVID Address</div> <div>0x0</div> </div> <div> <div>IA VR Type</div> <div>SVID</div> </div> <div> <div>GT_S SVID Address</div> <div>0x1</div> </div> <div> <div>GT_S VR Type</div> <div>SVID</div> </div> <div> <div>IA VR Offset VID Enabled</div> <div>Yes</div> </div> <div> <div>Platform IMON</div> <div>Disabled</div> </div> <div> <div>P2 to P2 Transition Clock Domain</div> <div>P2 to P2 Async to PCLK</div> </div> <div> <div>HSIO Lane Force Detect</div> <div>No Force Detect</div> </div> <div> <div>HSIO Lane Rx Detection Bypass</div> <div>Rx Detect No Bypass</div> </div> </div>			
#	Parameter	Platform	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.	RPP-S	No

Table 2-15. - CPU Straps (Sheet 2 of 3)

	Number of Active Big Cores Values: All Cores Active, 1 Core Active, 2 Cores Active, 3 Cores Active, 4 Cores Active, 5 Cores Active, 6 Cores Active, 7 Cores Active This setting controls the number of active Big processor cores. Note: This strap is intended for debugging purposes only. See BIOS Spec for more details on enabling or disabling processor cores.	RPP-S	All Cores Active
	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.	RPP-S	No
	Flex Ratio This setting controls the maximum processor non-turbo ratio. Note: This strap is intended for debugging purposes only. See BIOS Spec for more details on maximum processor non-turbo ratio configuration.	RPP-S	0x0
	Processor Boot at P1 Frequency Values: Yes/No This setting determines if the processor will operate at maximum frequency at power-on and boot. Note: This strap is intended for debugging purposes only.	RPP-S	Yes
	JTAG Power Disable Values: JTAG Power on C10 and Lower/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.	RPP-S	No JTAG Power on C10 and Lower
	Number of Active Small Cores Values: All Cores Active, 1 Core Active, 2 Cores Active, 3 Cores Active, 4 Cores Active, 5 Cores Active, 6 Cores Active, 7 Cores Active, 8 Cores Active This setting controls the number of active Small processor cores. Note: This strap is intended for debugging purposes only. See BIOS Spec for more details on enabling or disabling processor cores.	RPP-S	All Cores Active
	VCC 1.05 CPU Source Values: VCC 1.05v CPU Source PCH/VCC 1.05v CPU Source Platform Rail This setting determines where the VCC 1.05v CPU sourced from.	RPP-S	VCC 1.05v CPU Source PCH
	VCCP 1.05 CPU PG Exists Values: VCCP 1.05 CPU PG Not Present, VCCP 1.05 CPU PG Present This enables VCCP 1.05 CPU Power Gating capabilities if present on the platform.	RPP-S	VCCP 1.05 CPU PG Not Present
	VCCIN AUX IMON Enabled This setting determines if VCCIN Aux IMON is enabled Note: This strap should be left at the recommended default setting.	RPP-S	Yes
	IA SVID Address This setting determines the IA SVID Address. See Processor EDS for details. Note: This strap should be left at the recommended default setting.	RPP-S	0x0
	IA VR Type Values: SVID/Fixed VR This setting determines the IA Type. See Processor EDS for details.	RPP-S	SVID
	GT_S SVID Address This setting determines the GT_S SVID Address. See Processor EDS for details. Note: This strap should be left at the recommended default setting.	RPP-S	0x1
	GT_S VR Type Values: SVID/Fixed VR This setting determines the GT_S VR Type. See Processor EDS for details.	RPP-S	SVID

Table 2-15. - CPU Straps (Sheet 3 of 3)

	IA VR Offset Enabled Values: Yes / No This enables / disables the voltage offset for the IA VR levels to exceed 1.52v.	RPP-S	Yes
	Platform IMON Value: Enabled/Disabled Note: This strap should be left at the recommended default setting.	RPP-S	Disabled
	P2 to P2 Transition Clock Domain Values: P2 to P2 Sync to PCLK / P2 to P2 Async to PCLK This setting controls the P2 to P2 Transition Clock Domain	RPP-S	P2 to P2 Async to PCLK
	HSIO Lane Force Detect Values: No Force Detect / Force x16 Link / Force x8 Link / Force x4 Link Lanes 0-3 / Force x2 Link Lanes 0-1 / Force x1 Link Lane 0 This setting allows High Speed I/O lane configuration to be statically assigned to specific lane configurations (i.e. x2, x4, x8 x16 etc.) regardless of detection.	RPP-S	No Force Detect
	HSIO Lane Rx Detection Bypass Values: Rx Detect Bypass / Rx Detect No Bypass This setting enables / disables Receiver detection for HSIO Lane configuration. Note: This setting has no affect when the HSIO Lane Force Detect setting is configured to No Force Detect.	RPP-S	Rx Detect No Bypass

Table 2-16. - FW Update Image Build

Select FW Update Image Build on the left side menu to expand:			
<div> <div>FW Update Image Build</div> <div>1</div> <div> <div>OEM_KM Enabled</div> <div>Enabled</div> </div> <div> <div>NPHY Enabled</div> <div>Enabled</div> </div> <div> <div>SPHY Enabled</div> <div>Enabled</div> </div> <div> <div>ISH Enabled</div> <div>Enabled</div> </div> </div>			
#	Parameter	Platform	Settings
1	FW Update Image Build Note: Binaries for each of the FW Update Image Build settings below need to be populated under their respective tab locations.		
	OEM_KM Enabled Values: Enabled/Disabled This setting Enables / Disables OEM KM in the FWUpdate image.	RPP-S	Enabled
	NPHY Enabled Values: Enabled/Disabled This setting Enables / Disables PHY in the FWUpdate image.	RPP-S	Enabled
	SPHY Enabled Values: Binary File This loads the SPHY binary merged into the output image generated by the Intel® FIT tool.	RPP-S	Enabled
	ISH Enabled Values: Enabled/Disabled This setting Enables / Disables ISH in the FWUpdate image.	RPP-S	Enabled

Table 2-19. - Camera

Select Camera on the left side menu then click IPU Security Configuration on the right to expand:			
<div> <div>IPU Security Configuration</div> <div>1</div> <div> <div>Camera privacy feature control disabled</div> <div>true</div> </div> <div> <div>Secure Touch</div> <div>Disabled</div> </div> <div> <div>FW Secure Mode</div> <div>Enabled</div> </div> <div> <div>Secure Touch and Camera Mask</div> <div>0xFF</div> </div> </div>			
#	Parameter	Platform	Settings
1	IPU Security Configuration on		
	Camera privacy feature control disabled Values: True / False This setting enables / disables the Camera Privacy feature. Configuring this setting to 'False' means that the Camera Privacy GPIO pin value is used to mask / unmask all of the camera's data from being used.	RPP-S	True
	Secure Touch Values: Enabled / 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.	RPP-S	Disabled
	FW Secure Mode Values: Enabled / Disabled 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.	RPP-S	Enabled
	Secure Touch Camera Mask Values: Hex Input 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.	RPP-S	0xFF

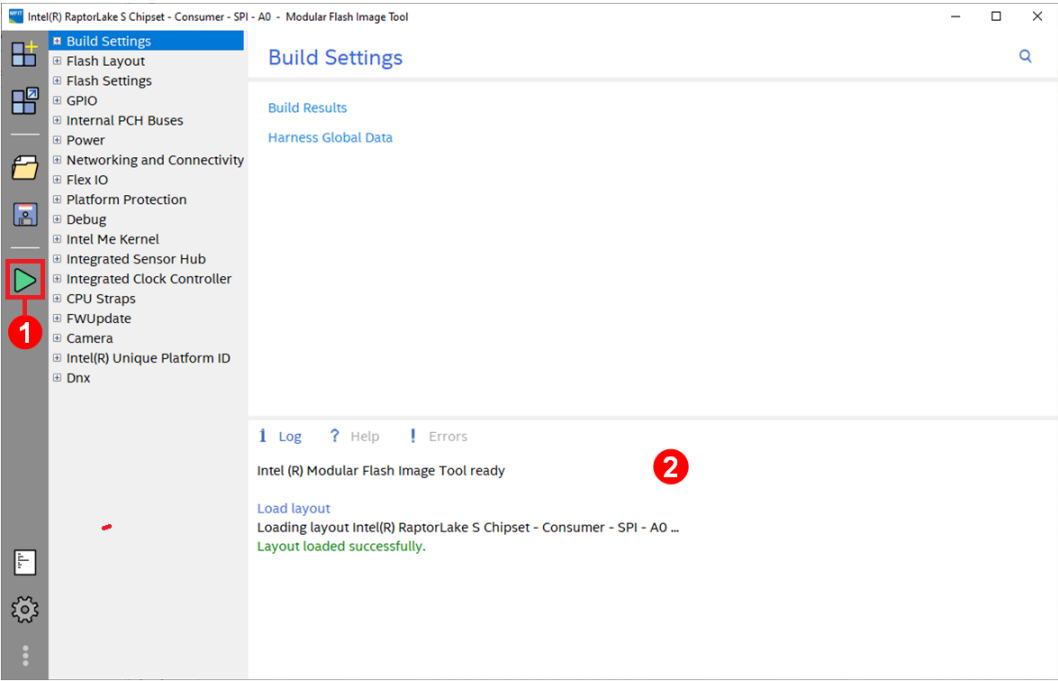

Table 2-20. - Intel® Unique Platform ID

Select Intel® Unique Platform ID Configuration on the left side menu then click Entitlement Configuration on the right to expand:			
<div> Entitlements Configuration 1 </div> <div> Intel(R) ICPS SW SKUing Eligible <input type="text" value="No"/> </div>			
#	Parameter	Platform	Settings
1	Entitlement Configuration		
	Intel® ICPS SW SKUing Eligible Value: Yes / No This setting enables Intel Connectivity Performance Suite License functionality on the platform.	RPP-S	No
Select Intel® Unique Platform ID Configuration on the left side menu then click Intel® Unique Platform ID Configuration on the right to expand:			
<div> Intel(R) Unique Platform ID Configuration 2 </div> <div> OEM ID <input type="text" value="0x0"/> </div>			
#	Parameter	Platform	Settings
2	Intel® Unique Platform ID Configuration		
	OEM ID Values: Hex Input This setting allows the OEM to configure their PCIe Vendor ID Unique ID into the platform FPFs.	RPP-S	0x0

Table 2-21. - Dnx

Select DnX on the left side menu then click DnX Fuses on the right to expand:			
<div> <div>DnX Fuses</div> <div>1</div> <div> DnX Enabled <input type="text" value="Yes"/> OEM Platform ID <input type="text" value="0x0"/> </div> </div>			
#	Parameter	Platform	Settings
1	DnX Fuses		
	DnX Enabled Values: Yes / No This setting enables / disables DnX capabilities Caution: Setting this option to No will permanently disable DnX on the platform hardware.	RPP-S	Yes
	OEM Platform ID Value: Hex This configures the OEM Platform ID that DnX uses to verify the image is correct for the platform. Before FPFs are fused, this field is ignored and DnX will accept any image. After FPS lock, only images with this Platform ID will be accepted by DnX. Caution: Ensure that the Platform ID value is correctly populated prior to close of manufacturing on the platform.	RPP-S	0

Table 2-22. - Intel® FIT - Build Image

		
1		Green Arrow button This button labeled upon selection allows build of the image
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 devices. These files are assumed to be named **outimage(1).bin** and **outimage(2).bin**.

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

3.1.1 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.

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 device 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® CSME Firmware Status

Use the following steps to check the platform health and Intel® CSME 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: 17.0.0.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® CSME FW has successfully initialized
- Intel® CSME 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

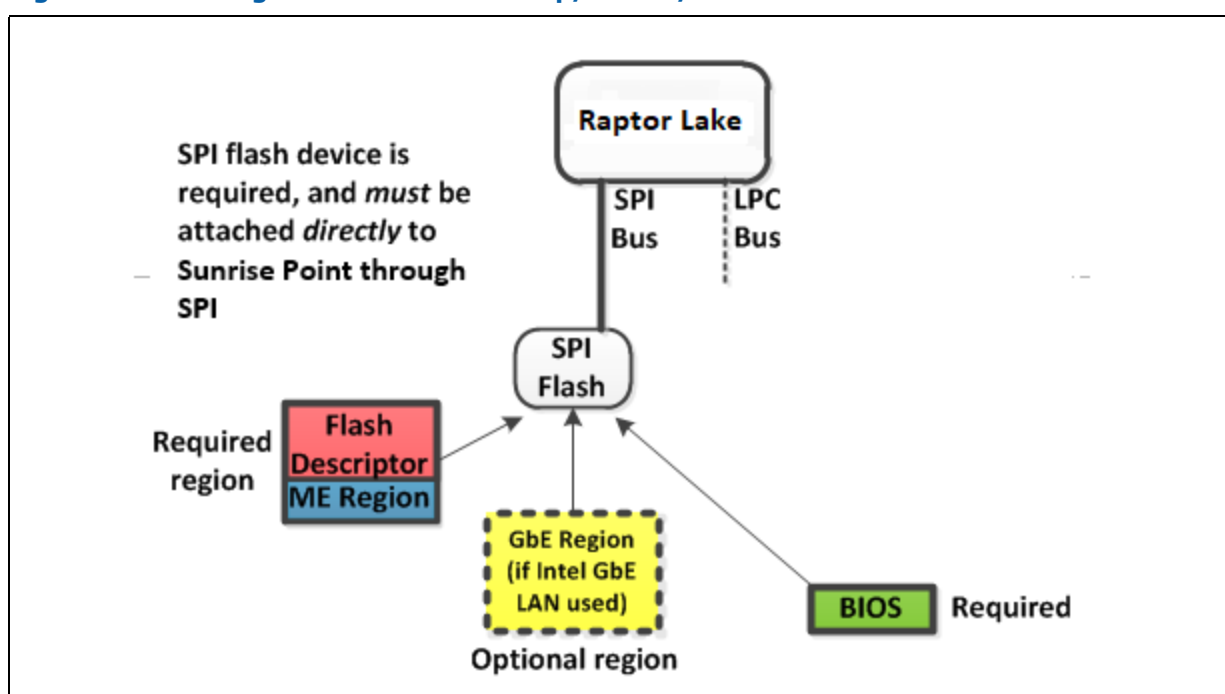
Problem / Issue	Solution / Workaround
System does not boot to DOS	By default, the system will boot to EFI Shell. To boot to DOS, <ol style="list-style-type: none"> 1. Enter BIOS menu, then go to the 'Boot' screen 2. Change 'Boot Option #1' to be your USB key (ensure USB key is formatted to be DOS bootable) 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 — Flash Configurations

This chapter covers only the basic information needed for clock control parameter programming. For a more detailed treatment of Mainstream - Desktop Family clocks, see Intel® Raptor Lake PCH-S Clocks and Intel® Converged Security and Management Engine — Platform Compliance Guide for Intel® CSME Hardware.

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



§ §

B Appendix — Boot Guard Configuration

B.1 Boot Guard Profiles

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

Table B-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.

B.2 Enforcement Policies

Table B-2. Enforcement Policy Description

Error Enforcement Policy (ENF)	Enforcement Mode Name	Description
0	Unrestricted Mode	Infinite time before shutdown – don't shutdown the platform, let everything run normally.
1	Remediation Mode	30 minutes before shutdown – enough time to remediate the system, e.g. update BIOS or other data on flash via host tools.
2	Reserved	
3	Restricted Mode	0 minutes before shutdown – instant shutdown policy.

B.3 OEM Profile Parameters

Table B-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 B-2 for details.

C Appendix — Intel® Platform Trust Technology

C.1 Intel® Platform Trust Technology

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

Table C-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.

D Appendix — Integrated Sensor Hub (ISH) Public Key Settings

The following table describes the configuration matrix required for ISH configuration for the Intel® FIT tool. Please see System Tools User Guide within ME kit, Manufacturing Test with Intel® Converged Security and Management Engine (Intel® ME) Firmware 12 and Intel® Integrated Sensor Solution on Raptor Lake Mobile, Raptor Lake Desktop, (CDI # WIP) for additional details.

CLSMNF = Close Manufacturing switch used with Intel® Flash Programming Tool (FPT)

PV = Production Version

For additional information on FPT see System Tools User Guide included with ME kit under system tools folder.

Table D-1. ISH Public Key Settings

Firmware	MCP	FPF Automatic Commit	FPF MEI command after CLSMNF (Yes/No)	FPF MEI command before CLSMNF (Yes/No)
Pre-production	Production	No	No - Not a valid combination	No - Not a valid combination
Production (PV not set)	Pre-production	No	Yes	No
Production (PV not set)	Production	No	Yes	No
Pre-production	Pre-production	No	Yes	No
Production (PV not set)	Production	Yes	No	No

Note: The Intel® FIT allows integration of binary files within Integrated Sensor Hub section under ISH Image and ISH Data. The Intel® FIT does not generate or create the required files. The table above lists configuration combinations that can be used.



Table D-2.

D.1 OpenSSL:

- Insert the desired certificate to OpenSSL to generate the certificate hash
- Use the following command to generate the certificate hash: ***openssl.exe dgst -sha256 [cert]***

Open SSL result for example: SHA256(ADL_DEBUG000_ODCA_CA2.cer)=
2458f69943a4779c58a419a035360868aa444faf28d54c9147664489bc740a1d

Table D-3.

1. Next highlight and copy the value returned by OpenSSL. This is the certificate Hash stream.
2. Go back into the Intel® mFIT tool and select the certificate to be used for the certificate Hash streams value.
3. Under the selected certificate set the "Certificate Enabled" option to "Yes".
4. Next input a name for your certificate in the "Certificate Friendly Name" entry box.
5. Finally paste the certificate Hash stream value copied from the command prompt window in step 1 into the "Certificate Stream entry box."

